

Internet, fraudes et corruptions

Noël PONS



© Gettyimages

Internet a ouvert le monde à la criminalité. Camouflée derrière le paravent de la liberté sans contrôle, elle peut aisément développer des escroqueries, créer un marché efficace pour la contrefaçon et corrompre le sport grâce aux paris manipulés.

Internet, fraud and Corruption

The internet has been opened up to the world of crime. Camouflaged behind the shield of freedom without controls, criminals have easily developed their scams, created an effective market for counterfeiting and corrupted sports with manipulated gaming



Noël Pons

Il est conseiller au Service central de prévention de la corruption (SCPC), auditeur interne certifié (CIA), inspecteur des Impôts. Il a publié plusieurs ouvrages dont, en 2006, *Cols blancs et mains sales-Economie criminelle, mode d'emploi* aux éditions Odile Jacob ; en 2004, il a coécrit avec François Vidaux, *Audit et fraudes*, paru aux éditions IFACI. Il est aussi l'auteur de plusieurs articles relatifs aux fraudes, à la corruption et au blanchiment, en particulier dans la rubrique « fraudes » de *La revue française de l'audit interne*.

Le grand banditisme a saisi l'opportunité de l'économie virtuelle offerte par l'Internet. Ce dernier a créé des débouchés nouveaux, inespérés, difficilement contrôlables, ainsi qu'une assise fiable pour les montages anciens. La criminalité a trouvé là un univers à sa mesure pour implanter et donner un essor nouveau à ses manipulations. C'est, pour elle, une nouvelle conquête de l'Ouest !

Avec Internet, on entre de plain-pied dans la mondialisation : tout peut être exécuté, depuis n'importe où, par n'importe qui. Certains sites permettent même un camouflage quasi parfait car ils ne gardent pas les données de leurs utilisateurs ; d'autres se refusent à répondre à tout droit de communication en jouant à « saute-paradis » fiscaux. Même si des poursuites sont diligentées par des structures d'État, elles mettent nécessairement du temps à atteindre leur but, l'essentiel est alors sauvé : les fonds ont disparu depuis longtemps

L'intérêt criminel pour Internet a existé dès l'origine. La première grande escroquerie connue aurait été le fait de mafiosi new-yorkais. En effet, ces derniers ont créé des sites pornographiques accessibles en payant une modique cotisation par carte de crédit. En revanche, une fois les codes des cartes récupérés, des milliers de prélèvements illégaux ont été effectués sur ces cartes, les personnes escroquées hésitant à porter plainte car, à l'époque, surfer sur de tels sites était honteux. Nous en sommes bien loin maintenant.

L'absence d'établissement stable, physiquement identifiable rend la commission d'infractions plus facile. Utiliser des sociétés écrans, de fausses identités, de fausses qualités est chose aisée, surtout sur la toile. La saisie des actifs est difficile, voire impossible en cas de condamnation, ce qui pérennise le montage frauduleux. De plus, dans le cas où une investigation serait couronnée de succès après la collaboration maximale des divers pays engagés, le nombre d'opérations frauduleuses qui ne peuvent être sanctionnées rend la peine peu dissuasive. Comme pour le blanchiment ou le trafic de drogues, la criminalité « embourbe » les contrôles. L'effet masse dont il joue rend la sanction acceptable, voire lui permet de lancer des leurres.

Internet et les manipulations

Les montages les plus développés sont constitués par des montages anciens adaptés au support. Il s'agit essentiellement :

- Opérations classiques telles que des extorsions de fonds contre des sociétés. La méthode est celle du « déni de

service » : les sociétés qui ne payent pas voient leurs serveurs bloqués par la multiplication de requêtes, et ne peuvent plus travailler. Les cibles sont diverses : les casinos internet et les sociétés de paris mais aussi des sociétés commerciales plus classiques.

- Des blocages de comptes clients ou fournisseurs par des encodages frauduleux. Une rémunération est demandée pour débloquer les comptes.
- De l'utilisation de contrefaçons de jeux dans des sites nouvellement créés et liquidés dans la journée permettant de récupérer les mises sans payer les paris.
- Des opérations de « Phishing » et leur corollaire le « cuckoo smurfing » (coucou), qui est une stratégie d'utilisation des comptes personnels de particuliers pour transférer des fonds.

Pour bien montrer l'implication criminelle de cette manipulation, dans l'un des cas identifiés, il s'agissait de transférer des fonds obtenus par la revente de drogue et par des escroqueries bancaires vers un pays de l'Est. Les fonds étaient regroupés dans une banque de l'hémisphère sud, éclatés entre une multitude de comptes particuliers, ils atteignaient ainsi le pays de destination. Une fois sur place, des étudiants locaux, chichement rémunérés, se servaient d'une entreprise de transfert de fonds pour les transmettre à leurs bénéficiaires. Donc, le blanchiment d'un montage relativement simple mettait en place trois méthodologies complexes différentes.

- Les données qui peuvent aussi être revendues à d'autres criminels, ainsi qu'à des gestionnaires de sites pornographiques. On connaît les liens entre la pornographie en général et la criminalité. Entrer dans un site de jeu, par curiosité ou pour jouer, peut conduire le jour suivant à trouver sa boîte inondée de spams à caractère pornographique et inversement. Il existe des liens déjà anciens entre ce type de sites, les sites de jeux et de paris et les activités criminelles.
- La distribution de sommes à des joueurs complices favorisée par l'absence de traçage, d'archivage des connexions et des mouvements financiers (fraude et blanchiment).
- Le camouflage de l'origine des sommes investies par le joueur. L'argent peut provenir d'un pays non coopératif, même si les mises proviennent d'un compte bancaire supportant une carte de paiement, rien ne dit que le joueur est le vrai propriétaire ou qu'il a gagné légitimement ces fonds. Ces derniers peuvent provenir d'une opération intermédiaire dans le processus de blanchiment. Les fonds illégaux (en espèces) sont en partie blanchis et sont investis sur place. Le Groupe d'action financière (GAFI), déjà, dans son rapport de 2001, avait souligné le risque de blanchiment lié à l'exploitation de casinos en ligne.

Internet et la contrefaçon

Le support de la vente sur Internet a permis aux criminels d'industrialiser, tout en la facilitant, la distribution des produits contrefaits. Ils utilisent leurs propres sites de vente directe, aussitôt disparus aussitôt reconstitués, dès qu'un risque se profile. Ils peuvent aussi se servir des sites d'enchères pour distribuer des produits sans attirer l'attention, eu égard à l'immensité du marché et au caractère individuel des échanges.

En effet, la structure très souple de certaines organisations articulées autour d'échanges rapides, peu ou pas contrôlés, entre clients et fournisseurs autorise toutes les dérives, qu'il s'agisse de contrefaçon ou de commerce clandestin. La plupart des sites de vente en ligne ont accepté le principe de précaution et effectuent désormais des contrôles en amont sur la qualité des articles mis en vente ainsi que sur l'identité des vendeurs. L'un d'entre eux, pourtant, se refuse à se soumettre aux condamnations essuyées sur ce point. Une telle structure, si elle n'effectue pas les contrôles *a minima*, constitue l'un des plus beaux supports de fraudes, de contrefaçon et de blanchiment en ne pratiquant pas les démarches préventives nécessaires ou en refusant de transmettre les informations demandées par les services de contrôle.

La criminalité maîtrise depuis l'origine, et fort bien, le développement du marché de la contrefaçon qui suppose des structures logistiques importantes, des investissements considérables et une organisation à la fois rigide – quasi militaire – et très flexible, car la réactivité, la capacité d'adaptation, la souplesse d'utilisation sont devenues des caractéristiques essentielles de la grande criminalité. Si le besoin de financement est considérable – mais la criminalité n'en manque pas – le retour sur investissement est à la hauteur de la mise. L'Internet lui donne l'opportunité de distribuer ses produits presque sans risque, lui offre un stade de blanchiment lucratif et peu contrôlé, parce que difficilement contrôlable, en raison de l'éclatement des opérations entre différents pays et de multiples structures, si le site n'est pas coopératif.

Internet et les corruptions

Les montages antiques de corruption dans les jeux et les paris ont été transposés sur Internet. Ceci est confirmé par une augmentation des mises dans des pays improbables sur des compétitions atypiques comme sur des événements connus. Corrélativement, une multiplication de cas de corruption dans les sports riches est

constatée. En effet, toutes les manifestations sportives, sans exception, ont fait l'objet de tentatives ou de corruptions. Le principe utilisé est assez simple, il combine les manipulations physiques et celles qui relèvent de l'Internet. Pour corrompre dans le milieu sportif, il est nécessaire de disposer d'un support – un club, un site de bookmakers – et de corrompre des joueurs. Cela ne pose pas de problème puisque les fonds ne manquent jamais et la menace physique est toujours présente. Une fois propriétaire d'une structure ou installé dans un tel cadre, il est aisé de convaincre diverses mafias de s'impliquer sur ces paris. Lorsqu'elles n'ont pas elles-mêmes organisé les montages, elles se laissent facilement persuader. Des paris « gagnant/gagnant » sont ainsi organisés depuis le lieu dans lequel leurs fonds sont stockés, et portent sur des compétitions se tenant dans n'importe quelle autre région du monde, la distance ne joue pas.

Ainsi, au cours des trois dernières années, on a pu assister à des mises importantes depuis un pays asiatique vers une équipe de troisième division belge, aux paris de gros « investisseurs », depuis Hong Kong ou depuis l'Australie, sur des compétitions africaines. On a vu ainsi se déclencher une véritable bourrasque de paris sur le tennis qui n'ont été limités que par la mise en place de procédures très contrôlées dans les plus grands tournois.

Une information récente (12 mars 2008), parue sur le site *webdopoker*, évoque une attaque externe effectuée par des hackers d'un joueur régulier. Les sommes porteraient sur des milliers d'euros. « *Un joueur a commencé à perdre régulièrement, sauf lorsque sa main était très bonne (paire d'as). Cependant, dans ce cas, les autres joueurs foldaient systématiquement. S'il bluffait, il était systématiquement démasqué. Les ingénieurs qui ont analysé le cas se sont aperçus que le joueur avait reçu d'un autre compétiteur un logiciel de calcul de probabilité qui contenait un Troyen. Ainsi, chaque fois que la cible jouait au poker, son opposant recevait sur son écran la main de son adversaire.* » Le « hacking » se met donc au service des fraudeurs.

Il faut cependant noter que la connaissance de ces manipulations est possible grâce à Internet et à la masse documentaire informatisée qu'il génère. Ce sont les sites de paris honnêtes qui, les premiers, ont identifié les atypismes dans les mises à partir d'analyses fines des informations figurant dans les fichiers. Ainsi, tel Janus aux deux visages, Internet peut être la pire des choses si on laisse faire, et un très bon moyen de contrôle si on utilise la documentation que chacune de ses opérations génère en respectant évidemment les libertés individuelles et les procédures légales.

Noël PONS