# La répression de la cybercriminalité : données et bilan 2001-2004 en matière de cartes bancaires

Yves RANDOUX*

Historiquement, la carte est un instrument d'accréditation destiné à renforcer l'identification du porteur au moment du paiement. Dans les années 1970, une piste magnétique a été apposée sur le verso de cette carte, devenue instrument de paiement, pour en faciliter l'exploitation électronique. La France, 20 ans plus tard, a franchi un pas supplémentaire en matière de sécurité en insérant un microprocesseur sur la carte, créant ainsi la carte à puce.

Aujourd'hui, ces deux modèles technologiques sont utilisés dans le monde pour assurer les paiements de proximité :

- l'un utilise la carte à piste magnétique destinée au contrôle en ligne des données d'identification associée le plus souvent à la signature manuscrite pour l'authentification du porteur ;
- l'autre est en mode *semi-off line* : c'est celui de la carte à microprocesseur avec contrôle de l'identification de la carte et de l'authentification du porteur par vérification du code confidentiel dans la puce et contrôle en ligne optionnel selon le montant de l'opération.

Le modèle à piste est largement reconnu comme obsolète ; tous les pays du monde, à l'exception notoire des États-Unis, organisent leur migration progressive vers la puce. Cette délicate et complexe opération s'achèvera vraisemblablement à la fin de la présente décennie.

Pourquoi la puce ? Pour répondre au souci légitime de protéger les actifs de leurs clients et lutter contre la fraude, ce mal endémique à tout système de paiement, les banques CB ont recherché un mécanisme simple, pratique et sûr. Elles ont fait, dès 1990, le choix de la carte à puce après une période de test de plus de 3 ans et l'ont adopté définitivement en faisant, de plus, le pari que simplicité et ergonomie attractive

* Administrateur du GIE Cartes bancaires.

pouvaient se conjuguer avec sécurité et coûts faibles. La technologie de la carte à puce permet, en effet, de résoudre de façon élégante les deux problèmes posés en matière de paiement électronique : l'identification et l'authentification. L'identification permet de s'assurer que le support, c'est-à-dire la carte, est un acteur autorisé dans l'opération faite par le porteur. Cette identification est réalisée électroniquement par un calcul de clés cryptographiques échangées entre la carte et le terminal. Elle donne au porteur le droit d'effectuer une opération dans le système qui reconnaît sa carte, mais celle-ci ne sera juridiquement « bouclée » que par la signature électronique qui matérialise son ordre de payer. Dans le monde de la carte à piste, l'authentification du porteur se fait par la signature manuscrite apposée sur le ticket de caisse édité par le terminal ; dans le monde de la carte à puce, cette authentification se déroule par la vérification par la puce du code secret composé sur le clavier et détenu par le porteur, qui est une véritable signature électronique.

Dans les deux cas, la banque reçoit des enregistrements électroniques soit *on line*, soit *off line,* protégés par des certificats électroniques, eux-mêmes protégés dans le transport, dans des conditions sécuritaires permettant à la banque d'accepter ou de refuser le paiement.

## SÉCURISER LE PAIEMENT ÉLECTRONIQUE

Les instruments de paiement (billets, pièces, chèques, virements, cartes...) ont toujours suscité convoitise et contrefaçon. L'introduction de l'électronique dans cet univers a fait apparaître une nouvelle forme de délinquance : la cybercriminalité. Avant de traquer leurs méfaits, quel est le cadre juridique protégeant les paiements et les retraits par carte bancaire ?

### La loi du 13 mars 2000

C'est en vertu de la loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique que l'Assemblée nationale adaptait officiellement le droit de la preuve de signature aux exigences des nouvelles technologies de l'information. Le Code civil est, en effet, modifié dans plusieurs articles :

- « la preuve littérale ou preuve par écrit s'étend à tout type de dispositif » (article 1316) ;
- « l'écrit sous sa forme électronique est admis comme preuve au même titre que l'écrit sur support papier » (article 1316-1) ;
- « l'écrit sur support électronique a la même force probante que l'écrit sur support papier » (article 1316-3) ;
- la signature électronique est également définie.

Cette loi transposant la directive européenne du 13 décembre 1999 ne modifie pas, en réalité, le cadre juridique dans lequel se déroulent les opérations par cartes bancaires CB. En effet, si le législateur européen a souhaité harmoniser le cadre juridique de la signature pour l'adapter aux exigences technologiques de notre époque, il n'a pas pour autant modifié les

régimes juridiquement protégés par des contrats.

## Le microprocesseur au service de la preuve de la signature

Les achats de biens et services se déroulent dans un cadre juridiquement protégé. Le système de paiement CB permet le bon déroulement de ces transactions puisqu'il repose sur une dualité de contrats : contrat entre la banque et le porteur ; contrat entre la banque et le commerçant/accepteur de transactions de paiement. Sur cette base contractuelle, bien avant la directive européenne, le juge, en France, valide la preuve des ordres de paiement signés par un code confidentiel. En 1989, la Cour de cassation consacre la valeur juridique d'un ordre de paiement par carte donné par un client par la composition de son code confidentiel. Elle estime, en effet, dans le cadre d'un paiement par carte bancaire CB, que le procédé de preuve de l'ordre de paiement, étant contractuellement accepté par les parties au contrat (la banque et son client), est licite. En d'autres termes, et de façon simplificative, on peut dire que la Cour de cassation reconnaissait, bien avant l'heure, le mécanisme de signature électronique par la composition d'un code numérique dans un système de paiement comme un outil de validation d'un ordre de paiement.

En revanche, il est important de signaler qu'en transposant la directive européenne, notre pays s'est doté des éléments technologiques appropriés aux exigences juridiques nouvelles. Sans entrer plus avant dans ce dispositif qui est en marge de notre sujet, il faut simplement retenir la valeur de l'engagement juridique que va désormais revêtir le simple clic, fut-il assorti de protections cryptographiques particulières, dans la vie courante des internautes, et plus généralement de tout acte commercial ou administratif à distance.

## La loi du 15 novembre 2001

La loi du 15 novembre 2001 relative à la sécurité quotidienne incrimine le fait d'utiliser Internet ou les médias pour mettre à disposition des informations pour contrefaire des cartes de paiement.

La loi sur l'économie numérique (juillet 2003) renforce les peines prévues en 1988 par la loi Godfrain qui réprime les atteintes aux systèmes de traitement automatisé des données en retenant pour les caractériser à la fois l'élément matériel (par exemple, casser une clé cryptographique) et l'élément intentionnel (l'adverbe « frauduleusement » du texte, « le fait d'accéder ou de se maintenir frauduleusement ») qui matérialisent cette volonté de nuisance.

Le législateur en 2001 a néanmoins été plus à l'écoute du consommateur en introduisant notamment trois dispositions nouvelles dans le Code monétaire et financier :

- création d'un nouveau motif d'opposition au paiement par carte (outre le vol ou la perte de la carte) : l'utilisation frauduleuse de la carte ou des données liées à son utilisation (article 34 de la loi) ;

- la limitation de la perte financière subie par le porteur limitée à 150 euros depuis le 1er janvier 2003 en cas de perte ou de vol de la carte (article 35 de la loi) ;
- l'exonération de la responsabilité du porteur en cas de paiement effectué frauduleusement à distance, sans utilisation physique de la carte, et en cas de contrefaçon de sa carte si, au moment de l'opération contestée, il était en possession physique de sa carte (article 36 de la loi).

Ces dispositions s'accompagnent également de la création d'un Observatoire de la sécurité des paiements par carte et d'un renforcement substantiel de l'arsenal pénal de lutte contre la fraude en matière de paiement électronique. Ainsi, le législateur accorde aux instances répressives la possibilité d'intervenir énergiquement contre les cybercriminels. Désormais « 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 au premier article L. 163-3 » est puni de 7 ans d'emprisonnement et de 750 000 euros d'amende. Le tribunal peut également, en vertu de l'article 43 de la loi, prononcer « l'interdiction des droits civiques et, pour une durée de 5 ans au plus, d'exercer une activité professionnelle ou sociale... ». La loi prévoit également que les « personnes morales peuvent être déclarées responsables pénalement des infractions commises » aux articles L. 163-2-2, L. 163-4-1, L. 163-7 et L. 163-10.

## LA CYBERCRIMINALITÉ DANS LE SYSTÈME DE PAIEMENT DE CARTES CB

Le dispositif juridique décrit précédemment est vertueux en lui-même, car les fraudes ne peuvent rester inconnues du système. En effet, la loi française pose pour principe l'irrévocabilité du paiement (article L. 132-2 du Code monétaire et financier), et celui-ci est repris dans le contrat porteur CB (même s'il limite à 150 euros le préjudice subi par un porteur en cas de perte ou de vol de sa carte).

Concrètement, la fraude à la carte bancaire s'articule sur deux mécanismes : l'usurpation d'identité, et la falsification du support.

### Le contournement technologique en paiement de proximité

Aucun système n'est totalement fiable et les fraudeurs sont en permanence à l'affût des failles, aussi minces soient-elles, que peuvent présenter les nouvelles technologies.

#### Présentation des mécanismes de paiement par carte

##### *Piste et signature manuscrite*

Piste et signature manuscrite sécurisent aujourd'hui la quasi-totalité des paiements de proximité dans le monde, à l'exception du système CB en France et, depuis peu, les systèmes MasterCard et Visa en Grande-Bretagne. Ce mécanisme permet d'identifier le porteur en exploitant de façon électronique sur

des serveurs d'autorisation les données figurant dans la piste. Chaque transaction émise par le terminal d'un commerçant est dirigée automatiquement vers le serveur de la banque du porteur qui, après vérification de plusieurs paramètres, matérialise son accord à la transaction en transmettant un numéro d'autorisation inscrit sur le ticket édité par le terminal du commerçant. Pour authentifier l'ordre de paiement ainsi donné, le porteur appose ensuite sa signature sur ce même ticket, dont un double lui est remis. C'est donc une combinaison technologique (piste et ordinateur *on line*) et manuscrite qui sécurise la plupart des paiements par carte dans le monde à l'heure actuelle.

### *Puce et code confidentiel*

Puce et code confidentiel constituent une autre voie explorée avec succès par les banques CB depuis 1990. Ce mécanisme permet l'identification et l'authentification du porteur par la technologie de la puce associée à un code confidentiel, connu du seul porteur.

Les banques CB ont de surcroît tiré pleinement partie de cette technologie en évitant de faire appel à chaque transaction de paiement au serveur bancaire pour autoriser les transactions courantes, adaptées à la typologie des cartes et/ou des commerçants. Au-delà des plafonds mis en place, un contrôle automatique s'effectue vers les ordinateurs bancaires. C'est cette infrastructure qui est désormais en cours de diffusion dans le monde sur la base de spécifications implémentées par Visa et MasterCard, largement puisées dans les réalisations de CB.

### *Le numéro de la carte*

Enfin, le numéro de la carte associé au cryptogramme visuel[1] est le plus souvent utilisé dans les paiements à distance soit par téléphone, soit sur Internet. Dans cette hypothèse, l'identification du porteur est réalisée uniquement par cette séquence de numéros soumise à l'autorisation *on line* du serveur bancaire.

### *Le rôle des serveurs bancaires*

Traditionnellement, leur rôle est méconnu, mais ils sont essentiels à la sécurisation des paiements et des retraits. Ils doivent à tout moment et partout dans le monde répondre à la question posée par le terminal du commerçant ou le distributeur automatique de billets : « Peut-on accepter cette transaction ? ». Agissant en direct ou par délégation des banques, ces serveurs sont dotés de programmes informatiques sophistiqués capables de déceler les fraudes et/ou les paiements/retraits aberrants. Sans cesse mis à jour, utilisateurs des technologies les plus pointues, ces serveurs sont, en quelque sorte, les cybersurveillants de la planète des opérations par carte, apportant aux uns la vigilance qu'ils en exigent et aux autres les affres des conséquences de leurs actes délictueux. Leur rôle consiste donc, dans le cas d'un paiement ou d'un retrait, à donner leur accord à l'opération, matérialisé sous la forme d'un numéro d'autorisation et validé par un certificat, une signature électronique en quelque sorte de l'opération. Dans le contexte spécifique d'une opération par carte CB, dès lors que le certificat est produit, celle-ci

devient irrévocable et le paiement garanti au commerçant. Les paiements à distance s'appuient sur un mécanisme analogue à celui qui vient d'être décrit, avec l'exception notoire que la preuve que le détenteur légitime de la carte, seul habilité à donner un ordre de paiement, est inexistante et qu'en conséquence, le paiement ne peut être garanti au commerçant.

**Les voies de contournement**

Sans vouloir faire l'apologie des techniques utilisées par les fraudeurs, leur objectif va essentiellement consister soit à usurper l'identité du porteur, soit à contrefaire le support de paiement.

***L'usurpation d'identité***

C'est le cas le plus fréquent dans la technologie piste et signature : la carte peut être volée et utilisée immédiatement par des fraudeurs qui imiteront la signature. Divers raffinements dans ce champ d'action peuvent être recensés à l'heure actuelle, d'autant plus que les fraudeurs agissent de plus en plus en bandes organisées, dotées de moyens informatiques puissants pour recopier et utiliser les pistes magnétiques ainsi volées soit localement, soit à distance grâce à Internet. On rencontre également ce type de fraude avec les cartes à puce : le délinquant est suffisamment habile pour voir le porteur frapper son code confidentiel lors d'un retrait d'espèces dans un distributeur automatique de billets par exemple, et le mémoriser, puis il vole la carte (vol à la tire, ou collet marseillais) : le fraudeur capture la carte et l'utilise jusqu'à la mise en opposition par le porteur.

***La contrefaçon du support « piste »***

Ainsi, dans de nombreux cas récents et dans certains endroits précis (distributeurs automatiques de billets, distributeurs automatiques de carburant), on a pu voir des fraudeurs disposer d'appareils permettant de copier la piste des cartes et d'enregistrer par une microcaméra le code confidentiel composé par le porteur, le tout à son insu.

Des transactions frauduleuses de retraits d'espèces étaient effectuées dans un pays frontalier 48 heures, voire 24 heures après la capture indélicate de ces données, au grand dam du porteur qui était débité sans jamais avoir quitté son lieu habituel de résidence.

La copie (*skimming* en anglais) de tout ou partie du dispositif piste est très fréquemment utilisée par les fraudeurs. La parade technique consiste à déployer des dispositifs *antiskimming* sur ces terminaux particulièrement vulnérables. Ils consistent essentiellement à modifier la structure physique de certains appareils pour empêcher l'insertion de mécanismes parasites. D'autres techniques, beaucoup plus sophistiquées, sont examinées dans le cadre de travaux de recherche et développement intensifs avec la participation active des banquiers, des industriels et des chercheurs, pour mettre au point des mécanismes de plus en plus sophistiqués de détection d'éventuels intrus dans le système des automates.

***La contrefaçon du support « puce »***

Il s'agit essentiellement d'une fraude appelée *yescard* ou carte qui dit toujours « oui » à la frappe de n'importe

quel code confidentiel. On l'a vu précédemment, pour qu'une opération de paiement se déroule correctement avec une carte à puce, il faut avoir le support requis et disposer du code confidentiel détenu par le seul porteur.

Les fraudeurs ont réussi (provisoirement) à contourner la technologie en copiant, à partir d'une carte volée, la valeur d'authentification de la carte (donnée statique spécifique à chaque carte), et en modifiant le programme de dialogue du terminal avec la carte pour qu'il accepte, sans contrôle effectif, n'importe quelle séquence de chiffres formant un code confidentiel.

Ce type de contrefaçon est limité aux seuls paiements pour lesquels il n'y a pas d'appel vers le centre serveur pour obtenir une autorisation. Dès lors qu'un tel appel s'effectue, la fraude est systématiquement détectée par l'analyse du certificat. Mais les fraudeurs ne s'y trompent pas et limitent leur action dans les magasins ou les zones de commerce où les biens achetés sont d'un montant systématiquement en dessous du seuil d'appel.

Ce type de fraude est donc difficile à détecter, et les parades mises en place par les banques démontrent une extrême capacité de redéploiement des fraudeurs. Ainsi, en début d'année, des actions ciblées dans tel ou tel département en ont stoppé la fraude qui s'est immédiatement reportée sur un autre département.

La véritable parade technologique à ce type de fraude, évaluée en 2000, décidée en 2002, sera rendue opérationnelle en 2005 en France. Elle consiste à rendre la valeur d'authentification « dynamique », c'est-à-dire utilisable une seule fois pour une seule transaction donnée. L'insertion d'un crypto-processeur dans les cartes bancaires CB (actuellement déjà testé avec succès par le Crédit mutuel) constitue donc la réponse technologique adaptée aux contrefaçons par *yescard*.

Mais déjà se dressent à l'horizon de nouvelles techniques redoutables pour casser cette nouvelle sophistication. En effet, la puissance informatique des micro-ordinateurs peut être dopée par des composants incorporant des fonctions logiques programmables. Partiellement à l'état de recherche et développement, de tels mécanismes peuvent représenter des menaces sur les systèmes de cartes, en attaquant les mécanismes de cryptage à clés. Il faut donc être vigilant sur l'émergence de ces nouvelles technologies, prometteuses en elles-mêmes dans des applications courantes, mais qui peuvent être provisoirement dévastatrices dans l'industrie des moyens de paiement par carte à puce faisant largement appel à la cryptologie.

## Le contournement technologique en paiement à distance

L'*underground* de la contrefaçon du paiement à distance est protéiforme. Chaque jour amène une nouvelle technologie, et on se contentera d'une brève typologie, étant précisé que les fraudes reposent essentiellement sur les deux mêmes bases que pour le paiement de proximité : usurpation d'identité et contrefaçon de support.

### Le « phishing »

Les mécanismes d'usurpation d'identité sont réunis dans une technique

appelée *phishing*. Ce mot résulte de la contraction de deux expressions anglaises : *fishing* (la pêche) et *phreaking* qui est une technique de piratage des commutateurs permettant de téléphoner gratuitement.

Cette technique est développée depuis une quinzaine d'années, mais elle a été redécouverte récemment à la faveur de quelques « arnaques » spectaculaires.

De façon pratique, le fraudeur essaie d'obtenir de sa cible des informations sensibles (numéro de carte et code confidentiel, par exemple) en lui demandant de se connecter sur un serveur Web pseudo-protégé, pour vérifier que les données le concernant sont exactes ou n'ont pas été altérées. La plupart des internautes pensent qu'il s'agit effectivement d'une demande authentique émanant de leur banque, complètent le formulaire et délivrent leurs coordonnées à ce faux site bancaire. Quelques clients en France ont pu être victimes récemment de ce genre de cybercriminalité. La seule parade à l'heure actuelle consiste à ne jamais répondre à ce type de mail : d'ores et déjà, plusieurs banques attirent l'attention de leurs clients par une information spéciale affichée lors de la connexion à leurs services en ligne.

Une autre version du *phishing* consiste à s'introduire par Internet dans l'ordinateur de l'internaute et à y déposer un programme pirate appelé *keylogger*. Ce programme capture dans un fichier toutes les interventions faites au clavier par l'internaute et émet discrètement les séquences de caractères ainsi piratées vers le serveur du pirate. Celui-ci doit alors se livrer à un désassemblage des données, mais il est très facile de repérer, par exemple, la connexion vers la banque, d'identifier les caractères du numéro de compte suivis du code confidentiel. Il est aisé alors au pirate de se connecter vers la banque de ce porteur et de procéder à des opérations de virement.

La détection de ce type de programme reste aléatoire. En revanche, les banques offrent rarement un service de virement totalement ouvert et quand bien même ce service serait ouvert, la traçabilité des ordres permettrait d'en retrouver l'auteur. Le risque le plus grand est dans la menace qu'un pirate peut faire peser sur une organisation bancaire, si plusieurs comptes étaient infectés par ce type de virus. On en arrive, avec ce type de comportement, à de véritables actions de cyberterrorisme visant à paralyser, sinon à détruire toute une partie du système bancaire.

De ce point de vue, la protection renforcée des réseaux informatiques bancaires doit devenir un sujet prioritaire de préoccupation des entreprises et des pouvoirs publics : chantages aux virus, bombes logiques, kit de *phishing* accessible sur Internet, et autres chevaux de Troie, constituent autant de menaces potentielles dont disposent les cybercriminels pour extorquer des fonds ou paralyser des systèmes. Les pratiques actuelles sont inquiétantes du point de vue de la sécurité des systèmes bancaires. En France, l'histoire récente d'AZF3, qualifiée parfois de rocambolesque, ne cesse d'intriguer les responsables monétiques : comment obtenir, par le chantage, 1 million d'euros en utilisant 2 000 cartes de crédit ? Inquié-

tant par son ingéniosité, ce type de chantage n'a pas été rendu opérationnel, mais démontre une capacité de créativité pour extorquer des fonds auprès d'une entreprise.

Aux États-Unis, selon le Gartner Group, cette technologie aurait déjà coûté 1,2 milliard de dollars aux banques et aux émetteurs de cartes de crédit. L'augmentation exponentielle de la puissance informatique rend encore plus dangereuses ces attaques cybercriminelles. Conscient de cette évolution, le *Cyber Security Research and Development Act* prévoit une dotation de 900 millions de dollars sur 5 ans pour développer la sécurité informatique et mieux protéger les réseaux contre les pirates.

Les parades face à de telles menaces sont difficiles à envisager : la conception de qualité et la robustesse des réalisations sont probablement les meilleures défenses que l'on peut leur opposer. Les investissements en recherche et développement pour protéger ces réseaux informatiques sont également indispensables pour anticiper ou prévenir les actes malveillants.

**La fraude dans la vente à distance**

Le monde de l'achat à distance est en constante évolution. Des statistiques diverses sont publiées et font état d'une activité en très forte progression. En France, en 2004, le volume financier du commerce électronique se situe aux environs de 10 milliards d'euros. On constate une baisse régulière de la fraude déclarée par les commerçants au moment même où leur chiffre d'affaires est en augmentation sensible. Il faut vraisemblablement en induire que les mécanismes de protection, tant des consommateurs que des e-marchands, s'améliorent année après année. En matière de vente à distance, les fraudeurs agissent principalement dans trois secteurs économiques : les achats de matériel informatique ; l'électronique grand public ; le secteur de la vente de produits et services dans l'industrie du tourisme, sans oublier le secteur téléphonie qui, en pourcentage de sinistres déclarés, demeure en tête même si financièrement, l'impact est de moindre ampleur que dans les autres secteurs recensés.

Sans être préoccupante sur le seul plan financier, la fraude sur Internet reste un problème de fond, car elle inhibe le développement harmonieux de ce type de commerce. L'internaute sait qu'on peut usurper son identité et capturer son numéro de carte. Les opérations de commerce électronique progressent, mais sont freinées faute d'une réelle sécurité pour les internautes, mais aussi pour les commerçants. La véritable solution dans ce domaine reste la mise en place d'un standard international d'identification forte : tout le monde en convient, mais la progression de cette évidence n'atteint pas la vitesse des électrons qui alimentent le Net ! Le Groupement CB, pour sa part, avec Visa et MasterCard, essaie de promouvoir autour du concept *3Dsecure* des solutions progressives de sécurisation sur le Net, qui vont permettre le transfert de responsabilités vers la banque du porteur de la carte. Grâce à une authentification forte, celui-ci sera protégé et la fraude progressivement éradiquée.

## UN ARSENAL LÉGISLATIF ADAPTÉ

Face à la montée de la cybercriminalité, la justice est dotée d'un arsenal législatif adapté.

En général, devant la multiplicité des attaques et la créativité dont font preuve les cyberterroristes, la question se pose volontiers sous la forme : « mais que fait la police ? ». Notre propos n'est pas d'examiner cette question, d'autant plus que la première partie a démontré l'existence d'un corpus législatif conséquent, renforcé récemment par la loi du 9 mars 2004, dite loi Perben II, portant adaptation de la justice aux évolutions de la criminalité, qui donne aux policiers des moyens étendus d'investigation.

De façon concrète, la police effectue un travail approfondi de repérage et d'arrestations. La création de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) en 2002 démontre la volonté des pouvoirs publics de spécialiser un corps de fonctionnaires pour réprimer cette délinquance. Compétent, mobile, intelligent, l'OCLCTIC a fait la preuve de sa grande efficacité contre la délinquance astucieuse en coopérant étroitement avec le Groupement CB dans les affaires de *yescard* et de *skimming*. Que deviennent les auteurs de ces crimes et délits en matière d'utilisations frauduleuses de cartes bancaires, une fois remis à la justice ?

Tel est l'objet de cette analyse totalement inédite qui est livrée ci-dessous, sur la base de données disponibles après application de la loi sur la sécurité quotidienne pendant 3 ans.

### Incriminations pénales

Le travail qui a été fait ne prend en compte que les affaires entre 2002 et 2004 que le Groupement a eu à connaître, par suite d'une plainte contre les auteurs des infractions (cf. annexe).

Dans le cadre ainsi défini, les infractions poursuivies concernent la fraude en matière de cartes de paiement. Six qualifications principales sont retenues (cf. tableau ci-après).

Une affaire récente vient de voir son épilogue en Cour de cassation. La chambre commerciale vient de déclarer non admis le pourvoi formé contre un arrêt de la cour d'appel de Paris du 25 juin 2002, qui consacrait le droit de suspension du Groupement concernant les commerces fraudés ou fraudeurs. La cour d'appel avait, en effet, estimé que le droit de suspension du Groupement, qui avait pour but d'assurer la sécurité du système de paiement par carte bancaire, n'était pas abusif, renforçant ainsi le rôle du Groupement dans la lutte contre la fraude.

Pour les seules affaires où le Groupement est l'une des parties prenantes, 3 ans de pratiques judiciaires démontrent une application très large par les tribunaux des dispositions de l'article 163-4 du Code monétaire et financier, avec une sévérité particulière dans toutes les affaires de *white plastic*. On ne peut pas encore se prononcer sur les affaires de fabrication de *yescard*, car peu de jugements ont été rendus sur ce type de fraude. S'agissant, qu'on le veuille ou non, de fabrication de fausse

**Tableau**
**Six qualifications principales d'incrimination pénale**

| Incrimination | Peine |
|---|---|
| Escroquerie et complicité d'escroquerie (article 313-1 du Code pénal) | 5 ans d'emprisonnement et 375 000 euros d'amende |
| Contrefaçon ou falsification de cartes de paiement ou de retrait (article 163-4 du Code monétaire et financier) | 7 ans et 750 000 euros d'amende |
| Usage d'une carte de paiement ou de retrait contrefaite ou falsifiée | 7 ans et 750 000 euros d'amende |
| Acceptation, en toute connaissance de cause, d'une carte de paiement contrefaite ou falsifiée comme moyen de paiement | 7 ans et 750 000 euros d'amende |
| Mise à disposition de moyens visant à contrefaire ou falsifier des cartes bancaires (article 163-4-1 du Code monétaire et financier) | 7 ans et 750 000 euros d'amende |
| Introduction frauduleuse dans un système de traitement automatisé de données (loi Godfrain, article 323-1 du Code pénal) ayant entraîné la suppression ou la modification de données du système. | 2 ans et 30 000 euros d'amende |

monnaie, même si, pour les cartes de paiement ou de retrait, il ne s'agit pas de crime mais de délit, on n'imagine pas le juge se montrer moins ferme dans une autre branche de la délinquance technologique, fut-elle astucieuse.

La cybercriminalité technologique est une hydre dont on n'a pas fini de couper les têtes. Ce constat quelque peu désabusé traduit une réalité de plus en plus complexe. Il y a quelques années, en effet, on trouvait volontiers des « *hackers* sans reproche », en ce sens qu'ils essayaient d'attaquer un système ou de créer un virus pour se faire connaître ou se lancer des défis. Cette ère est désormais révolue. Le *hacking* est définitivement devenu une affaire de terrorisme, en ce sens qu'il fait planer une menace permanente sur les systèmes financiers : aucun geste, aucune attitude ne sont anodins chez le *hacker* qui recherche désormais, d'une façon ou d'une autre, un retour sur investissement ! Individuel ou collectif, le *hacking* est devenu une forme de cyberterrorisme visant les entreprises les plus importantes, comme l'ont illustré quelques affaires récentes en France.

Au-delà de l'aspect strictement délictuel de telles pratiques, une organisation comme le Groupement CB ne peut que s'inquiéter de la montée en puissance de ces réseaux mafieux, plus ou moins surveillés par les services de renseignements, et dont l'objectif principal est de capturer des fonds pour les recycler et faire prospérer leurs affaires criminelles. Seules les politiques appropriées de sécurité de haut niveau peuvent constituer une réponse à ce type de défi, auquel est régulièrement confrontée l'industrie des moyens de paiement.

# *ANNEXE*

## Bilan succinct des affaires

### Affaires de « white plastic »

Dans cette fraude, les prévenus ont copié des pistes de cartes bancaires sur des points de compromission en capturant, à l'insu des porteurs, leur code confidentiel, selon des procédés plus ou moins sophistiqués.

En 2002 : 6 affaires ont été jugées, 5 ont été qualifiées de contrefaçon ou falsification et usage, et 1 d'escroquerie. Les préjudices sont compris entre 90 euros et 575 000 euros. Les peines prononcées sont très lourdes et s'étagent de 12 mois d'emprisonnement avec sursis à 30 mois d'emprisonnement ferme.

En 2003 : 5 affaires, dont 4, ont été qualifiées de contrefaçon et 1 d'escroquerie. Les peines se situent entre 6 mois d'emprisonnement avec sursis et 4 ans d'emprisonnement ferme.

En 2004 : 11 affaires sont jugées et 1 est en cours d'instance. Sur ces 12 affaires, 1 a été qualifiée d'introduction frauduleuse dans un système de traitement automatisé des données, 8 de contrefaçon ou complicité de contrefaçon et 3 de complicité d'escroquerie ou escroquerie. Sur les 10 affaires jugées, les peines prononcées sont comprises entre 8 mois d'emprisonnement avec sursis et 5 ans d'emprisonnement ferme.

On constate donc que les dispositions du Code monétaire et financier relatives à la contrefaçon/falsification sont majoritairement utilisées par les magistrats, qui se montrent rigoureux dans l'application de la loi. Seuls 4 dossiers sur 23 ont fait l'objet de la qualification d'escroquerie, alors qu'il s'agissait en réalité de contrefaçon/falsification.

### Affaires de « yescard »

Une quarantaine d'affaires d'usage de *yescard* ont été jugées depuis 2002. Dans la plupart des cas, l'incrimination retenue est celle d'usage de cartes contrefaites ou de contrefaçon de cartes de paiement. Les peines prononcées sont majoritairement des peines de prison ferme ; il est vrai que les délinquants sont bien souvent des récidivistes. En revanche, ce qui apparaît de plus en plus fréquemment, c'est l'obligation d'indemniser les victimes, assortie de sursis et d'une mise à l'épreuve. Le juge d'application des peines vérifie que les obligations mises ainsi à la charge du délinquant sont remplies et, dans le cas contraire, la peine d'emprisonnement doit être exécutée.

### Affaires de cartes étrangères contrefaites

Les affaires de contrefaçon de cartes étrangères sont les plus nombreuses, et les tribunaux n'hésitent pas à prononcer des peines d'emprisonnement ferme.

## *ANNEXE (suite)*

### Bilan succinct des affaires

Sur 44 affaires recensées depuis 2002, 30 ont été qualifiées de contrefaçon et/ou d'usage de cartes contrefaites, 17 sont qualifiées d'escroquerie et 3 d'escroquerie avec la circonstance aggravante de bande organisée.

En 2002 : 6 affaires dont les préjudices sont compris entre 3 000 euros et 85 000 euros. Les peines prononcées se situent entre 6 mois d'emprisonnement avec sursis et 4 ans d'emprisonnement ferme.

En 2003 : 17 affaires ont été jugées pour des préjudices allant de 1 900 euros à 50 000 euros. Les peines vont de 3 mois d'emprisonnement avec sursis à 4 ans d'emprisonnement ferme ; plusieurs interdictions du territoire français ont également été prononcées.

En 2004 : 21 affaires ont été jugées pour des préjudices compris entre 2 200 euros et 160 000 euros. Les peines sont comprises entre 3 mois d'emprisonnement avec sursis et 4 ans d'emprisonnement ferme.

### Cas particulier des commerçants

S'agissant de fraude à la carte bancaire, le commerçant peut se trouver directement, ou par l'un de ses préposés, acteur d'une fraude soit en qualité de complice d'une escroquerie, soit en acceptant volontairement des cartes contrefaites ou falsifiées. La complicité d'escroquerie est plus facile à prouver que l'acceptation de cartes contrefaites ou falsifiées, car il s'agit d'une infraction plus générale, plus large, notamment concernant l'intention frauduleuse. L'acceptation de cartes contrefaites ou falsifiées implique, en effet, que le commerçant connaisse la nature exacte des cartes ; ce qui peut être difficile à prouver, ou que la sophistication des fraudeurs en matière de contrefaçon des supports rend plus difficile l'incrimination d'acceptation de supports falsifiés. Sur la période 2002-2004, 9 affaires ont été jugées et 3 sont actuellement en attente de jugement.

Enfin, un commerçant peut être impliqué en tant qu'acteur dans la contrefaçon/falsification de cartes, en participant de manière active à un réseau organisé. Son commerce est alors un point de compromission, c'est-à-dire un lieu où l'on peut capturer les données de la piste et le code confidentiel, qui seront utilisés par la suite pour fabriquer des *white plastic*.

*Note*

1. Par cryptogramme visuel, on entend une série de trois chiffres protégés par un algorithme, destiné à protéger les données de la carte lors de la saisie d'un paiement à distance.

## *Bibliographie*

Conseil de l'Europe, Convention sur la cybercriminalité.

Gasquet (de) M.-A., étude interne de la jurisprudence du GIE Cartes bancaires.

Fia-Net, *La sécurité des transactions commerciales sur Internet,* livre blanc, 4ème édition, mai 2004.

Le Stanc C., *Du hacking considéré comme un des beaux arts et de l'opportun renforcement de sa répression,* chronique, Juris Classeur, avril 2002.

Salmond T., *Phishing : Guidance, Best Practice and Lessons Learnt,* étude interne de l'APACS (UK), mai 2004.