Collection des
rapports officiels

Rapport au ministre du Budget, des Comptes publics et de la Fonction publique

Jeux en ligne et menaces criminelles

ALAIN BAUER

La documentation Française

Collection des rapports officiels

Rapport au ministre du Budget, des Comptes publics et de la Fonction publique

Jeux en ligne et menaces criminelles

Alain Bauer

Rapports officiels

Rapport au ministre du Budget, des Comptes publics et de la Fonction publique

ISBN 978-2-11-007904-6
ISSN 0981-3764
DF : 5R019240
www.ladocumentationfrancaise.fr
Paris, 2009

Photos de couverture :
Premier ministre
service de la photographie
Diffuseur :
La Documentation française
Sculpteur : Marielle Polska
et photo goodshoot

Sommaire

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

LE MINISTRE

PARIS, LE 25 FEV 2008

Nos réf. : 2008-015HM

Monsieur le Président, cher ami,

Lors de nos récents entretiens, vous m'avez fait part des travaux que vous conduisez au sein du département de recherches de l'Institut de Criminologie de l'Université de Paris II sur les menaces criminelles contemporaines et notamment les réflexions que vous avez engagées sur la criminalisation de la société civile européenne par le biais des jeux d'argent.

Comme vous le savez, les autorités françaises ont engagé à l'automne 2007 une réflexion sur la réorganisation globale du secteur des jeux et la modernisation de leur régime juridique et fiscal.

Sans renoncer aux principes généraux qui ont présidé jusqu'à ce jour à la politique des jeux en France, il s'agit de définir les modalités selon lesquelles, il pourrait être procédé aux adaptations requises par le développement rapide du marché, non régulé à ce jour, des jeux en ligne.

La nature spécifique de ces activités rend en effet nécessaire de se doter rapidement des outils qui permettront de les canaliser et de les contrôler afin d'en limiter les risques pour l'ordre social et l'ordre public.

Dans ce cadre, je souhaiterais que vous mettiez en place un groupe de travail en vue d'analyser les menaces criminelles susceptibles de résulter d'une ouverture du marché des jeux en ligne et de proposer les voies et moyens d'y remédier.

Je vous prie d'agréer, Monsieur le Président, l'assurance de ma considération distinguée.

Bien à vous

Eric WOERTH

Monsieur Alain BAUER
Président de l'Observatoire national de la délinquance
108 Boulevard de Sébastopol
75003 Paris

MINISTÈRE DU BUDGET
DES COMPTES PUBLICS
ET DE LA FONCTION PUBLIQUE
139, rue de Bercy - Télédoc 146 - 75572 Paris Cedex 12

Remerciements

À M. Thierry Pujol, président de la Commission de la sécurité et de la gestion des risques de la WLA (*World Lottery Association*).

À MM. Ales Husak (République tchèque) et Tero Nykanen (Finlande), hauts dirigeants de sociétés de jeux et loteries de leurs pays.

Aux dirigeants de la société Keynectics et de la RGA (*Gambling Association Remote*)**.**

Aux services de police de l'Union européenne, des États-Unis et du Canada, qui ont bien voulu dialoguer avec nous, formellement ou informellement, durant nos travaux.

Introduction

Pour les criminologues, la question de l'ouverture à la concurrence des jeux, en ligne ou classiques, n'est pas un sujet en soi. La lutte contre l'addiction, comme phénomène social ou clinique, interpelle, mais hors du champ de nos compétences. Ce qui intéresse les spécialistes porte exclusivement sur la criminalisation des jeux.

Depuis toujours, faits divers et gestion des jeux se sont trouvés mêlés, en France comme à l'étranger. Création d'une ville du jeu (Las Vegas, mais pas seulement) par les organisations mafieuses, racontée notamment au cinéma, assassinats (Jean-Dominique Fratoni), disparitions (Agnès Le Roux), attentats et règlements de comptes, peuplent l'univers des casinos comme autant de rappels. Et la présence de nombreux appareils clandestins en France a généré une guerre des jeux qui, entre 1993 et 2004, a fait 301 victimes.

Les États ont toujours considéré avec attention le phénomène et les services judiciaires luttent contre la corruption, le racket ou le blanchiment. L'apparition de l'internet, par la suppression des frontières et des règles de contrôle, y compris la protection des parieurs et leur garantie de rémunération, crée un nouvel espace de préoccupation.

Bien évidemment, nombre des acteurs du jeu sont honnêtes et leurs entreprises légitimes. Mais comme en matière d'optimisation fiscale (le joli nom officiel de la fraude professionnalisée à l'impôt), la tolérance de systèmes *off shore* permet à chacun de se brancher sur le même tuyau qui permet aussi de blanchir l'argent du racket, de la corruption, des rétrocommissions, du crime et, en plus petite quantité, du terrorisme.

Voilà pourquoi le ministre du Budget, des Comptes publics, de la Fonction publique et de la Réforme de l'État a demandé ce rapport afin de permettre de mieux fixer des règles, fiables et efficaces, de négociation en vue d'une ouverture maîtrisée. Avec plus de 12 000 sites de jeux en ligne accessibles (dont une grande partie de sites « aspirateurs » visant simplement à pêcher des joueurs pour de véritables dispositifs), le marché du jeu en ligne draine près de 2 milliards d'euros en Europe (pour 36 milliards en France tous jeux confondus) [1].

(1) Pour l'association européenne des opérateurs de jeux (EGBA), le marché des jeux traditionnels devrait atteindre 95 milliards d'euros en 2012, soit 90 % de part de marché.

Selon les estimations d'un rapport du CERT-LEXSI5 basées sur les rapports d'activité des grands opérateurs étrangers, en 2005, en France, l'activité illégale des jeux en ligne représentait entre 300 et 400 millions d'euros annuels de produit brut des jeux alors que l'activité légale des jeux à distance de la Française des jeux (FDJ) et du Pari mutuel urbain (PMU) ne représentait que 110 millions d'euros de produit brut des jeux. Cela signifie qu'environ 75 % de l'activité des jeux à distance en France est illégale actuellement. Selon les études australiennes, la proportion serait de plus de 86 %.

Ces éléments donnent une idée assez claire des enjeux, financiers et légaux, de la criminalisation du jeu en général et sur internet en particulier.
Ce d'autant plus qu'une nouvelle réglementation européenne sur les transferts de valeurs (SEPA, *Single Euro Payments Area*) pèse également sur le dispositif :
– les moyens de paiements traditionnels vont être supplantés par des moyens transeuropéens comme les virements et prélèvements européens SEPA ;
– pourraient être utilisés, comme des jetons de jeux, des valeurs virtuelles d'échange comme le Linden de Second Life, les points de fidélité et coupons divers ;
– la réglementation européenne va mettre fin aux tutelles nationales comme le GIE CB et ouvrir le marché des transactions de paiement à de nouveaux opérateurs qui ne seront pas obligatoirement des banques ;
– parallèlement, les évolutions technologiques vont multiplier les canaux utilisables pour échanger des fonds (1) ;
– les mobiles GSM vont être un support privilégié pour les paiements de proximité (sans contact, porte-monnaie) et distants (carte SIM associée à une CB) ;
– les bornes en libre-service connectées à internet et dotées de moyens de paiement diversifiés (accepteurs de billets, CB, porte-monnaie électronique, GSM sans contact…) vont donner accès à de nombreux services dont pourraient faire partie les sites de jeux (la Française des jeux et Sagem Sécurité ont développé une borne, au même titre que le PMU).

De ce fait, pour procéder à des mouvements de fonds, il y aura une multiplication des canaux et des opérateurs ainsi qu'une délocalisation totale, ce qui changera les capacités de surveillance telles qu'elles existent aujourd'hui avec les banques et leur tutelle les banques centrales.

Le rapport Durieux a déjà fixé les contours d'une ouverture maîtrisée, nous laissant le soin de traiter de la dimension criminelle. Il nous revenait donc, en animant un groupe d'experts français et internationaux, et après audition d'un certain nombres d'acteurs professionnels et policiers européens, d'en détailler ici les compléments nécessaires.

Alain BAUER
Criminologue

(1) On notera à ce propos que la fraude identitaire a coûté 32 milliards d'euros aux États-Unis en 2007.

Perspective du rapport

Dans un système d'inspiration idéologique, la perfection et la satisfaction sont atteintes à la condition d'omettre, d'oublier, ce qui pourrait troubler la belle harmonie de la construction théorique.

Or dans le cas de l'ouverture des marchés des jeux, d'inspiration libérale, un oubli massif est, là encore, immédiatement constatable : celui du crime.

En effet, la lecture attentive, par les membres de la commission, de tous les textes réglementaires ou légaux régissant lesdits jeux, ce tout d'abord à Malte et à Gibraltar (qu'on nous présente souvent comme des modèles en la matière), n'a pas permis de trouver la moindre référence au risque criminel ou mafieux en tant que tel, ces textes se bornant à de rapides renvois aux législations antiblanchiment en vigueur.

Il semble ainsi que les autorités européennes sont, en matière de risques criminels dans le domaine des jeux en ligne, assez largement dans l'oubli, voire dans le déni.

Et elles ne semblent pas les seules dans ce cas, les sports les plus affectés par les infiltrations criminelles tentant aussi de nier que le problème existe (naïveté ? intimidation ?).

Chapitre I

Les fraudes

Libéralisation des jeux sur internet : les risques réels de fraude

La Commission européenne a décidé de libéraliser les jeux sur internet. D'essence libérale, ce projet a pour but de mettre fin aux anciens monopoles d'État et d'ouvrir les jeux à la concurrence.

Dans la perspective de l'octroi de licences internet à des entreprises privées, il est indispensable de créer un référentiel des risques présents dans le secteur. Aux risques exposés ci-dessus, il convient d'ajouter quatre catégories de risques supplémentaires : la fraude sur le retour financier exigé, les risques propres aux privatisations ainsi que la problématique des manipulations (sur l'exemple des concessions de service public) et pour terminer l'évolution de la situation dans le temps.

D'abord analyser les postulants et encadrer les risques

Il est d'abord nécessaire de prêter attention aux entreprises, dont l'ancienneté ne dépasse pas quelques trimestres, dont la localisation est vague et dont les détenteurs de capital semblent assez peu connus, ou plus exactement assez difficiles à identifier (fonds de pension, localisations dans des paradis réglementaires, etc.). Il pourrait être ainsi risqué d'octroyer une licence à une société dont l'installation est dans une structure *off shore* même si elle bénéficie d'une cotation dans une bourse de premier ou de second ordre.

Les entreprises les plus intéressées par l'ouverture du marché sont celles dont le modèle économique est fragile voire aléatoire. Cette fragilité ressort de la structure de son activité, par exemple une société qui est spécialisée dans les paris en ligne et qui brusquement par croissance externe (la croissance externe permet de rentrer rapidement dans un secteur mais ne donne à aucun moment le savoir-faire qui permet de durer) entre dans un nouveau domaine qu'elle ne maîtrise pas et dans lequel elle subit des pertes.

Dès lors, l'entrée dans un marché protégé peut constituer pour elle une condition de survie.

En effet, si ce principe (accord de licence) devait devenir la règle, il serait risqué de ne pas avoir effectué une cartographie des risques présents dans le secteur et d'anticiper les dérives possibles. La méconnaissance des risques de fraude, de corruption et de blanchiment dans un secteur aussi sensible pourrait conduire à toutes sortes de dérives.

Mais il convient au préalable de s'assurer que les divers lobbyistes ne manipulent pas les chiffres. En effet, dans ce secteur, il ne faut jamais oublier que les chiffres, les projections ou les espérances de gains sont difficilement évaluables du fait de l'absence de base solide pour les réaliser. Il se pourrait que les évaluations les plus positives, si elles comportent une espérance de gains considérable, ne soient pas réalistes.

Les fraudes classiques utilisant des détournements de base

Ces fraudes peuvent consister en un détournement des données bancaires des clients, de manière à ponctionner le compte bancaire par utilisation directe ou en revendant les données à des groupes criminels. Cela peut être le fait de l'organisation elle-même ou de salariés mal intentionnés ou encore de salariés faisant l'objet de chantage. La manipulation consiste à prélever des données stockées. Elle est possible dès l'instant où la maîtrise de l'activité est approximative.

Ces fraudes peuvent aussi prendre la forme de montages pour limiter les remboursements des gains en fixant par exemple des limites de remboursement qui créent chez le joueur une tentation à poursuivre le jeu sans prendre conscience de l'importance des pertes.

Par ailleurs, elles peuvent consister en un environnement poussant au jeu ainsi que des facilités de crédit rapidement octroyé par exemple. Cette facilité permet de jouer plus vite mais augmente aussi les opportunités de pertes. D'autant plus qu'il peut arriver que des liens aient été tissés entre les bookmakers en ligne et les bookmakers classiques. Ces derniers cumulent souvent avec leur activité principale - la prise de paris - l'activité secondaire de récupération des remboursements des créances accordées en ligne.

L'absence de mise en place d'une procédure de prévention pour les mineurs ou pour les personnes en état de faiblesse peut également être un indicateur de risques.

Enfin, il peut s'agir d'une utilisation détournée d'analyses réalisées ponctuellement par des prestataires qui laissent penser au non-spécialiste que le contrôle est constant alors qu'il n'est que ponctuel. Ceci portant le plus souvent sur l'analyse des taux de retours par type de jeux.

Sur ce point, les exigences suivantes devraient pouvoir figurer dans le cahier des charges. Ainsi, lorsqu'un joueur vient sur un site, il devrait :
– laisser un numéro de carte bleue ou payer par chèque, mais sans prélèvement automatique ;
– n'ouvrir un compte que s'il a plus de 18 ans ;
– être résident français ;
– disposer d'un compte bancaire en France et adresser un relevé d'identité bancaire (RIB) ;

– disposer d'un code confidentiel qui lui est adressé par courrier postal à son domicile ;
– limiter les mises à, par exemple, 100 euros par semaine par carte bancaire et 500 euros par chèque ;
– enfin, ne pas faire l'objet de publicités intempestives.

Les montages utilisant l'outil informatique

Ces montages passent par la manipulation des logiciels. En conséquence, il est suggéré de mettre en place une sorte de clause d'auditabilité qui autorise des opérations de contrôles directes ou par un mandataire dans les secteurs qui sont considérés comme risqués (analyses de log, test avec des fausses données des logiciels, etc.).

Il est également conseillé de procéder à une analyse régulière mais avec une périodicité irrégulière, sur l'ensemble des fichiers de la gestion commerciale ainsi qu'une analyse de l'historique. Cette opération fonctionne selon un mode aléatoire ou dans chacune des situations prévues.

La responsabilité de la lutte antiblanchiment incombe aussi à ces structures, d'où l'intérêt d'éviter qu'elles ne disparaissent. Pour éviter et prévenir ces risques, il semble essentiel que la structure distribuant les licences exige du bénéficiaire la mise en place d'un système de contrôle interne couplé à des outils spécifiquement dédiés au risque de fraude et de blanchiment.

On peut envisager ainsi l'intégration des exigences suivantes :
– existence d'un chemin d'audit pour chacune des opérations : si on prévoit un montant non significatif au-dessous duquel le chemin d'audit ne serait pas mis en place, analyser le risque d'occurrence des fraudes à effet levier dès l'origine et mise à jour régulière ;
– mise en place de points de contrôle placés de manière à ce qu'une agression extérieure puisse être identifiée très rapidement ;
– exigence d'un suivi des opérations en matière de blanchiment ;
– exigence d'un *reporting* régulier mais effectué de manière aléatoire de manière à ce qu'un effet de surprise soit toujours présent.

Détournements classiques relatifs aux droits dus

L'une des tentations les plus fortes pour le bénéficiaire est de limiter le produit ouvrant droit à paiement des sommes prévues en contrepartie de l'obtention de la licence.

Les méthodes classiques permettant de minorer autant que de besoin la base soumise au prélèvement se limitent à deux montages :
– manipulation des fichiers de la gestion commerciale de manière à ce que les pièces comptables ne laissent apparaître aucun indice de manipulation ;
– glissement des charges qui n'ont rien à voir avec le contrat dans la base de calcul.

Propositions de contrôles à installer pour éviter la fraude

Les précautions à prendre pourraient être organisées de la manière suivante.

Ouverture du marché et conditions d'entrée

Trois types d'entreprises sont susceptibles d'être intéressées par l'ouverture du marché.

Le premier groupe est constitué par celles qui, depuis des décennies, travaillent dans le secteur, elles l'ont créé et maîtrisent le domaine, elles apportent une certaine crédibilité bien que la plupart ont toujours exercé leurs activités économiques dans un cadre contrôlé, donc dans un environnement protégé. Elles ne posent guère de problèmes si ce n'est à la marge, leur intérêt, sauf pour les entreprises liées avec les États, étant de payer le moins de taxes possibles et de ne pas être contrôlées.

Un second groupe est composé par des entreprises qui n'ont aucune expérience mais qui entrent sur le marché dans le but, soit de créer une valeur intéressante à la revente, soit de retirer un maximum de gains des opérations sans être entravées dans leur activité. Un risque économique plus général peut les affecter car elles ont souvent une insuffisante maîtrise de leur propre activité tout en cherchant à dégager un profit maximum.

Enfin, le dernier groupe comprend une composante criminelle directe ou indirecte qui peut aisément entrer sur le marché au travers de prête-nom. Pour faire face à ce dernier risque, il serait souhaitable que les appels d'offres lancés par les gouvernements soient restreints afin de ne prendre en compte que des entreprises ayant une longue expérience dans le domaine (sept années pourraient constituer un délai raisonnable).

Par ailleurs, il est essentiel, dans un souci de transparence, de prévoir des dispositions relatives à la répartition du capital de l'entreprise qui bénéficie d'une licence. Avant d'accorder une licence, il convient de vérifier que l'entreprise existe bien, qu'elle exerce de manière directe cette activité, qu'elle n'est pas le faux nez de tel ou tel groupe ou de tel ou tel fonds incontrôlés. Il est souhaitable de susciter des audits externes pour s'assurer de la qualité de quelques points clés. Il conviendrait également d'exiger que les organisations obtenant des licences restent soumises à certaines obligations, afin de préserver la crédibilité du secteur. Ainsi, la société bénéficiaire devrait garder les mêmes caractéristiques tout au long de la gestion de la licence. Il en va de la sécurité de la convention comme de celle des utilisateurs.

En effet, à la lumière des montages les plus classiques déjà constatés dans des opérations de privatisation, les détournements de licences consistent, une fois l'obtention de la licence rendue effective, à réorganiser l'entreprise de manière à la rendre incontrôlable. Dans ce cas, la disparition d'actifs au travers de sociétés *off shore* est un risque élevé.

À cet égard, en modifiant les caractéristiques de la capitalisation par des rachats ou échanges prévus de longue date, le bénéficiaire de la licence peut très rapidement être remplacé par un tiers absent de la procédure. Par ce moyen, des structures exclues du marché pourraient y entrer de manière officieuse.

Nous estimons qu'il pourrait être pertinent d'exiger que le responsable soit une personne physique pour les sociétés implantées dans les pays d'Europe dans lesquels la responsabilité de la personne morale est absente ou non appliquée.

De la même façon, il est possible de rendre les contrôles inopérants en procédant à une délocalisation de la structure administrative, à des restructurations internes ou en modifiant l'organisation du système informatique.

Ces simples manipulations, qui semblent refléter des évolutions légitimes au regard du droit des affaires, peuvent avoir pour effet de neutraliser le contrôle de l'État qui a accordé les licences. C'est pourquoi, il semble logique d'imposer une assise territoriale au bénéficiaire. Celui-ci devra résider et installer l'ensemble de ses systèmes dans le pays qui lui confie la licence de manière à présenter une unité de contrôle.

Pour prévenir tout risque de corruption, il convient aussi de s'assurer que les personnes, fonctionnaires ou membres des cabinets ministériels qui ont organisé la distribution des licences, ne puissent pas avoir une seconde carrière dans les entreprises dont ils ont eu à traiter. Cette exigence devrait même être renforcée par rapport aux prescriptions de droit commun qui s'appliquent au « pantouflage » des agents publics.

Dans les termes du contrat relatif à l'octroi d'une licence dans le domaine des jeux, il est donc essentiel d'inclure un certain nombre de clauses : clauses de territorialité, clauses de cohérence dans le capital, clauses d'auditabilité de la gestion commerciale ainsi que des clauses stipulant la suspension et la rupture du contrat en cas de non-respect des engagements.

Il est donc essentiel d'exiger que le bénéficiaire reste le même pendant toute la période de la convention, à la fois structurellement et géographiquement. Ceci implique l'octroi de licence pour des périodes relativement courtes.

Contrôler le risque de fraudes dans la gestion des jeux

Il convient de prévenir le risque de fraude résultant de cette gestion en mettant en évidence les opportunités de fraudes les plus évidentes dans ce secteur économique. Un État qui accorderait une licence à une organisation susceptible de frauder risquerait en effet de voir son image durablement ternie.

Précautions à prendre au regard des paris à cote

Ce type de pari doit être soumis à un régime particulier, certains ne sont d'ailleurs pas autorisés en France. Il s'agit :
– des paris hippiques à cote fixe ;
– des paris sur les écarts de cote *(spread betting)*. Le gain final de ce type de paris ne peut être déterminé à l'avance. Le joueur peut donc gagner ou perdre plusieurs multiples de sa mise et par conséquent le risque financier de l'opérateur peut s'avérer important et le risque pour le joueur élevé (effet de levier) ;
– des bourses d'échanges de paris entre joueurs, où l'opérateur ne fait que mettre à disposition des moyens techniques permettant de mettre en contact les joueurs ;
– des paris en cours de rencontre *(live betting)*, principale source de chiffre d'affaires des bookmakers (environ deux tiers du chiffre d'affaires de certains). La question du *live betting* devra se poser à l'avenir pour permettre à l'offre autorisée de jouer son rôle de canalisation de l'offre sur ce segment en proposant du *live betting* responsable tant du point de vue de la protection contre le jeu excessif que de la lutte contre la corruption sportive.

Pour les autres paris, le code de bonne conduite des pronostics sportifs, promu par *European Lotteries*, et signé à ce jour par quarante-trois loteries dont la Française des jeux, a élaboré un dispositif de règles préventives et de procédures de surveillance relatives au risque de corruption ou de blanchiment associé aux jeux de contrepartie.

Limiter le développement non maîtrisé des fraudes à l'encontre des joueurs, de la corruption dans les paris et du blanchiment

Les précautions sont les suivantes :
1) exiger la mise place et faire contrôler régulièrement mais de manière aléatoire (éviter la manipulation des supports à l'approche des contrôles de fin d'année par exemple) l'implémentation des mesures antiblanchiment ainsi que la remontée d'informations vers l'UIF (Unité d'investiture financière) ;
2) mettre en place une clause d'auditabilité qui permet à une autorité de régulation émanant d'un pouvoir d'État (pas de sous-traitance à une structure privée car étant payée par le client un conflit d'intérêt est mécaniquement mis en place) de contrôler les logiciels d'audit et les fichiers au regard du risque de la fraude (un chemin d'audit existe et peut être suivi) et de manipulations des données ;
3) prélever une taxe sur les opérations effectuées par les sociétés de paris privées afin de financer, à partir du chiffre d'affaires de ces dernières, les frais d'addiction qui au final sont payés par la collectivité ;
4) contrôler les mineurs : procédurer les opérations et bloquer les entrées ;
5) envisager légalement pour les structures privées (pour le public, cela ne présente guère d'importance car les associations sportives sont d'essence publique) l'application d'un droit d'image sur les compétitions qui génèrent des paris ;
6) mettre en place des systèmes de contrôle embarqués sous forme de requêtes qui soient en mesure de traiter de manière systématique (comme les outils de remontée d'atypismes antiblanchiment) les erreurs, les modifications des fichiers de traitement des données, etc., ces traitements faisant l'objet de *reporting* récurrents.

Protéger les droits de l'État ou de la structure qui accorde les licences

• Sur les personnes susceptibles d'être choisies

Le premier risque est celui des postulants, les entreprises, dont l'ancienneté ne dépasse pas quelques trimestres, dont la localisation est vague et dont les détenteurs de capital semblent assez peu connus, ou plus exactement assez difficiles à identifier (fonds d'investissement, localisations dans des paradis réglementaires, etc.). Il pourrait être ainsi risqué d'octroyer une licence à une société dont l'installation est dans une structure *offshore* même si elle bénéficie d'une cotation dans une bourse de premier ou de second ordre. La cotation n'est pas dans ce secteur un critère de vertu.

Les entreprises les plus intéressées par l'ouverture du marché sont celles dont le modèle économique est fragile, voire aléatoire. Ce caractère ressort de la structure de son activité, par exemple une société qui est spécialisée dans les paris en ligne et qui brusquement, par croissance externe (la croissance externe permet de rentrer rapidement dans un secteur mais ne donne à aucun moment le savoir-faire qui permet de durer), entre dans un nouveau domaine qu'elle ne maîtrise pas et dans lequel elle subit des pertes.

Dès lors, l'entrée dans un marché protégé peut constituer pour elle une bouée de survie.

• Protection du paiement des redevances

Les précautions sont les suivantes :
1) exiger que, pendant la durée de la concession ou de la licence, la structure de la société bénéficiaire ne soit pas modifiée par des rachats intempestifs, par des modifications d'actionnaires ou par toute opération relative à des modifications du haut de bilan. Objectif : éviter les modifications de structures qui affectent le paiement des redevances.
2) exiger que, pendant la durée de la concession, l'ensemble des systèmes informatiques, les logiciels de jeux et le *back office* soient localisés dans le pays qui accorde la concession, de manière à permettre un contrôle aléatoire immédiat. Le risque de fractionnement, de manipulations développées dans des contrées lointaines étant majoré. Objectif : éviter les manipulations des données de nature à minorer les résultats sur lesquels sont calculées les redevances (grand classique des fraudes).
3) intégrer une clause d'auditabilité permettant d'évaluer la qualité et l'exhaustivité de la remontée d'informations depuis le système de gestion commerciale vers le système comptable de manière à ce que la base qui permet d'évaluer les redevances ne puisse pas être manipulée.
4) exiger la mise en place d'une charte de déontologie et une obligation de formation des cadres (comme la procédure antiblanchiment) ; une procédure formelle mais importante symboliquement.

Chapitre II

L'activité criminelle

La dimension humaine : criminels, mafieux et jeux en ligne

L'industrie des jeux et paris en ligne est actuellement non régulée, avec un risque d'infiltration par le crime organisé, sans protection pour les joueurs, et un accès incontrôlé pour les enfants ou les personnes vulnérables. En outre, cette situation entraîne une perte de revenus fiscaux pour l'État. Les activités concernant les jeux et les paris ont depuis toujours été dans le viseur des organisations criminelles. L'évolution technique entraînant la mise sur internet de ce type d'activité est donc logiquement regardée de près par ces mêmes organisations. Si celles-ci perdent le bénéfice des transactions en liquide, elles gagnent en audience et en manque de transparence.

Pourtant, cette réalité criminelle n'est que peu prise en compte par les autorités. Gibraltar et Malte, deux des principaux pays d'accueil des sites de jeux en ligne, évoquent certes les risques de blanchiment mais renvoient simplement aux législations locales, avec le principe, comme en France, de déclaration de soupçons (1).

En Afrique du Sud par exemple, les parlementaires ont modifié le *National Gambling Amendement Bill* de 2004 pour légaliser les jeux en ligne en mai 2008. Outre les problèmes de fraude et de dépendance, les députés sud-africains ont souhaité, dans une note annexe à la loi, attirer l'attention sur les risques de blanchiment par le crime organisé et de financement du terrorisme.

Le monde du tennis, très touché par la corruption (voir *infra*), semble prendre conscience du problème, même si les professionnels de ce sport préfèrent ne pas communiquer sur le sujet. S'inspirant de l'exemple du cricket, les organismes du tennis ont demandé un rapport sur les risques liés aux paris sportifs : *Environmental Review of Integrity in Professional Tennis* (mai 2008, de Jeff Rees et Ben Gunn), qui s'est lui-même inspiré d'une étude faite en février 2008 par l'université de Salford *(Risks to the integrity of sport from betting corruption)*.

(1) Gibraltar : *Gibraltar Criminal Justice Ordinance* et *Anti Money Laundering Guidelines.* Malte : *Prevention of Money Laundering and Funding of Terrorism Regulations*.

Jeux et paris, une activité très criminogène

Avant même l'existence de l'informatique et de l'internet, les activités de paris suscitent la convoitise des criminels qui tentent d'influer sur les résultats des rencontres sportives.

• 1913 : Pascoe Bioletti, un criminel anglais dont le fils travaille chez un bookmaker de Genève, tente de corrompre des joueurs du West Bromwich Albion FC et du Birmingham City FC. Il est condamné à cinq mois de prison en 1914.

• 1919 : c'est le *Black Sox Scandal* qui entraînera l'exclusion à vie de 9 joueurs de baseball dont 8 des White Sox de Chicago. Au cœur de l'affaire : Arnold Rothstein, l'un des plus importants parrains new-yorkais, impliqué dans des affaires de jeux, de trafic d'alcool et de stupéfiants.

• 1921 : de graves soupçons pèsent sur une course hippique de Saratoga Springs (un des principaux champs de courses de l'État de New York), le cheval gagnant appartient à Arnold Rothstein.

• 1951 : une affaire de corruption touche le basket universitaire américain. 7 équipes sont concernées. On relève dans l'affaire le nom de **Thomas Eboli** (également très présent dans la boxe, il a été le *boss* de la famille Genovese de 1969 jusqu'à son assassinat en 1972).

• 1973 : scandale du prix « Bride Abattue » en France ; implication de plusieurs figures du banditisme dans cette affaire de courses truquées (dont Jean-Louis Fargette, futur « parrain » de Toulon, abattu en 1993 et Jacky Imbert, figure du milieu marseillais depuis les années 1960). Le Milieu avait mis la main sur l'inventeur d'une formule mathématique basée sur les probabilités pour parier.

• 1978-1979 : plusieurs joueurs de basket du Boston College sont corrompus par les frères Rocco et Tony Perla. Pour maximiser leurs profits (basés sur les paris sur la différence de points entre les équipes), les frères font appel à des associés de la famille Lucchese (Henry Hill et James Burke), sur autorisation du capo Paul Vario. La fraude ne sera découverte qu'avec les révélations d'Henry Hill en 1980 (1).

• 1994 : la mise sur écoutes de Victor Spink par la police australienne pour un trafic de 15 tonnes de cannabis permet de mettre à jour une affaire de courses hippiques truquées.

• 1994 : Bruce Grobbelaar (gardien de l'équipe nationale sud-africaine et du club de Liverpool), le goal de Wimbledon et un joueur d'Aston Villa sont soupçonnés d'avoir accepté de l'argent d'un syndicat de parieurs malaisiens.

• 1997 : les syndicats de parieurs sino-malaisiens réussissent à saboter les lumières du stade de West Ham et de Crystal Palace (première division de football britannique), les interruptions de matchs influant sur les paris. En 1999, c'est le stade de Charlton Athletic qui est ciblé.

(1) L'histoire d'Henry Hill est racontée dans le film *Les Affranchis* de Martin Scorsese avec Ray Liotta dans le rôle de Hill et Robert De Niro dans celui de Jimmy Burke.

• 2000 : des écoutes téléphoniques en Inde mettent en lumière les liens entre un syndicat criminel indien et un capitaine de l'équipe de cricket d'Afrique du Sud. Trois autres joueurs sont impliqués. Le capitaine est exclu à vie.

• 2004 : le site de paris en ligne Betfair identifie des paris anormaux. L'enquête permet de mettre en cause 80 courses hippiques en deux ans. 6 jockeys sont arrêtés.

• 2004 : la police sud-africaine arrête 33 personnes (dont 19 arbitres et officiels) pour avoir truqué des matchs de football.

• 2004 : plusieurs joueurs du club de rugby de St. Helens (Grande-Bretagne) sont sanctionnés pour avoir fait des paris en ligne contre leur équipe.

• 2005 : scandale de corruption dans le football brésilien (au moins un responsable de la FIFA acheté), 11 matchs annulés.

• 2005 : vaste affaire de corruption dans le football belge, les clubs de Lierse, La Louvière, Sint-Truiden, AEC Mons, V. Geel et G. Beershot sont impliqués. Des soupçons pèsent également sur un club français et un club finlandais.

• 2005 : scandale de corruption dans la deuxième division de la *Bundesliga*. Un arbitre semble être le pivot de l'affaire, faisant le lien entre des joueurs et une organisation criminelle croate liée à une agence de paris. 13 matchs sont concernés.

• 2006 : Opération Slapshot par le FBI, 3 équipes de la NHL (hockey) sont concernées (les Coyotes de Phoenix, les Sharks de San José et les Maple Leafs de Toronto). La famille Scarfo de Philadelphie est impliquée dans l'affaire.

• 2006 : gros scandale de matchs truqués en Italie, la Juventus, l'AC Milan, la Fiorentina, le Lazio sont impliqués.

• 2007 : le FBI enquête sur les deux dernières saisons de la NBA (basket). Les enquêteurs n'excluent pas une implication de la Cosa Nostra dans cette affaire mais n'en ont pas la preuve.

En plus des épreuves sportives, le crime organisé s'est toujours intéressé aux établissements de jeux. On peut évidemment citer l'infiltration d'abord directe (financement, notamment *via* les fonds de pension du syndicat des camionneurs), puis indirecte (contrôle des syndicats, de la prostitution, de l'usure…) dans les casinos du Nevada (Las Vegas) et du New-Jersey (Atlantic City). On a également noté l'infiltration des familles mafieuses après que les réserves indiennes aient reçu l'autorisation en 1988 de mettre en place des casinos tribaux sur leur territoire. Plus récemment (2001), le Bureau de contrôle des jeux de l'Illinois a bloqué l'implantation d'un casino à Rosemont du fait des liens des promoteurs avec la famille de Chicago.

D'autres organisations sont également impliquées dans les activités de jeux. Ainsi, le Milieu israélien contrôle des casinos clandestins en Israël[1] même ou prend des parts dans des casinos à Prague[2] ou à Chypre, en association avec les organisations mafieuses turques. En Turquie, le « roi des casinos », Omer Lufti Topal, déjà condamné pour trafic de drogue, contrôlait un casino sur 5, jusqu'à son assassinat en juillet 1996. Topal, en forte « odeur de Mafia », s'était allié avec des organisations criminelles russes après qu'une loi interdise les casinos aux citoyens turcs[3].

En Chine, les jeux de hasard sont officiellement interdits mais il existe de nombreux casinos clandestins (tenus par des triades ou par des indépendants devant de toute façon payer un tribut aux organisations mafieuses[4]) ou des sites en ligne (basés à Hong-Kong et à Taïwan notamment). Au Japon, ce sont les yakuzas qui contrôlent les machines à sous et les casinos clandestins : en mai 2008, un cercle clandestin est découvert à Nagoya (11 employés et 33 joueurs arrêtés). En avril 2008, une opération menée à Turin dévoile la présence de la Cosa Nostra et de la Ndrangheta dans 5 cercles clandestins, où se vendaient également des stupéfiants et où se pratiquaient des activités usuraires.

En France, plusieurs affaires ont montré l'intérêt du crime organisé pour les établissements de jeux :
– entre 1962 et 1968 : « guerre » des cercles de jeux entre les Corses Jean-Baptiste Andréani (soutenu par les frères Guérini de Marseille) et Marcel Francisci[5] (lié aux frères Zemmour). Plusieurs fusillades, attentat à la bombe, meurtres pour le contrôle des cercles parisiens ;
– 1977 : disparition d'Agnès Le Roux, fille de la propriétaire du casino du Palais de la Méditerranée à Nice et concurrente du casino Ruhl tenu par Jean-Dominique Fratoni et des financiers romains ;
– 1985 : Paul Mondoloni (ancien de la *French Connection*) tente de mettre la main sur le Ruhl. Il est abattu avant d'avoir réussi l'opération ;
– 1991 : affaire de la Sofextour, une société créée par Giovanni Tagliamento (neveu et bras-droit du *boss* de la Camorra Michele Zaza), parrain corse ;
– 1997 : plusieurs allers-retours de proches de la Brise de mer[6] sont repérés entre la France et la Russie. L'enquête montre que le Milieu corse veut investir dans un casino en Sibérie ;

(1) Une des premières décisions quand l'Autorité palestinienne a eu un minimum de pouvoir a été de légaliser les jeux et d'autoriser l'installation d'un casino (avec sans doute des fonds du milieu israélien).

(2) En 2003, Félix Abutbul, figure de la pègre israélienne, est abattu par balles à la sortie de son casino à Prague. Un an plus tard, son fils, Assi Abutbul, est l'objet d'une tentative de meurtre à la grenade devant ce même casino. Un autre fils Abutbul, François, a été impliqué dans la tenue d'un casino clandestin sur un bateau. Le clan Abutbul, pilier du milieu israélien, a des contacts avec des criminels français.

(3) Cette loi a favorisé l'apparition de casinos clandestins, un flux de nouveaux clients étrangers (principalement russes) et un détournement de certains clients turcs vers la Chypre du Nord.

(4) En région parisienne, il y aurait 4 à 5 casinos clandestins destinés à la communauté asiatique (voir Jérôme Pierrat, *Mafias, Gangs et Cartels - La criminalité internationale en France*, Paris, Denoël, 2008).

(5) Abattu en 1982 à Paris.

(6) Le gang de la Brise de mer est un groupe de criminalité organisée en Corse. Source Wikipédia.

– 2007 : un règlement de comptes ayant fait 3 morts à Marseille en 2006 permet aux enquêteurs de découvrir un financement occulte impliquant le Cercle Concorde à Paris. Dans cette affaire : plusieurs voyous corses, une figure de la pègre marseillaise et un banquier genevois.

Au-delà de leurs intérêts pour et dans les casinos, le grand banditisme français est impliqué, depuis le début des années 1980, dans l'exploitation des machines à sous illégales. La gestion de ce marché criminel rapporte des revenus réguliers aux malfaiteurs, revenus servant ensuite à d'autres activités (trafics de stupéfiants, achat d'armes de guerre pour le braquage de fourgons blindés…). On estime qu'il existe entre 6 000 et 7 000 machines à sous clandestines en France, rapportant, selon l'emplacement, entre 4 000 et 7 000 euros par mois, partagés à égalité entre le placier et le gérant de l'établissement d'accueil. Dans les années 1990, une guerre pour le contrôle du marché des machines à sous a touché la partie sud-est de la France : entre 1993 et 2004, cette guerre du Milieu a entraîné près de 300 règlements de comptes, faisant autant de victimes [(1)].

Jeux, paris en ligne et Mafia

L'implication de la mafia italo-américaine dans le cyber-espace est essentiellement liée à l'industrie des jeux et des paris en ligne (mais également à la pornographie). Aux États-Unis, les paris (notamment sur les événements sportifs) représentent 200 milliards de dollars annuellement, dont seulement 3 milliards sont légalement effectués à Las Vegas. Les paris illégaux sont majoritairement aux mains du crime organisé aux États-Unis (en premier lieu par les clans italo-américains mais aussi, selon la communauté d'origine, par les organisations asiatiques, la *Corporación* cubaine…) et ces activités de jeux sont souvent couplées avec une activité d'usure.

• Mai 2008 : la police de Philadelphie, aidée du FBI, procède au démantèlement d'un réseau de paris clandestins très perfectionné. 8 serveurs informatiques, tournant avec 19 ordinateurs, enregistraient les paris (sur le basket, le baseball, le hockey, les courses automobiles…) passés par téléphone ou par internet. Les parieurs avaient un numéro d'identification personnel. 9 personnes sont interpellées et les enquêteurs soupçonnent des liens avec la famille mafieuse locale.

Source : "High-tech sports-gambling ring busted'
(Philadelphia Daily News, 16 mai 2008).

• Mai 2008, la justice a procédé à l'inculpation de 23 personnes dans le New-Jersey, notamment pour jeux illégaux, extorsion, fraude et racket syndical. Parmi les personnes inculpées figurent : Andrew Merola (chef du réseau, important membre de la famille Gambino dans le New-Jersey), Charles Muccigrosso (dit « Buddy Musk », également soldat des Gambino) et Martin

(1) Voir Xavier Raufer et Stéphane Quéré, préface d'Alain Bauer, *Machines à sous et criminalisation en France*, Notes & Études de l'Institut de criminologie n° 3, Département de recherche sur les menaces criminelles contemporaines, septembre 1999.

Tacetta (membre et ancien sous-boss de la faction de la famille Lucchese dans le New-Jersey). Ils sont accusés d'avoir organisé des paris et des jeux illégaux *via* internet (site basé à l'étranger), un service téléphonique gratuit et d'avoir utilisé deux sections syndicales pour détourner des fonds et pour extorquer des sociétés, notamment de construction. Il s'agit de la section 1153 du *Laborer's International Union of North America* (LIUNA) et de la section 825 de l'*International Union of Operating Engineers* (cette section compte 7 000 membres, notamment des conducteurs d'engins de chantier).

Communiqué de l'*US Attorney*, mai 2008.

• Depuis quelques mois, les professionnels du sport (notamment du tennis, plus facile à influencer car n'étant pas un sport d'équipe) s'inquiètent des pressions pesant sur les joueurs. Ces pressions et menaces semblent directement liées à l'explosion des paris en ligne, et donc à des enjeux financiers importants. Les tennismen mettent en cause des organisations criminelles russes. Le nº 1 britannique Tim Henman a été l'un des premiers à lancer l'alerte, conforté en cela par les déclarations de Novak Djokovic (nº 3 mondial) qui a reconnu une proposition de 125 000 euros pour perdre un match lors d'un tournoi en Russie en 2006.

• L'ancien champion australien Pat Cash craint pour sa part une pression croissante surtout sur les futurs champions, plus vulnérables aux propositions financières. Cash a invité les dirigeants du tennis à mettre en place une unité anticorruption, suivant l'exemple du cricket (jeu également soumis aux pressions des parieurs, notamment issus de la pègre indo-pakistanaise). En France, les joueurs Mickaël Llodra et Arnaud Clément ont reconnu avoir été approchés. Mêmes aveux du côté du russe Dimitri Tursunov, de l'américain Paul Goldstein, du brésilien Flavio Saretta (100 000 euros pour perdre au premier tour de Roland-Garros), le belge Gilles Elseneer (100 000 dollars pour perdre au premier tour de Wimbledon en 2005), le marocain Younes El-Aynaoui (25 000 euros pour se « coucher » lors d'un tournoi du circuit secondaire) ou du serbe Janko Tipsarevic.

• En juillet 2007, les observateurs se sont étonnés de l'abandon d'un joueur russe en Pologne face à un quasi-inconnu alors qu'il avait gagné 6-2 le premier set. Les paris enregistrés sur internet (site de paris Betfair[1]) à l'occasion de ce match étaient de plus de 6 millions d'euros, soit dix fois plus qu'attendus[2]. Les rumeurs sur l'influence des paris sur les résultats des sportifs ont été démenties par Rafael Nadal (nº 2 mondial). Même discrétion du côté de Roger Federer (nº 1 mondial). Les organisations professionnelles (ATP pour les hommes et WTA pour les femmes) sont réticentes à communiquer sur le sujet, même si elles semblent s'en inquiéter (l'ATP a par exemple pris l'attache de la *British Horseracing Authority*, chargée du contrôle des courses de chevaux en Grande-Bretagne). Pourtant, certains dénoncent des « amitiés suspectes » entre joueurs et mafieux.

(1) Opérateur de jeux et de paris en ligne, opérant en Grande-Bretagne (licence de jeux : 105-002062-R-104133-001), en Australie, à Malte, en Italie, en Autriche et en Allemagne.

(2) Quelques semaines plus tard, le même joueur, Davidenko, est sanctionné par l'arbitre lors d'un match à Saint-Pétersbourg pour « manque de combativité ».

• En octobre 2007, la Fédération française de tennis, à l'occasion du tournoi de Paris-Bercy, a tenté de limiter la corruption : présence de policiers des RG dans l'enceinte du tournoi, accord avec certains sites de paris pour détecter des mouvements financiers anormaux, surveillance des matchs pour repérer les « anomalies sportives »… Des spectateurs qui tentaient de passer des paris dans l'enceinte du tournoi *via* leurs ordinateurs portables ont même été expulsés. Des mesures similaires ont été prises en décembre 2007 pour l'Open d'Australie, une première pour un tournoi du Grand Chelem, puis en mai 2008 lors du tournoi de Roland-Garros.

Le tennis n'est pas le seul sport concerné par la corruption liée aux paris. En novembre 2007, l'Union des associations européennes de football (UEFA) s'est rapprochée d'Europol, notamment pour enquêter sur quinze matchs jugés suspects (des rencontres de Coupe d'Europe et d'autres comptant pour les éliminatoires de l'Euro 2008). Les matchs en question concerneraient des équipes bulgares, géorgiennes, serbes, croates et baltes. Une dizaine d'autres matchs pourrait également être visée, notamment le match Liverpool contre Besiktas Istanbul (8 à 0), lors duquel l'équipe turque aurait été approchée par des mafieux. La corruption présumée serait principalement liée à des paris pris sur internet par des réseaux asiatiques. Aidées d'Interpol, les polices asiatiques ont lancé plusieurs opérations contre les paris illégaux : en octobre 2007, 266 perquisitions ont été menées à Hong-Kong, Macao, Chine, Singapour, Thaïlande, Vietnam et Malaisie (432 arrestations). Cette opération, baptisée « Soga », visait des réseaux de paris illégaux portant sur un total de 680 millions de dollars par an. Les réseaux asiatiques apparaissent dans des matchs joués en Belgique, aux Pays-Bas, en Allemagne et en France (1).

• En novembre 2006, la Gendarmerie royale du Canada lance l'Opération Colisée, entraînant 90 perquisitions et l'arrestation de 73 personnes (d'autres seront arrêtées les semaines ou les mois suivants). Cette opération vise particulièrement la mafia de Montréal (un de ses parrains historiques est d'ailleurs interpellé). Les personnes interpellées doivent répondre d'un total de près de 1 000 chefs d'inculpation parmi lesquels association de malfaiteurs (« gangstérisme »), tentative de meurtre, extorsions de fonds, fraude fiscale, blanchiment, trafic de stupéfiants (800 kg de cocaïne et 40 kg de marijuana saisis) mais également jeux illégaux. Les activités de paris sur internet étaient plus particulièrement gérées par Lorenzo Giardino et Francesco Del Balso. Sur 18 mois, le réseau, opérant depuis un serveur basé au Belize, puis dans la réserve amérindienne de Kahnawake, a enregistré pour 520 millions de dollars canadiens (333 millions d'euros) de paris illégaux pour un bénéfice de 26 millions de dollars (16,5 millions d'euros) (2).

Communiqué de la Gendarmerie royale du Canada/
***différents articles de la presse canadienne dont* The Montreal Gazette**
du 6 mars 2007 et* La Presse *du 18 janvier 2007.

(1) Voir notamment : « Le tennis, nouvelle proie de la mafia des jeux » le *Midi-Libre* du 15 octobre 2007. « Jeu, set, match et paris truqués », *Le Monde* du 1er novembre 2007. « Jeu, set et fraude », *Libération* du 3 novembre 2007. « Mobilisation contre la corruption sur les courts », *Le Figaro* du 12 décembre 2007. « Enquête sur quinze matchs européens truqués », *MyFreeSport*, 1er décembre 2007. "Interpol *vs* illegal betting', AFP du 23 janvier 2008.

(2) Il ne s'agit là que d'une estimation par les services de police.

• En 2006, les autorités américaines ont décidé de poursuivre la société britannique BetOnSports[1], pour racket et fraude. La justice américaine l'accuse d'être liée à Bestlinesports.com, basé au Costa Rica. Ce site de paris en ligne était dirigé par Joseph « Boca Joe » Fafone et son fils Joseph Junior, inculpés en 2002. Ils sont considérés comme des membres de l'équipe de Frank « The Bear » Basto[2], soldat des Gambino. BetOnSports avait déjà été signalé comme ayant des liens avec la société Safe Deposit Sports (sous contrôle de la mafia new-yorkaise), louant des bureaux au siège costaricain de BetOnSports. 10 autres collaborateurs et 3 autres sociétés appartenant à la Kaplan Gambling Enterprise (Direct Mail Expertise, DME Global Marketing and Fulfillment, Mobile Promotions) sont inculpés d'escroquerie, conspiration et fraude. La justice américaine a fait fermer les pages Web de la société, entraînant par ricochet une baisse ponctuelle des actions des sociétés Partygaming (– 22 % en deux jours) et SportingBet (– 45 %), leaders des jeux en ligne et cotés à la Bourse de Londres.

***Financial Times* du 5 août 2006**
et *Journal du Net* du 28 juillet 2006.

• En février 2006, 49 personnes sont interpellées lors de 34 perquisitions dans le New-Jersey, à New York et en Floride, permettant la saisie de 3 millions de dollars en liquide, de 6 armes à feu et de petites quantités de cocaïne et de marijuana. Ce réseau de paris illégaux était dirigé par un associé des Genovese. Les paris étaient placés par téléphone et par internet *via* une société basée au Costa Rica[3].

***Associated Press* du 9 février 2006.**

• En 2005, Frank « Lefty » Rosenthal ouvre son propre site de conseils en paris sportifs (http://www.frankleftyrosenthal.com). Il est également consultant en paris sportifs (football américain, basket, base-ball, hockey) pour quatre sites de jeux en ligne basés au Costa Rica et à Antigua (betcris.com ; betwwts.com ; betjazzsports.com ; bodog.com). Rosenthal est l'ancien directeur de l'hôtel-casino Stardust à Las Vegas, habitant actuellement en Floride suite à une tentative de meurtre à la voiture piégée en 1982 et à son placement sur le *Black Book* des autorités du Nevada en 1988. Incarné en 1995 dans le film *Casino* par Robert De Niro, « Lefty » est impliqué dans les jeux illégaux depuis les années 1950 et a été l'homme de la famille de Chicago dans les casinos de Las Vegas dans les années 1970.

***The Miami Herald* du 13 février 2005.**

(1) Pour 2005, BetOnSports a publié un bénéfice d'exploitation de 20,1 millions de dollars, en croissance de 65 %. Le volume des mises enregistrées sur la période par la société s'élève à 1,77 milliard de dollars, en croissance de 25 % sur un an.

(2) Condamné en mai 2002 à 65 mois de prison pour trafic de cocaïne et jeux illégaux.

(3) À noter que Dominick Curra, considéré comme le bookmaker personnel de John Gotti, a été arrêté le 12 mars 2002 au Costa Rica, où il possédait des intérêts dans des sociétés de jeux en ligne. Il était recherché par les États-Unis pour une affaire de faux tableaux.

• En janvier 2005, 17 personnes sont inculpées pour avoir monté un réseau de paris illégaux couvrant New York, le New-Jersey, la Floride, le Nevada et le New-Hampshire. Dirigé par 3 associés du clan Gambino (les frères Gérald et Cesare Uvari et le fils de Cesare, Anthony), ce réseau gérait 80 000 dollars de paris par jour soit près de 200 millions de dollars sur un peu plus de quatre ans. Parmi les personnes inculpées figure également un entraîneur hippique de New York, soupçonné d'avoir dopé des chevaux sur certaines courses. Les prises de paris se faisaient, par téléphone ou par internet, *via* des sociétés basées aux États-Unis mais surtout aux Antilles néerlandaises et à l'île de Man, permettant ainsi d'éviter les services fiscaux.

***New York Daily News* du 14 janvier 2005.**

• La mafia italo-américaine n'est pas la seule impliquée dans le commerce sur internet. À la fin des années 1990, les autorités canadiennes et américaines (dont la SEC, le service de contrôle des activités boursières, et la *Food and Drug Administration*) se sont intéressées au cas de la société Starnet Computer Communications, créée en mai 1995. Cette société s'est spécialisée dans la diffusion de shows érotiques sur internet, puis, à partir de 1997, dans les jeux en ligne depuis Antigua et même dans la vente de produits paramédicaux (vitamines notamment). À la tête de cette société figure Ken Lelek (inculpé en 1999 pour violation de la loi canadienne sur les jeux), associé avec Lloyd Robinson (1) dans une autre société de l'industrie du sexe, That's Entertainment. Plusieurs enquêtes semblent également montrer les liens entre Lelek et le crime organisé italo-américain, notamment avec la famille Genovese et le clan Caruana-Cuntrera. La société Starnet est en fait soupçonnée de blanchir l'argent de plusieurs organisations criminelles, accusation qu'elle réfute en précisant qu'elle a organisé une conférence à Antigua sur la cybercriminalité.

Voir notamment le *Vancouver Sun* du 1er août 2000 et le *Toronto Sun* du 20 novembre 2000.

• En Italie, les autorités antimafia ont décidé en juin 2008 de poursuivre 126 personnes impliquées dans des courses de chevaux clandestines entre 2001 et 2003. Organisées par le clan Villabate de Cosa Nostra (également impliqué dans le secteur des machines à sous illégales), les courses se tenaient en Campanie, dans les Pouilles, en Calabre, en Ombrie, en Lombardie et dans le Piémont. Non seulement le clan mafieux gérait les paris clandestins sur ces courses, mais en plus il s'intéressait aux courses officielles en utilisant le dopage et la corruption de jockeys. Les paris étaient gérés par internet et l'un des trois repentis dans cette affaire a déclaré avoir constitué une société aux Seychelles où il devait également installer un serveur informatique. Le procès est prévu en septembre 2008.

***Il Sole 24 Ore* du 9 juin 2008.**

(1) Robinson est membre du chapitre Hells Angels de Vancouver.

Propositions

- *Création d'une autorité de régulation sur les jeux et les paris, chargée de l'ensemble du secteur, en ligne ou pas. Cette autorité pourrait disposer des moyens de l'actuelle section « Courses et jeux » des Renseignements généraux (RG).*
- *Instauration d'un système de licences.*
- *Identification des actionnaires des sociétés obtenant une licence mais également de l'ensemble des partenaires, des sous-traitants et des employés.*
- *Obligation que les serveurs des sites soient accessibles sur le territoire national.*
- *Obligation de déclaration de soupçon portant sur le sujet (le joueur qui parie beaucoup d'argent) ou l'objet (les flux inhabituels de mises sur un événement sportif particulier).*
- *Partage d'informations au niveau européen sur la corruption des sportifs (voir l'affaire du jockey britannique exclu des champs de courses du Royaume-Uni mais pouvant courir en France).*
- *Limitation, lors de tournois, à l'accès aux sportifs et instauration d'une sorte de « délit d'initié » sportif.*
- *Mise en place d'un partenariat avec les fédérations sportives pour détecter des résultats sportifs « anormaux ». Cette détection pourrait être comparée au flux de paris sur l'épreuve considérée.*
- *Possibilité de bloquer des joueurs touchés par l'addiction soit par l'adresse IP soit par ses coordonnées de cartes bancaires (ayant conscience cependant que cette barrière est relativement facilement franchissable).*
- *Distinction entre sites avec licences et sites sans licences : on avertit le joueur potentiel qu'il risque d'être victime de fraude sur des sites illégaux non-certifiés.*

La dimension technique : informatique, internet et jeux en ligne

La criminalité liée aux jeux d'argent et de hasard sur internet

Jeux truqués, blanchiment d'argent, *phishing*, détournement de comptes, vols d'informations bancaires et personnelles, *spam*, etc. Les fraudes liées aux jeux d'argent et de hasard sont nombreuses et majoritairement contrôlées par le crime organisé.

Depuis l'apparition des premiers casinos en ligne, les organisations criminelles ont rivalisé d'ingéniosité pour développer à une échelle industrielle des systèmes de fraude complexes destinés à atteindre deux objectifs principaux, le blanchiment d'argent et la manipulation des jeux pour pirater les comptes bancaires des internautes.

Au début de l'année 2006, de nouveaux *bots*(1) sont apparus sur le Net. Ces programmes sont principalement diffusés sur les sites de communautés de joueurs et des *spams* les incitent à télécharger des utilitaires censés aider les joueurs. Les ordinateurs infectés participent sans l'intervention de leur propriétaire à des parties de poker en ligne sur des sites de jeux ciblés. Les malfaiteurs sont désormais passés maîtres dans l'art d'organiser des jeux avec des participants virtuels qui perdent systématiquement au profit du pirate.

Certains casinos suggèrent aux joueurs qui suspectent la présence d'un *bot*, de lui envoyer un message instantané dans la mesure où les robots ne peuvent techniquement pas participer à des conversations en ligne. Mais les malfaiteurs ont trouvé récemment une parade et les *bots* répondent désormais qu'ils ne « chatent » pas...

Le piratage des comptes bancaires se fait à deux niveaux, soit les internautes sont inscrits sur des sites de jeux en ligne et leurs coordonnées bancaires sont enregistrées dans la base de données des serveurs, soit la récupération des informations personnelles se fait de manière « traditionnelle », c'est-à-dire en utilisant des leurres *(phishing)* ou des *keyloggers*(2) qui enregistreront les données de l'utilisateur pour les transmettre au pirate.

(1) Un *bot* est un agent logiciel automatique ou semi-automatique qui interagit avec des serveurs. Il se connecte et interagit avec le serveur comme un programme client utilisé par un humain, d'où le terme *bot*, qui est la contraction de « robot ». On les utilise principalement pour effectuer des tâches répétitives que l'automatisation permet d'effectuer rapidement. Ils sont également utiles lorsque la rapidité d'action est un critère important, avec par exemple les robots de jeu ou les robots d'enchères, mais aussi pour simuler des réactions humaines, comme avec les *bots* de *chat* (Source Wikipedia).

(2) Logiciel qui permet d'enregistrer la frappe sur les touches du clavier et des copies d'écran à distance, les informations sont ensuite transférées au pirate qui les utilise à des fins malveillantes.

En avril 2006, l'éditeur d'antivirus finlandais F-Secure a détecté un *rootkit*[1] diffusé sur le site CheckRaised.com regroupant une communauté de joueurs de poker en ligne.

En accédant grâce à ce logiciel malveillant aux ordinateurs des joueurs, le pirate visualisait leur jeu en temps réel et organisait des parties dont il était l'unique gagnant. Quelques semaines plus tard, Betfair Poker publiait sur son site un avertissement à l'intention des utilisateurs les informant de la circulation d'un pourriel[2] qui tentait de rediriger les joueurs de poker vers un site internet qui, s'il était consulté, téléchargeait un cheval de Troie sur leurs ordinateurs afin d'en prendre le contrôle à distance. Comble de l'ironie, le pourriel en question suggérait la lecture d'un article du site de la BBC relatant le fait qu'un *spam* sur Betfair circulait sur la toile.

Le *phishing*

Plus lucratif que le trafic de stupéfiants depuis 2005 selon le FBI, c'est une activité florissante exploitant la crédulité des internautes.

Le *phishing* est un mode d'attaque qui allie technique et *social engineering*[3] pour monter des escroqueries financières. Un faux site web imitant souvent à la perfection celui d'une banque est transmis à un internaute *via* un e-mail frauduleux qui va l'inciter à donner des informations confidentielles sur son compte bancaire et son identité. Désormais les leurres reproduisent les sites des casinos les plus populaires pour tromper les joueurs et collecter leurs informations personnelles.

Les e-mails étant des leurres, ils sont utilisés pour pêcher des mots de passe et des coordonnées bancaires des utilisateurs dans les mers profondes d'internet. Ce terme était employé en 1996 par les pirates qui subtilisaient les mots de passe des comptes utilisateurs d'AOL. Ces comptes piratés étaient appelés *phish*[4], en 1997 ils devinrent une monnaie d'échange entre pirates qui échangeaient quelques comptes contre un programme ou un logiciel dont ils avaient besoin.

Au fil des ans, les attaques de *phishing,* dont l'objectif était de dérober des numéros de compte AOL, se sont muées en une sinistre entreprise criminelle et, à partir de 2003, les principales banques américaines, anglaises et australiennes avaient déjà subi plusieurs attaques.

(1) Ensemble de programmes malveillants manipulés à distance par un pirate informatique.

(2) Le pourriel ou *spam* désigne une communication électronique non sollicitée.

(3) *Social engineering* : obtention d'informations plus ou moins confidentielles dans le but de les exploiter en vue d'une attaque informatique. L'approche se fait « physiquement », le malfaiteur entre en contact et se lie d'amitié avec des personnes travaillant sur le site de la cible en organisant une rencontre fortuite dans un café, salle de sport, etc. Lorsque la confiance s'installe, les langues se délient.

(4) Il est courant, dans le milieu des pirates informatiques, de changer le « f » pour un « ph ».

À présent, les organisations criminelles et mafieuses ont déployé des techniques sophistiquées de *phishing* et de *malwares* (1) pour subtiliser les comptes des joueurs en ligne, organiser et manipuler des parties de poker. Selon les objectifs fixés, les parties sont programmées pour perdre ou gagner et permettent de transférer de l'argent sale sur un compte bancaire ouvert dans un paradis fiscal selon des montages complexes impliquant de multiples niveaux d'intermédiaires. Il est à craindre que dans les prochains mois l'attention des malfaiteurs ne se focalise sur la conception de *malwares* ciblant les casinos licenciés. Les attaques de déni de service distribué DDoS (*Distributed denial-of-service*) seront certainement employées pour extorquer des sommes exorbitantes aux opérateurs, comme cela avait été le cas en 2004.

En 2007, le site Fulltiltpoker.com aurait subi une attaque lancée par un *botnet* et aurait été dans l'obligation de rembourser les joueurs floués. Selon *USA Today*, 2,5 à 3,5 millions de dollars seraient blanchis de cette manière chaque année.

Les attaques de déni de service distribué

En juillet 2004, la police russe accuse un gang de hackers d'avoir lancé des attaques de déni de service sur 9 entreprises anglaises, principalement des sites de paris en ligne. Selon l'*Associated Press*, les pertes s'élèveraient à environ 40 millions de livres sterling. Le ministère de l'Intérieur russe a informé les journalistes que le gang demandait le versement de rançons de 50 000 dollars pour stopper les attaques. De plus en plus d'entreprises subissent des tentatives d'extorsion de fonds, sous la menace d'attaques de déni de service dirigées contre leurs serveurs. 6 000 à 7 000 d'entre elles ont d'ailleurs cédé à la pression des malfaiteurs, mais ce chiffre pourrait être loin de la vérité, les victimes ne souhaitant pas de publicité néfaste à leurs entreprises. En mars 2004, les 20 sites de paris en ligne les plus importants en Angleterre ont subi 33 attaques de déni de service en l'espace de 15 jours.

Bien que tout porte à croire qu'il s'agisse d'actions menées par la mafia russe, selon les enquêtes du FBI et des services de renseignements britanniques, des hackers indépendants russes utilisent aussi ces méthodes pour leur propre compte (2).

Le DDoS représente l'attaque principale opérée par les *botnets*. L'opération est simple et imparable : l'ordre émanant du pirate indiquera de lancer des requêtes simultanées à une même cible. C'est comme si un standard téléphonique de 100 lignes recevait 100 000 appels au même instant, il lui serait impossible de résister à une telle surcharge et il tomberait immédiatement en panne. C'est ce qui se passe pour les serveurs, le nombre de requêtes étant largement supérieur à leur capacité de réception, le crash est inévitable et le temps nécessaire à la réparation peut varier de quelques heures à plusieurs jours.

(1) Code malveillant.

(2) Sources : Dan Ilett - ZDNet UK.

Au-delà des effets pénibles produits, les conséquences financières sont considérables dès lors que le site ciblé est à vocation commerciale. Les organisations criminelles ont mis en place un système de chantage au DDoS pour rançonner les entreprises qui vivent du commerce en ligne. Les Anglais en ont fait les frais particulièrement avec les sites de bookmakers (1) dont les pertes abyssales ont contraint les plus virulents à céder au chantage financier. La *National High-Tech Crime Unit* (NHTCU) de Grande-Bretagne affirme que ces attaques sont l'œuvre du crime organisé, les amateurs n'étant pas équipés pour un acte d'une telle ampleur. En fonction des événements de l'actualité (notamment sportive comme la coupe du monde de football ou l'*American Super Bowl*), les menaces d'attaques sont plus élevées.

Début 2004, un bookmaker anglais souhaitant conserver son anonymat a reconnu que son entreprise avait subi plusieurs attaques. Le gang utilisait le service contact clientèle du site internet pour communiquer anonymement. Les malfaiteurs menaçaient de créer des pannes sur ses serveurs en lançant des attaques de déni de service s'ils ne recevaient pas une rançon dont le montant variait de 10 000 à 30 000 livres sterling.

L'extorsion en ligne fonctionne parce que ce procédé est très rentable et représente un risque pénal relativement faible. Selon Alan Paller du *SANS Institut Conference* de Londres, 6 000 à 7 000 entreprises payent une rançon. Tous les sites de paris en ligne sont victimes d'extorsion et payent. Les prix augmentent aussi et ils sont passés fin 2004 à environ 40 000 dollars. Il y a fort à parier que cette méthode connaîtra un développement sensible prochainement.

Blue Square, l'un des plus grands bookmakers anglais, a reconnu avoir été la victime de ce chantage après que ses serveurs eurent été attaqués par un déni de service massif suite à un odieux chantage. L'organisation criminelle lui avait ordonné de payer la somme de 7 000 euros faute de quoi des e-mails contenant des images pédophiles seraient envoyés à tous ses clients de sa part. L'insupportable appel téléphonique a été immédiatement suivi d'un déni de service de plus de 5 heures, selon la BBC, en provenance de PC compromis situés en Amérique du Sud. L'attaque a été suivie d'un e-mail émanant de Serbie confirmant le montant de la rançon et précisant qu'en cas de refus, la prochaine charge serait plus puissante donc plus longue.

Tracer les criminels

Jusqu'en 2006, on pouvait détruire un *botnet* en supprimant le poste de contrôle et de commande du pirate que l'on tentait de retrouver plus ou moins aisément. Aujourd'hui, et ce depuis l'apparition d'une nouvelle forme de *botnet* dont Storm Worm conçu par la tristement célèbre organisation criminelle *Russian Business Network* (RBN) au début de l'année 2007, il se propage sur les réseaux pair-à-pair (peer-to-peer). Le système pair-à-pair permet de nommer un ensemble constitué des utilisateurs (en nombre pas forcément défini, ni fixe, mais plutôt de

(1) Les bookmakers sont des individus qui organisent et gèrent les paris de toute sorte qu'ils soient sportifs ou qu'ils portent sur le vainqueur d'élections présidentielles, le sexe du futur bébé d'une star, etc.

manière générale), du protocole qui leur permet de communiquer (Gnutella, BitTorrent, CAN, etc.) et du fonctionnement du protocole entre ces machines. Le terme de réseau pair-à-pair permet de désigner les machines et leur interconnexion à un moment donné, avec un nombre défini de machines/utilisateurs.

Dans un système pair-à-pair, les postes utilisateurs ne jouent pas exclusivement les rôles de client ou de serveur mais peuvent assurer parallèlement les deux fonctions. Ils sont en effet simultanément clients et serveurs et jouent aussi le rôle de routeur, en passant les messages de recherche voire les données vers leurs destinataires. Cette architecture réseau permet ainsi aux *botnets* de se déployer sans qu'il soit possible de localiser le poste de contrôle et de commande principale ; chaque ordinateur infecté étant un porteur du virus indépendant, si un poste est supprimé, un autre prend immédiatement la relève.

À ce jour, il n'a pas été possible de quantifier précisément le nombre de postes compromis par Storm, mais on évalue le *botnet* à plusieurs millions de machines. Aucune parade n'a été mise en place et les experts en sécurité des systèmes d'information affirment qu'aucune forme de protection disponible actuellement ne pourrait stopper une attaque de déni de service lancée par Storm. Au vu des enjeux financiers, les casinos et sites de paris en ligne seraient bien en difficulté s'ils devaient faire face à des tentatives d'extorsions et des menaces de DDoS.

Les casinos non licenciés prolifèrent actuellement dans des pays à faible régulation ou dans des micronations comme Sealand, cette « île métallique » construite durant la Seconde Guerre mondiale afin de défendre le Royaume-Uni contre les attaques aériennes et rachetée par un excentrique britannique en 1967.

Celui-ci a eu l'idée de génie de créer son propre État puisque l'île se situait en dehors des eaux territoriales britanniques. Deux récents jugements ont confirmé la légalité de cet État et ce, en dépit de la forme peu commune de l'île. De telles décisions de justice nous font nous poser un certain nombre de questions : les mafieux ne vont-ils pas construire des fausses îles un peu partout, afin d'échapper aux juridictions ?

En attendant, la principauté de Sealand propose d'héberger tous les sites (sauf ceux ayant trait à la pédophilie) pour permettre à leurs détenteurs d'échapper à toute forme de réglementation. De plus, les *phishing* de casino émanent principalement de serveurs hébergés par ces micronations qui représentent une véritable aubaine pour tous ceux qui souhaitent tirer profit de l'ouverture du marché des casinos et sites de paris en ligne.

Blocage des adresses IP des sites non licenciés

Le souhait émis récemment de bloquer les adresses IP des sites non licenciés ne peut être une solution applicable en raison des techniques de fast-flux DNS qui permettent d'attribuer des milliers d'adresses IP à un même nom de domaine.

Le système fonctionne de la façon suivante. Un individu possède un site dont le nom de domaine est par exemple www.mon-casino.com et pour que les internautes puissent s'y connecter, il faudra lui attribuer une adresse IP, par exemple 80.246.10.132. Il est possible de bloquer cette adresse IP pour que personne ne puisse s'y connecter. Pour éviter une saturation en cas de connexions multiples, les malfaiteurs utilisent une technique parfaitement légale de répartition de charge de serveurs DNS (1). À la seule différence qu'au lieu d'effectuer cette répartition de charge sur des serveurs DNS, ils vont utiliser leurs *botnets* et les milliers d'ordinateurs infectés pour attribuer autant d'adresses IP à leur nom de domaine. Ces IP seront alors celles des ordinateurs compromis des utilisateurs qui ignorent totalement l'activité se déroulant sur leurs machines. Cela permet ainsi de changer l'adresse IP toutes les 3 minutes : une fois l'adresse IP du site sera localisée en France, une autre fois en Suède ou en Chine. Le fast-flux DNS est une technique qui évite aux malfaiteurs de se faire localiser et leur offre une redondance optimale. Les utilisateurs dont les ordinateurs serviront d'émetteurs d'adresses IP seront aussi bien utilisés pour les campagnes de *phishing* que comme joueur zombie dans une partie truquée.

Blocage des adresses utilisateurs

Il sera tout aussi difficile de parvenir à bloquer les adresses IP des utilisateurs pour prévenir les problèmes d'addictions ou de fraudes éventuelles. Cela indépendamment des sites licenciés qui auraient installé un système d'authentification permettant de garantir l'identité du joueur, puisque celle-ci ne saurait être liée qu'à une seule adresse IP. Le joueur voudra se connecter depuis son domicile, sa résidence secondaire, chez ses amis, en vacances, etc. L'utilisation de proxies (sites intermédiaires qui permettent à l'internaute de rester anonyme) sera optimisée pour leurrer les opérateurs, le nombre d'abonnement peut aussi être augmenté (par exemple un abonnement chez Orange et un autre chez Free), et offrir les garanties exigées sur l'identité du joueur.

Fraudes liées aux joueurs

Les innombrables forums sur les jeux en ligne font état de nombreuses victimes de fraudes. Elles concernent principalement le piratage des comptes d'utilisateurs inscrits dans des établissements financiers comme Netteler. En septembre 2006, un internaute français a eu son compte chez Neteller entièrement vidé par plusieurs virements effectués en moins de 4 minutes au profit du site 10Bet, alors qu'il était à son bureau et dans l'impossibilité de se connecter (2). Deux autres joueurs sur ce forum ont été victimes du même problème de virement depuis leur compte Neteller vers celui de 10Bet. Quatre autres utilisateurs ont témoigné des mêmes faits sur le forum du site princepoker.com :

(1) Serveurs de noms de domaine.

(2) Source : forum du site clubpoker.net.

NETELLER - Cher membre NETELLER,

You have successfully transfered funds from your NETELLER account to a registered NETELLER merchant. 03 : 20 PM 31/08/2006

Total transferred to merchant : 100.00 USD

Please keep this e-mail for your records.

Should you have any questions or feel you have received this e-mail in error, please contact NETELLER Customer Service, available 24 hours a day.

Thank you for choosing NETELLER.

Cordialement,

Le Service à la clientèle NETELLER

support@neteller.com

Numéros de téléphone du Service à la clientèle NETELLER

Veuillez contacter votre fournisseur de service téléphonique local pour connaître les coûts éventuels des numéros 800.

En mai 2008, des joueurs indiquent sur le forum du site sos-casino.monforum.com des problèmes de règlement de la part de plusieurs casinos en ligne. Un utilisateur tente depuis plusieurs mois de récupérer les 7 000 dollars gagnés sur le site walkerpoker.com sur son compte Neteller, le site semble trouver toutes les excuses possibles pour retarder le virement.

Cotedazurpalace.com, casinoriva.com, casino-vendome.com, casinodelrio.com, cameocasino.com, casinolux.com et casinotreasure.com sont également signalés sur le forum de commentcamarche.net pour leur mauvaise volonté à payer les gagnants. Les systèmes de bonus selon lesquels le joueur peut doubler sa mise ou se voir offrir des jetons d'une valeur variant de 100 à 300 euros sont en fait des leurres car les clients ne peuvent pas les monnayer s'ils veulent se retirer du jeu. Le règlement des bonus est en principe inscrit sur chaque site mais il n'est pas clairement indiqué alors que les incitations à l'obtention de ces bonus sont permanentes et souvent mises en valeur par des fenêtres pop-up. Un internaute explique ainsi qu'après avoir voulu retirer les 99 euros gagnés au jeu, le site l'a informé que les gains n'étaient accessibles qu'aux joueurs ayant misé un minimum de 550 euros. Un autre a été débité de 1 000 euros sur sa carte visa sans explication par cotedazurpalace.com.

Les versions de démonstration sont trompeuses, la majorité des sites propose aux internautes de tester les plates-formes de jeu, un joueur a expérimenté le jeu en réel après avoir gagné plusieurs parties sur la version de démonstration. Il a perdu l'intégralité de sa mise. Ce test a été effectué lors de la rédaction de ce rapport. Il s'avère que sur certains sites, la version de démonstration est pratiquement toujours gagnante, ce qui semble difficile à croire dans la réalité.

Les sites ladbrokes et casino770, yatching-casino et casino.com ont été testés en juin 2008. Il s'avère que les machines à sous font toujours gagner les joueurs dans les démonstrations. Les deux premiers casinos doublent la mise au cours des 10 premières minutes de jeu (sur chaque machine à sous testée, soit un minimum de 4 machines par site), avec le troisième, 50 % de la mise a été remportée au bout de 15 minutes. Le dernier qui demandait à l'internaute une inscription avant de jouer, a accepté un faux nom, une fausse adresse, les États-Unis comme pays d'origine (alors que la connexion venait de France) et un faux numéro de téléphone. Il est nécessaire d'informer largement les internautes des risques liés à ces casinos non licenciés.

Autre problème, l'envoi de *spams* ciblés aux utilisateurs. En avril 2008, un psychiatre fait état d'une patiente récemment « accrochée » au poker qui a dépensé 27 000 euros en trois mois. La jeune secrétaire a tenté d'arrêter de jouer mais reçoit quotidiennement des *spams* exclusivement dédiés au poker. Devant la tentation permanente (un peu comme si on offrait des verres de vin à un alcoolique), elle a de nouveau cédé et sa dette atteint aujourd'hui 35 000 euros.

Répression

Le volet « répression » est du ressort du ministère de l'Intérieur. La loi a été actualisée le 5 mars 2007 et ne concerne que les jeux en ligne.

Sont ainsi prévues :

• une approche judiciaire : incrimination de la publicité, alourdissement des peines ;

• une approche administrative : faire pression sur les intermédiaires techniques (fournisseurs d'accès) et financiers (banques). Dans cette perspective, deux obligations ont été retenues :

– pour les fournisseurs d'accès : informer l'internaute sur l'illégalité des sites de jeux. À noter que des directives européennes empêchent les États d'imposer des contraintes exorbitantes aux fournisseurs d'accès, comme celle de fermer un site ;

– pour les banques : la nécessité de bloquer les gains issus des sites illégaux.

D'autres moyens sont utilisés :

• face aux sites illégaux qui sponsorisent des manifestations sportives : l'annulation de la manifestation ;

• lorsque le compte bancaire utilisé par site est domicilié en France : la saisie ou le blocage des intérêts du site.

Annexe

Annexe 1 : extraits d'une note officielle émanant d'un pays voisin de la France (1)

(police judiciaire...)

POLICE JUDICIAIRE NOTE DE SERVICE
xxx

Numéro d'émission **xxx**
xxx Date d'émission (mai 2008)

Destinataire(s) ► Monsieur le Directeur xxx
► xxx
Copie: ► xxx
► xxx

OBJET Détection de menaces – 'explosion' d'ouvertures d'établissements de paris sportifs : *background organisations criminelles et terroristes/radicales*
Référence(s)
Chargé de dossier xxx

Ces derniers mois, la ville de XXX notamment a vu fleurir sur son territoire divers établissements de paris sportifs. Nos informations dans le Milieu XXX font apparaître que certains sujets originaires des Balkans auraient repris des établissements de ce type.

D'autre part, il est clair que le Milieu des jeux et paris est un terrain propice sur lequel les organisations criminelles aiment développer une partie de leurs activités. Nous avons donc entamé quelques vérifications. Ce qui suit ne se veut pas une analyse complète et exhaustive. Toutefois, nous pouvons d'ores et déjà affirmer que **tous les signaux d'alerte pouvant laisser présumer d'une activité criminelle organisée** se sont allumés au fur et à mesure de l'avancement de nos vérifications.

1. volet 'XXX'

L'un des établissements le plus visible à XXX est le XXX situé rue XXX. En réalité, il s'agit d'un établissement dépendant de ***BETTING xxx*** créée en avril 2006 dont l'activité déclarée est l'organisation de jeux de hasard et d'argent.

Outre l'établissement de XXX, existe un établissement du même type à XXX ainsi qu'un à XXX (ouverture XXX) Bd XXX. XXX signale un quatrième établissement à XXX dont on ne nous a pas parlé. Parallèlement à ceux-ci existent deux ***xxx*** franchisés sur XXX soit rue XXX et Place XXX.

Dans l'établissement XXX, nous rencontrons le 'patron'. Il s'identifie à

► **B...**, de nationalité marocaine, né à XXX
L'intéressé est très bien connu et a été libéré de xxx le XX-05-2006 suite à une condamnation pour infraction à la législation des stupéfiants. Les autres condamnations remontent aux années 90 (prostitution, coups, menaces, destructions, abus de confiance, faux et/ou usage, recel, vols...)

Interrogé sur l'origine de son personnel, il apparaît qu'un employé, originaire des Balkans soit le bien connu :

(1) Les éléments permettant identification en ont été supprimés, s'agissant d'une enquête en cours.

►**R...**, de nationalité croate, né à XXX
Dlié xxx depuis mars 2008
L'intéressé est bien connu pour des faits d'infractions en matière d'explosifs, abus de confiance, stups, menaces, armes, vols, coups etc.

Selon COFACE, **B...** est directeur général de ***BETTING XXX.*** L'intéressé s'épanchera sur ses déboires avec l'un de ses associés, le nommé :

► **K...**, de nationalité norvégienne, né à XXX
Dlié xxx
Bien connu pour des faits de blanchiment d'argent, loteries, jeux, infractions concernant les instruments financiers, exploitation de la débauche, stups, publicité pour services sexuels etc.

On rappellera que le nom de **K...** était déjà associé à celui, bien connu également, de **Z…** dans l'ouverture d'un établissement du même type à XXX rue XXX. Cet établissement est toujours actuellement ouvert L'établissement, qui fait débit de boissons également, est bien géré par :

► **Z...**, de nationalité marocaine, né à XXX
Dlié xxx
Connu pour vente de stupéfiants, menaces d'attentat, abus de biens sociaux, organisation criminelle, milice privée etc. L'intéressé est en attente de jugement pour des faits d'association de malfaiteurs, infraction à la législation sur les stupéfiants, ébranlement du crédit de l'Etat.

Parmi les autres associés de la ***BETTING xxx,*** on retrouve notamment

► **P...**, XXX, né à XXX
Il est connu pour abus de biens sociaux, escroqueries, détournement ou destruction, faux, coups etc.

Revenons maintenant aux deux enseignes **xxx** franchisées de xxx et de xxx. Le gérant de ces établissements n'est autre que :

► **B...**, de nationalité italienne, né à XXX
Dlié xxx
L'intéressé est patron de divers établissements (dont le XXX) et est bien connu pour stups et armes...

2. volet EURO/xxx xxx

Nous passons alors au contrôle de l'établissement à l'enseigne La Taverne XXX située XXX. Le café dépend en fait de la ***xxx*** créée le XX-10-2007 dont le patron est

► **E.…**, de nationalité macédonienne, né à XXX
Dlié xxx
Dit '***XXX***' dans le Milieu. Il est archi-connu pour vols qualifiés, extorsion, détention arbitraire, vols violence etc.

Plusieurs établissements de paris, dont celui-ci, dépendraient d'une société ***EURO xxx*** :

Les recherches en XXX nous permettent de découvrir qu'il s'agit en fait de la ***xxx EURO xxx*** dont la faillite a été prononcée par le Tribunal de commerce de XXX le XX-04-2008. Le conseil d'administration est (était ?) composé de :

► **K...**, de nationalité turque, né à XXX
Dlié xxx
Il est connu pour coups et blessures, stupéfiants, sûreté de l'état (des documents de propagande du PKK ont été découverts à l'occasion d'une perquisition chez lui suite à la saisie de 58 kg de cocaïne dans un container en provenance du Chili), faillite frauduleuse, faux etc.

EURO xxx n'existe plus. Approchons dès lors **TOP xxx** :

Il s'agit d'une société constituée et immatriculée en janvier 2005 et occupant de 10 à 19 personnes dont l'activité est l'organisation de jeux de hasard et d'argent. Le conseil d'administration est composé de :

► **K...**, de nationalité turque, né à XXX
Dlié xxx
L'intéressé est très connu pour **sûreté de l'état** (lié à xxx et à l'activisme kurde), milice privée, traite des êtres humains, coups et blessures, abus de confiance. Il est le frère de **XXX** (*cf* ci-dessus).

► **K...**, de nationalité turque, née à XXX
Dliée xxx
L'intéressée est connue **sûreté de l'état**, traite des êtres humains en vue de leur exploitation économique...

Toujours du milieu *Balkans* XXX, nous savons qu'un autre établissement de ce type a également été ouvert rue XXX. Il s'agit également d'un établissement 'couplé' débit de boissons et paris sportifs. Le gérant en est :

► **A...**, macédonien, né à XXX
Dit '***XXX***', L'intéressé fait actuellement l'objet du dossier xxx pour organisation criminelle, trafic international de stupéfiants, infractions à la loi sur les jeux de hasard, armes et vols organisés.

(etc., sur 7 pages...)

Eric Woerth, ministre du Budget, des Comptes publics et de la Fonction publique, a confié, en février 2008, au criminologue Alain Bauer, une mission d'étude préparatoire à l'ouverture maîtrisée du marché des jeux sur Internet. L'objectif de cette mission portait sur une évaluation des menaces criminelles qui pourraient résulter de cette ouverture et sur la formulation de recommandations.

Selon les estimations d'un rapport du CERT-LEXSI, l'activité illégale des jeux en ligne représentait en France, en 2005, entre 300 et 400 millions d'euros annuels de produit brut des jeux, alors que l'activité légale de la Française des jeux et du Pari mutuel urbain sur Internet ne représentait que 110 millions d'euros. Cela signifie qu'environ 75 % de l'activité des jeux à distance en France est actuellement illégale.

Alors que le rapport Durieux avait fixé les contours d'une ouverture maîtrisée, il était nécessaire de s'interroger sur la criminalisation du jeu en général, et sur Internet en particulier, notamment au regard des enjeux financiers et légaux soulevés. Après audition de différents acteurs professionnels et de policiers européens, il revenait à la mission présidée par Alain Bauer, de proposer dans son rapport les voies et les moyens d'y remédier.

Cette étude a été réalisée avec le concours du Département de recherche sur les menaces criminelles contemporaines (DRMCC) de l'Institut de criminologie de Paris. Y ont participé : Laurence Ifrah, criminologue spécialisée sur les menaces Internet, Noël Pons, conseiller au service central de prévention de la corruption, Stéphane Quéré, criminologue, et Xavier Raufer, directeur des recherches au DRMCC.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

La Documentation française
29-31, quai Voltaire
75344 Paris Cedex 07
Téléphone : 01 40 15 70 00
Télécopie : 01 40 15 72 30
www.ladocumentationfrancaise.fr

Prix : 7 €
ISBN : 978-2-11-007904-6
ISSN : 0981-3764
DF : 5RO19240
Imprimé en France

9 782110 079046