Cybercriminalité et domaine bancaire

MYRIAM QUÉMÉNER*
Magistrat

Aujourd'hui, la cybercriminalité menace les circuits bancaires et financiers. Fraudes, vols d'identité, spams, phishing, cybermenaces se multiplient et deviennent de plus en plus sophistiqués. L'utilisation d'Internet, tant par les banques, les établissements de paiement et de monnaie électronique que par les particuliers facilite aujourd'hui le développement des fraudes et des détournements financiers, en prenant peu de risques. Le canal Internet est particulièrement touché par la fraude, comme le soulignent les statistiques publiées depuis plusieurs années par l'Observatoire de sécurité des cartes de paiement. La lutte contre la fraude mobilise tous les acteurs et constitue une priorité des autorités publiques : les cyberdélinquants, essentiellement motivés par l'appât du gain, peuvent ainsi obtenir des profits plus importants qu'en se livrant au trafic de stupéfiants.

Pour commettre ses méfaits, la criminalité organisée diversifie ses activités délinquantes et utilise de plus en plus les réseaux numériques, compte tenu des avantages qu'ils présentent. C'est dans ce contexte que se développe ce que l'on nomme « cybercriminalité », qui englobe trois catégories d'activités criminelles, à savoir :

– les infractions visant les systèmes d'information et les systèmes de traitement automatisé de données (STAD), comme le déni de service et le piratage ;

– les formes traditionnelles de criminalité, telles que la fraude en ligne, les escroqueries et la contrefaçon ;

– le blanchiment.

Ainsi, la majeure partie des gains financiers criminels se réalise de plus en plus sur les réseaux, au travers de schémas complexes, de systèmes de blanchiment difficiles à démanteler, en profitant notamment de difficultés juridiques entre les États et le manque de moyens de lutte mis en œuvre.

Le crime organisé est en mutation et devient de plus en plus varié, dans ses méthodes et ses structures et dans son impact sur la société. Le « nouveau paysage criminel » est marqué par des groupes plus mobiles et plus flexibles investissant différents territoires et types de criminalité, aidés par un usage illicite d'Internet. Le crime organisé est un *business* de plusieurs milliards d'euros en Europe et il prend encore de l'ampleur. L'expansion des technologies Internet et mobile, la prolifération des itinéraires et des méthodes de trafic illicite ainsi que les possibilités offertes par la crise économique mondiale ont tous contribué à aggraver ce phénomène.

Éléments chiffrés relatifs aux cyberfraudes

Selon le dernier rapport de l'Observatoire de sécurité des cartes de paiement[1], le taux de fraude s'établit pour l'année 2011 à 0,077 %, en légère augmentation pour la quatrième année consécutive, correspondant à un montant total de fraude de 413,2 millions d'euros (contre 0,074 % et 368,9 millions d'euros en 2010). Alors que la fraude à l'international est en léger recul, cette hausse de la fraude s'explique au niveau national par une augmentation de la fraude sur les paiements à distance.

Ainsi, le taux de fraude sur les paiements à distance atteint 0,321 %. On notera en particulier que le taux de fraude sur les paiements sur Internet continue d'augmenter pour s'établir à 0,341 %. L'augmentation est plus modérée pour les paiements à distance effectués par courrier ou par téléphone. L'ensemble des paiements à distance, qui représente 8,4 % de la valeur des transactions nationales, compte ainsi pour 61 % du montant de la fraude. Le montant moyen d'une transaction frauduleuse est également en augmentation, pour s'établir à 130 euros contre 122 euros en 2010. Les secteurs voyage-transport, commerce généraliste et semi-généraliste, services aux particuliers et téléphonie et communication représentent 70 % du montant de la fraude sur Internet, apparaissant ainsi comme les plus exposés. La comparaison des taux moyens de chacun des secteurs d'activité complète cette information et permet de constater que certains secteurs, qui comptent pour une faible part du total de la fraude, subissent toutefois une exposition élevée ; c'est le cas des produits techniques et culturels, de l'équipement de la maison, de l'ameublement et du bricolage. On note également que le taux de fraude sur le secteur des jeux en ligne a fortement baissé en 2011 à 0,303 % (contre 0,478 % en

*Myriam Quéméner a écrit *Établissements financiers et cyberfraudes*, collection « Les essentiels de la banque et de la finance », RB Édition.

1. http://www.banque-france.fr/observatoire/index.htm.

2010 et 0,740 % en 2009), et qu'il se situe désormais en dessous du taux moyen de fraude tous secteurs confondus. Cette tendance s'explique par un déploiement progressif des dispositifs d'authentification non rejouable du porteur par les sites de jeux en ligne, conformément aux recommandations de l'Observatoire et aux actions complémentaires de sensibilisation de l'Autorité de régulation des jeux en ligne.

Actualités et cybercriminalité financière

Quotidiennement, les médias révèlent des affaires de vols de données bancaires, d'usurpation d'identité et d'escroqueries commises à l'occasion de transactions bancaires.

Par exemple, une vague de cyberattaques visant des banques américaines, européennes et latino-américaines a permis à ses auteurs de récolter près de 80 millions de dollars, selon une étude publiée mardi 26 juin par deux sociétés spécialisées dans la cybersécurité [2].

Selon cette étude de Guardian Analytics et McAfee, les auteurs de l'« Opération flambeur » ont cherché à dérober à 60 banques dans le monde entre 75 millions et 2,5 milliards de dollars.

Le réseau a utilisé des techniques « sophistiquées » et visé des comptes en banque très fournis en Europe, avant de migrer vers l'Amérique latine puis les États-Unis, soulignent les sociétés, qui donnent un aperçu rare des cyberattaques pouvant viser les établissements financiers. Plus de 36 millions d'euros ont été volés sur 30 000 comptes bancaires appartenant à des entreprises ou des individus en Europe, a dévoilé le spécialiste de la sécurité Check Point. Un *botnet* a servi à mener une attaque sophistiquée. Des criminels auraient mis en place un réseau de machines zombies grâce à un *malware* (le trojan Zeus) qui aurait infecté des PC et des appareils mobiles sous Android et BlackBerry. La méthode s'est faite en deux temps : infection du PC, puis infection du téléphone. Cela a ensuite permis aux pirates d'intercepter les SMS de la procédure d'identification sur les comptes bancaires en ligne.

Les banques visées sont majoritairement en Italie (50 %), mais l'Allemagne, les Pays-Bas et l'Espagne ont également été touchés. Quant aux utilisateurs, ils sont 39 % à être originaires d'Italie, 38 % d'Espagne et 20 % d'Allemagne.

Autre affaire d'importance, une banque britannique a reconnu en octobre 2012 que des cyberattaques de « *grande envergure* » avaient perturbé ses services en ligne dans le monde entier sans toutefois affecter les données privées de ses clients. La banque a fait état « *d'attaques par déni de service de grande envergure* ». Ces attaques « *n'ont affecté aucune donnée clientèle, mais ont empêché les clients d'utiliser les services en ligne de HSBC, y compris les services bancaires* ». HSBC n'a pas avancé d'hypothèses quant à l'origine de ces attaques, mais la banque est dans le collimateur du mouvement anticapitaliste Occupy. Elle est par ailleurs soupçonnée par la justice américaine d'être mêlée au blanchiment d'argent sale pour des cartels de drogue mexicains et d'avoir transféré de l'argent via sa filiale aux États-Unis pour des régimes auxquels Washington a imposé des sanctions comme l'Iran, le Soudan et la Corée du Nord. L'Observatoire national de la délinquance et des réponses pénales a fait appel au Club de la sécurité de l'information français (Clusif[3]) pour dresser un bilan de la cybercriminalité et présenter les tendances en la matière et plus précisément à un membre de l'entreprise McAfee[4], groupe *leader* dans la sécurité informatique, ce qui montre que le secteur privé s'est parfaitement investi dans ce domaine qui est aussi un marché, un *business*. Ce panorama souligne les dernières tendances en matière de cybercriminalité, avec une hausse des attaques par déni de service, des *malwares*[5] sur les mobiles et des vols de données bancaires.

Il souligne des orientations préoccupantes, comme l'apparition à la place des forums de véritables boutiques en ligne où l'on peut faire son choix selon différents critères tels que la banque, la localisation ou la nationalité de la victime. Le trafic de cartes se transforme en cybercriminalité de masse et plusieurs dizaines de milliers de cartes bancaires d'origine française ont ainsi été repérées.

Techniques cybercriminelles

Il suffit souvent aux cybercriminels de trouver l'identifiant d'un compte en ligne et, s'ils arrivent à pénétrer dans le système même d'un gérant de *cloud*, ils ont directement accès à des grands volumes de mots de passe ou de cartes de crédit, par exemple. Sony en a fait l'année dernière la triste expérience, avec plus de 24 millions de comptes clients piratés. Pour obtenir des informations personnelles sur les utilisateurs, les cyberdélinquants ont mis au point différentes techniques, qui vont des logiciels espions aux attaques par « hameçonnage ». L'objectif est ainsi d'amener les victimes à révéler des informations personnelles ou confidentielles On distingue plusieurs types d'attaques par hameçonnage, parmi lesquels le hameçonnage par courriel, qui comprend trois grandes phases :

– au cours de la première phase, les cyberdélinquants identifient des sociétés légitimes qui proposent à leurs clients – les cibles potentielles – des services en ligne et communiquent avec eux par voie électronique. Il s'agit par exemple d'établissements financiers ;

– ils créent ensuite des sites Internet qui ressemblent aux sites de ces sociétés. Ces « sites d'espionnage » demandent aux victimes de s'identifier de manière classique et collectent, ce faisant, des informations personnelles sur les clients (numéros de compte, mots de passe pour les opérations bancaires en ligne, etc. [6]) ;

2. http://www. lemonde. fr/technologies/article/2012/06/26/80-millions-de-dollars-detournes-dans-une-cyberattaque-visant-des-banques_1724984_651865. html.

3. Ce club professionnel, constitué en association indépendante et ouvert à toute entreprise ou collectivité, accueille des utilisateurs et des offreurs issus de tous les secteurs d'activité. Sa finalité est d'agir pour la sécurité de l'information, facteur de pérennité des entreprises et des collectivités publiques. Il entend sensibiliser tous les acteurs en intégrant une dimension transversale dans ses groupes de réflexion *management* des risques, droit, intelligence économique… Des groupes de travail se réunissent régulièrement pour traiter de thématiques en fonction de l'actualité et des besoins des membres. Le Clusif a des relais régionaux (Clusir) et des partenaires européens (Clusi).

4. François Paget, expert en sécurité IT chez McAfee.

5. Logiciel espion.

6. M. Quéméner, J.-P. Pinte, *Cybersécurité des acteurs économiques : réponses stratégiques et juridiques*, Hermes Lavoisier, 2012.

– pour les orienter vers ces sites d'espionnage, les cyberdélinquants envoient aux internautes des courriels qui ressemblent à ceux normalement émis par les sociétés dont ces derniers sont clients, commettant souvent par là même une violation de la marque commerciale.

L'automatisation de l'envoi de *spams* par le biais de *botnets*, ordinateurs dont le contrôle est pris à distance, la possibilité d'agir à distance et la garantie d'un relatif anonymat sont autant d'atouts que les cyberdélinquants ont parfaitement compris et intégrés dans leurs méthodes, incluant désormais l'appropriation de techniques et de technologies avancées. Désormais, il existe des liens étroits entre la criminalité classique et la criminalité informatique et les cybercriminels font de plus en plus partie de réseaux internationaux très organisés.

Les criminels n'ont pas besoin, comme les premiers auteurs de virus, d'être experts en informatique : on trouve en vente libre les logiciels espions les plus élaborés. On trouve aussi les données collectées par ces logiciels espions : informations bancaires et informations personnelles suffisantes pour acheter en ligne ou transférer des fonds.

Ensuite, la panoplie des arnaques aux particuliers évolue peu : de la promesse d'un investissement très rentable ou d'un transfert de fonds d'un compte bloqué en Afrique, en passant par la fraude aux enchères, la non-expédition du produit payé ou l'exploitation d'un numéro de compte collecté par ce procédé frauduleux. Le plus surprenant, c'est que ces arnaques continuent à faire des victimes, avec un taux de succès assez constant, alors que le nombre de tentatives explose, doublant même tous les quatre mois dans le cas du *phishing*.

Les réseaux numériques démultiplient le nombre des infractions et les délinquants se jouent des frontières en commettant leurs délits dans des pays où la législation est inexistante ou embryonnaire, ce qui aboutit à la création de « cyberparadis ». En effet, l'une des difficultés rencontrées dans la lutte contre la cybercriminalité est que cette forme de délinquance mondiale défie les règles classiques de compétence territoriale fondées sur la souveraineté des États, devenant ainsi un défi pour la coopération internationale.

Cette révolution numérique peut nuire non seulement aux droits et à la sécurité des individus, mais aussi, en visant les entreprises et même les États, à l'économie.

Outre les aspects d'extranéité que l'on trouve souvent dans les procédures liées à la cybercriminalité, des éléments techniques relatifs aux technologies numériques peuvent complexifier les enquêtes visant à démanteler les réseaux ; le secteur des nouvelles technologies de l'information et de la communication a été identifié comme un secteur à fort risque de blanchiment d'argent.

Grâce à la rapidité et à la souplesse d'exécution des transactions financières offertes par Internet, la cybercriminalité a su effectivement détourner le fonctionnement des systèmes informatiques pour l'utiliser comme vecteur dans l'exécution d'une activité illégale.

Aujourd'hui, les activités criminelles proviennent souvent des pays émergents rencontrant des difficultés économiques comme l'Afrique de l'Ouest, les pays andins comme le Brésil, la Bolivie. Par ailleurs la Chine, l'Inde mais aussi la fédération de Russie et les pays de l'ancien bloc soviétique, où Internet se développe de plus en plus sans que soit mis en place des lois ou des régulations quant à son usage, sont des pays où fleurit la cybercriminalité. Les pirates informatiques s'attaquent essentiellement aux entreprises et institutions financières, car s'ils parviennent à accéder à leur base de données, ils ont alors la mainmise sur l'ensemble des données des individus de toute une structure économique, ce qui peut représenter des centaines de personnes.

Techniques des cyberdélinquants

Pour obtenir des informations personnelles sur les utilisateurs, les cyberdélinquants[7] ont mis au point différentes techniques, qui vont des logiciels espions aux attaques par « hameçonnage » sollicitant les victimes pour qu'elles révèlent des informations personnelles ou confidentielles. On distingue plusieurs attaques de ce type. Par le biais d'un courriel, les cyberdélinquants identifient des sociétés légitimes qui proposent à leurs clients – les cibles potentielles – des services en ligne et communiquent avec eux par voie électronique. Il s'agit par exemple d'établissements financiers. Ils créent ensuite des sites Internet qui ressemblent aux sites de ces sociétés. Ces « sites d'espionnage » demandent aux victimes de s'identifier de manière classique et collectent, ce faisant, des informations personnelles sur les clients (numéros de compte, mots de passe pour les opérations bancaires en ligne, etc.).

La méthode du *carding* permet de créer des cartes virtuelles et il existe des sites de *carding* : on peut y acheter ou vendre des accès à des comptes bancaires, des numéros de cartes volés, des copies de pistes magnétiques et des profils personnels complets. Selon ses compétences, le *carder* (trafiquant de cartes bancaires) peut mettre à jour des algorithmes bancaires, procéder à la copie des données informatiques de cartes (du support magnétique ou de la puce) sur des supports vierges ou encore organiser des attaques virtuelles visant à dérober des identifiants bancaires (*phishing* ou *pharming* de cartes). Le *carding* est donc une fraude aux cartes bleues.

La méthode du *skimming* est une opération frauduleuse qui consiste faire des copies magnétiques des cartes bancaires à l'aide d'un lecteur mémoire (appelé *skimmer*). Le code confidentiel peut être capté à l'aide d'une micro-caméra. Les données ainsi acquises sont par la suite inscrites, soit sur les pistes magnétiques d'une carte contrefaite pour être utilisées dans des commerces non complices ou pour des retraits de numéraires dans les DAB, soit sur des cartes dites « *white plastic* » (cartes blanches avec bande magnétique) utilisées dans des commerces complices. Si ces méthodes sont plus complexes que l'usurpation d'identité et si des qualités informatiques sont requises, elles peuvent être décelées : les *skimmers* peuvent être identifiés et les sites de *carding* débusqués et fermés.

Les tentatives de *phishing* et le *spam* ciblant les réseaux

7. M. Quéméner, *Établissements financiers et cyberfraudes*, Revue Banque Édition, mai 2011.

sociaux ont tendance à augmenter. Les chevaux de Troie et les logiciels espions sont deux des principaux outils qu'un cybercriminel utilise pour obtenir des accès non autorisés et dérober des informations d'une victime dans le cadre d'une attaque, en s'installant à l'insu des utilisateurs dans leur ordinateur.

Répression de la cybercriminalité financière

De nombreuses qualifications pénales permettent de réprimer les actes à la cybercriminalité financière et bancaire. Les systèmes de traitement automatisé de données se trouvent aujourd'hui au centre d'un contentieux important, qui ne cesse de s'accroître en raison du développement que prend la communication par Internet. Les systèmes de traitement automatisé de données sont tantôt les moyens de commettre une infraction comme par exemple, des fraudes aux cartes bancaires, contrefaçon, tantôt les objets d'une infraction. Dans cette dernière hypothèse, c'est le système informatique lui-même qui est victime d'atteintes frauduleuses ou illicites. On parle généralement de fraudes informatiques pour désigner les actes frauduleux visant les systèmes.

La loi n° 88-19, 5 janv. 1988 relative à la fraude informatique dite « Loi Godfrain » incrimine de façon autonome, et indépendamment de toute référence au commencement d'exécution de la tentative des simples actes préparatoires que constitue la participation à un groupe formé ou à une entente établie en vue de commettre des fraudes informatiques (C. pén., art. 323-4). La loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004 est venue ajouter l'importation, la détention, l'offre, la cession ou la mise à disposition d'un équipement d'atteinte aux systèmes de traitement automatisé des données (C. pén., art. 323-3-1). Les articles 323-1 à 323-4 du Code pénal prévoient un ensemble divers d'atteintes pouvant être portées à un système de traitement automatisé de données, que le législateur a présenté « *par degrés de gravité croissante* ».

Il convient de noter que de nombreuses procédures aboutissant à des interpellations au plan national aboutissent. Les délinquants achètent sur des forums Internet dédiés à ce genre de fraude, des numéros de cartes bancaires pour faire des achats sur Internet, ou des pistes magnétiques (ou *dumps*) capturées illégalement et utilisées pour effectuer des retraits aux distributeurs de billets. Elles sont soupçonnées aussi d'avoir revendu les numéros de cartes bancaires sur Internet et acheté des *dumps* pour fabriquer, pour leur utilisation propre ou celle de complices, de fausses cartes qu'elles encodaient elles-mêmes. Le nombre de cartes piratées dépasserait largement 10 000, réparties sur plusieurs pays[8].

Mesure de prévention

Face à ces fraudes, les banques et les sites marchands ont commencé à mettre en place des moyens de protection, notamment l'envoi au détenteur de la carte d'un texto contenant un code permettant de valider la transaction. L'Observatoire de sécurité des cartes de paiement, dans son dernier rapport, insiste pour que ses recommandations relatives à l'adoption de dispositifs permettant l'authentification non rejouable du porteur de la carte, tels que « 3D-Secure », soient mises en œuvre par les e-commerçants, notamment les plus grands d'entre eux, pour les paiements les plus risqués.

L'Observatoire préconise l'adoption par les sites marchands de dispositifs permettant l'authentification non rejouable du porteur de la carte (tels que 3D-Secure) pour les paiements les plus risqués. Des sites transactionnels – comme voyages-sncf.com ou airfrance.com – jouent un rôle important dans sa généralisation. Développé par Visa et MasterCard et commercialisé par les grandes banques françaises, le dispositif 3-D Secure permet aux exploitants de sites de commerce électronique de limiter les risques de fraude sur Internet, liés aux tentatives d'usurpation d'identité. Malgré une amélioration de l'efficacité des dispositifs de sécurisation des opérations de paiement par carte sur Internet en 2011, l'Observatoire regrette que seulement 23 % des transactions de paiement sur Internet soient à ce jour sécurisées par des dispositifs d'authentification non rejouables via 3D-Secure.

Il s'agit d'une préconisation nationale qui pourrait se transformer en objectif européen afin de favoriser l'émergence d'un réel marché unique du numérique. En revanche, l'Observatoire de la sécurité des cartes de paiement prend du recul vis-à-vis des *smartphones* comme outil transactionnel : « *Étant par essence multi-applicatifs, multitâches et dépourvus à ce jour d'éléments de sécurité, ils sont peu adaptés aux requis habituellement exigés en France sur les terminaux de paiement traditionnels dédiés à cette fonction.* »

Le paiement sans contact via les *smartphones* étant développé par l'industrie, il est nécessaire d'expertiser les réelles conditions de fiabilité : « *Il faudrait garantir un niveau de sécurité équivalent à celui prévalant pour les terminaux de paiement traditionnels.* » Même réserve exprimée vis-à-vis des solutions de portefeuilles électroniques qui émergent (comme Google *Wallet*). Il s'agit d'offres alternatives « qui *ne doivent pas se faire au détriment de la sécurité de la carte de paiement* ». L'Observatoire multiplie les recommandations : protection des données sensibles (dont celles liées aux cartes de paiement), mise en œuvre d'une authentification non rejouable à la 3D-Secure du porteur au moment de l'enregistrement de la carte dans le portefeuille ainsi que pour les opérations de paiement par carte les plus risquées, mise en place de règles claires quant au partage des responsabilités (utilisateurs, marchands, gestionnaires de *wallets*).

8. http://www. leparisien. fr/faits-divers/piratage-de-cartes-bancaires-22-interpellations-en-france-05-02-2013-2541527.php.

Une nécessaire adaptation des stratégies de lutte

Le caractère transnational et de plus en plus structuré de certaines formes de délinquance, l'opacité des modes d'action ainsi que l'extrême sophistication des nouvelles formes de criminalité, la mise en jeu d'intérêts économiques et démocratiques importants, ou simplement l'application d'un droit technique et évolutif, imposent l'adaptation du système répressif, et notamment son adaptation organique.

Le développement des politiques de sécurité

Avec l'explosion des activités en ligne, il est devenu urgent pour les banques de moderniser leurs outils de sécurité informatique. La lutte contre les cyberfraudes nécessite la mise en œuvre d'outils complémentaires, permettant notamment de détecter les paiements risqués afin de les sécuriser au moyen d'une authentification renforcée. Ces moyens d'authentification renforcée doivent dorénavant être généralisés pour faire reculer la fraude sur les paiements par carte sur Internet. Ils doivent également être adaptés aux évolutions technologiques et aux modes de consommation, notamment en ce qui concerne le recours croissant au téléphone mobile pour commander et payer sur Internet.

À ce titre, les portefeuilles électroniques peuvent faire partie des réponses adaptées pour sécuriser les paiements sur ce canal. Pour autant, l'Observatoire invite les professionnels à poursuivre leurs efforts afin de proposer des dispositifs assurant l'authentification renforcée sur l'ensemble des canaux de distribution. L'une des solutions consiste à authentifier de manière renforcée le porteur de la carte, particulièrement pour les transactions les plus risquées, comme le permet par exemple 3D-Secure, le mécanisme le plus répandu aujourd'hui en France et à l'étranger. D'autres solutions, comme les portefeuilles électroniques peuvent contribuer à renforcer l'authentification du porteur sur les nouveaux canaux de paiement (notamment le canal mobile…). 3D-Secure est un dispositif permettant d'authentifier le porteur d'une carte de paiement de manière renforcée à l'occasion, par exemple, d'un achat sur Internet. L'acheteur doit saisir un code d'authentification à usage unique, reçu le plus souvent par SMS, pour valider le paiement de ses achats.

Le 1er février 2013, la Banque Centrale Européenne [9] a publié un ensemble de recommandations concernant la sécurité des paiements sur Internet. Les principales préconisations concernent l'initiation des paiements, l'accès aux données sensibles, la limitation du nombre de tentatives de connexion, la création de mécanismes de surveillance des transactions, la mise en place de niveaux de sécurité multiples ainsi que des dispositifs d'alerte des clients. Ces recommandations constituent la première réalisation du Forum européen sur la sécurité des moyens de paiement de détail.

L'organisation accrue de la lutte contre la cybercriminalité

Par ailleurs, la Commission européenne a été à l'origine de la création du Centre européen de lutte contre la cybercriminalité pour contribuer à la protection des entreprises et des citoyens européens contre ces menaces informatiques grandissantes. Le centre est établi au cœur de l'Office européen de police, Europol, à La Haye (Pays-Bas). L'EC3 [10] va se concentrer sur les activités illicites en ligne menées par des organisations criminelles, notamment les attaques dirigées contre les services de banque en ligne ou d'autres activités financières en ligne et la criminalité touchant aux infrastructures critiques et aux systèmes d'information de l'UE. Il constitue le point focal européen dans la lutte contre la cybercriminalité et se concentrera sur les activités illicites en ligne menées par des groupes criminels organisés, et plus particulièrement sur celles qui génèrent des profits considérables, comme la fraude en ligne impliquant le vol des détails de comptes bancaires et de cartes de crédit.

Internationalisation des outils législatifs

La cybercriminalité, par essence mondiale, impose des réponses européennes et internationales. La convention de Budapest élaborée par le Conseil de l'Europe demeure aujourd'hui le seul traité en matière de lutte contre la cybercriminalité et a le mérite de proposer un cadre juridique commun afin de lutter contre ce phénomène. Adoptée par une trentaine de pays à ce jour, elle a également un protocole additionnel relatif au racisme et à la xénophobie. Par ailleurs, l'ONU aurait le projet de créer une convention universelle, certains pays estimant que la Convention de Budapest n'a pas qu'une vocation régionale et s'opposant notamment à son article 32 qui prévoit la possibilité de poursuivre des investigations initiées dans un pays donné à l'étranger, ce que certains États assimilent à de l'ingérence contraire à la souveraineté des pays.

La réponse de l'Union européenne dans la lutte contre le crime organisé s'adapte à la complexité de cette délinquance en réseaux et vise aussi bien la criminalité financière, le blanchiment d'argent que les nouvelles formes de la criminalité organisée comme la cybercriminalité. L'approche intégrée qui guide l'Union européenne s'étend de la prévention à la répression et repose sur une coopération efficace entre les services répressifs des États intégrant notamment l'échange d'informations et l'entraide en matière de saisies et de confiscations, la lutte contre la criminalité organisée étant globale. ■

9. http://www.banque-france.fr.

10. Dépêches Juris-Classeur, 16 janvier 2013, 2553. Inauguration du Centre européen de lutte contre la cybercriminalité (EC3).