Université Libanaise
Faculté de Droit et des Sciences
Politiques et Administratives
Filière Francophone

Les lois pénales à l'épreuve des moyens d'escroquerie

Mémoire pour l'obtention du DEA
en Droit interne et international des affaires

Préparé par

Sally Abou Nasr

Membres du jury:

M. le Professeur Abboud AL SARRAJ	**Directeur**
Dr. Randa EL FAKHRY	**Membre**
M. le Professeur Wissam GHAYAD	**Membre**

2017

«L'université n'entend donner aucune approbation, ni improbation aux opinions émises dans ce mémoire. Celles-ci doivent être considérées comme propres à leur auteur».

Dédicace

Je dédie ce mémoire à mon défunt père et à ma chère mère pour leurs sacrifices sans limites, leurs encouragements continus et leur amour. J'espère qu'ils seront toujours fiers de moi.

A mon Cousin bien aimé, à mes amis et à tous ceux qui m'ont soutenue tout au long de mon parcours et m'ont donné la force de continuer.

Que ce travail soit l'accomplissement de leurs vœux et le fruit de leur soutien infaillible.

REMERCIEMENTS

Je voudrais exprimer toute ma gratitude à mon directeur de mémoire le Professeur Abboud Al Sarraj pour sa disponibilité, son aide précieuse et ses encouragements permanents.

Je tiens également à remercier Dr. Randa el Fakhry pour toutes ses remarques et commentaires bienveillants qui m'ont poussé à améliorer mon travail.

Je remercie également le Professeur Wissam Ghayad d'avoir accepté d'évaluer mon travail en tant que membre du jury.

Mes remerciements vont également à ma famille pour son support sans faille tout au long de ces années.

LISTE DES ABRÉVIATIONS

Art.	Article
Al.	Alinéa
Art. préc.	Article précité
Bull. crim.	Bulletin criminel
CA	Cour d'appel
Cass.	Cour de cassation
Cass. crim	Arrêt de la chambre criminelle de la Cour de cassation
CCL	Code de commerce libanais
CPF	Code pénal français
CPL	Code pénal libanais
Comm.	Commentaire
D.	Dalloz
Dr.pénal	Droit pénal
Éd.	Édition
Gaz.Pal.	Gazette du Palais
Ibid.	Ibidem **(**au même endroit**)**
Idem	De même
JCP	Jurisclasseur périodique ; la Semaine Juridique
Mém.	Mémoire
Mém. préc.	Mémoire précité
N^{o}	Numéro
Note préc.	Note précitée
Obs.	Observations

Op. cit.	Opus citatum (ouvrage précité)
P.	Page
RSC	Revue de sciences criminelles
Rev.soc.	Revue des sociétés
S.	Sirey
V.	Voir

SOMMAIRE

INTRODUCTION

«Il est aussi facile de se tromper soi-même sans s'en apercevoir, qu'il est difficile de tromper les autres sans qu'ils s'en aperçoivent»[1].

Ce proverbe est pour moitié vrai puisque force est de constater que les moyens mis en œuvre par certains escrocs sous-tendent une intelligence sans égard qui, mise au profit du phénomène criminel, atteint non seulement les gens simples crédules mais vise souvent toutes les couches sociales.

Psychiatres et psychanalystes relèvent que l'escroc «*cherche à éblouir et se faire aimer de sa victime*» pour mieux l'escroquer.

L'escroquerie est donc un interdit sanctionné pénalement qui repose sur un principe de base «la ruse», avec des armes: pouvoir de persuasion, sans scrupule, anonymat, capacité d'adaptation, inspiration de confiance … et qui évolue sur des terrains de chasse de plus en plus variés: courriels, sites de rencontre, sites de petites annonces, loteries, offres de prêt ou bourse d'études…

Souvent qualifiée de «*délinquance astucieuse*» ou «*d'infraction de ruse par excellence*», l'escroquerie constitue un délit original: c'est une appropriation frauduleuse sans emploi de violence, dont le but est de se faire remettre un bien par son propriétaire au préjudice de celui-ci[2].

En effet l'escroc, s'il poursuit au fond le même but que le voleur, à savoir s'emparer du bien d'autrui, il agit d'une manière bien différente. Le voleur appréhende, soustrait et enlève la chose convoitée à la victime alors que l'escroc lui, plus rusé, va provoquer, à l'aide de moyens frauduleux, la remise de la chose désirée par son propriétaire après l'avoir induit en erreur. Notons également que le vol est considéré comme une infraction violente alors que l'escroquerie, elle est une infraction astucieuse.

[1] FR. LA ROCHEFOUCAULD, «*réflexions ou sentences et maximes morales*», (1664), 115.
[2] P. GATTEGNO, «*Droit pénal spécial*», éd. Dalloz 1995, Paris, p.217, nº425.

On ne confondra pas non plus l'escroquerie avec l'abus de confiance. Dans l'abus de confiance la remise de la chose s'effectue régulièrement en vertu le plus souvent d'un contrat et l'infraction n'apparaitra qu'ensuite. Par contre, dans l'escroquerie, la remise de la chose est, comme nous le verrons, provoquée de façon irrégulière par l'escroc.

Partant de ce qui précède, nous dirons que le délit d'escroquerie est un délit spécial: c'est l'exemple type de l'évolution de la criminalité qui, de musculaire ou violente à l'origine, est passée à une criminalité ingénieuse.

La doctrine s'est à son tour intéressée au délit d'escroquerie et en a relevé les maintes spécificités que nous trouvons importantes à souligner pour avoir une idée générale de base sur ce délit hors du commun:

Michèle-Laure Rassat, soulève judicieusement que l'escroquerie suppose l'utilisation astucieuse de moyens frauduleux, de mauvaise foi et par le recours à la ruse, en vue de se faire remettre une chose, par son propriétaire, au préjudice de celui-ci[3].

Michel Veron, souligne à son tour, que l'escroquerie constitue «*l'exemple parfait de la délinquance d'astuce*»[4], puisque l'escroc provoque lui-même la remise, *«après avoir induit en erreur la victime en utilisant des moyens frauduleux*».

Patrice Gattegno, va même jusqu'à qualifier l'escroquerie de « *délinquance astucieuse*», de «*délit multiforme qui s'adapte aux conditions sociales, historiques et techniques du monde*»[5].

Partant de là, Marie-Paul Lucas de Leyssac et Alexis Mihman affirment fermement dans leur ouvrage que l'escroquerie entre dans la catégorie des «*infractions dites complexes (…) dont le développement passe par une pluralité d'actes de nature différente*»[6], vu que sa commission suppose que l'agent ait employé des moyens frauduleux pour tromper sa victime et la conduire à se déposséder en lui remettant l'objet exploité.

---

[3]M-L. RASSAT, «*droit pénal spécial, infraction des et contre les particuliers, droit privé précis*», 5ème éd., Dalloz 2006, Paris, p.137, n^{0}111.
[4]M. VERON, «*droit pénal spécial*», 3ème éd., Sirey Université, 2010, Paris, p.285, n^{0}407.
[5]P. GATTEGNO, op. cit, p.217, n^{0}427.
[6]M-P LUCAS DE LEYSSAC, A. MIHMAN, «*droit pénal des affaires, manuel théorique et pratique*», éd. Economica 2009, Paris, p.44, n^{0}66.

Philippe Conte ajoute à tout ce qui précède, une précision non négligeable selon laquelle vu que l'escroquerie est une infraction de commission, il faut que la sollicitation émanant de l'escroc soit non seulement «*positive*» mais également «*déterminante de la remise faite par la victime*»[7].

De même, la doctrine s'est penchée sur l'étude approfondie de la personnalité criminelle du titulaire de l'infraction et de l'intention criminelle qui l'anime:

A ce propos, Michèle-laure Rassat, évoque l'escroc comme un individu ayant une personnalité originale qui le démarque de la majorité des délinquants. Elle considère que l'escroc est le plus souvent âgé (autour de la cinquantaine) contrairement aux autres délinquants «voleurs» qui sont plutôt jeunes (dans la vingtaine). Mais ce qui différencie, à son sens, vraiment l'escroc des autres délinquants c'est surtout son intelligence supérieure aux autres. En effet l'escroc est capable de faire des plans, il est plutôt prévoyant manipulateur et rusé, au point de dire qu'il a *«l'art de bien jouer la comédie*»[8], et de maitriser son rôle à la perfection.

Face à l'escroc les victimes de son délit sont à classer en deux principales catégories: il pourrait s'agir de certaines «*victimes-coupables*», ou à l'opposé de victimes qu'on pourrait qualifier de «*pitoyables*».

Les victimes sont considérées comme des «victimes-coupables» lorsqu'elles se sont fait escroquer dans des opérations moralement discutables qui constituaient, selon la conviction de la victime, une bonne affaire ayant pour but de l'enrichir.

Les «victimes pitoyables» sont celles qui sont tombées dans les pièges de l'escroc et se sont fait arnaquer pour avoir cru à la mise en scène parfaitement agencée par ce dernier. Ce sont celles qui, déshérités de l'esprit, collaborent sans conscience à ce qui leur est arrivé et qui ne sont pas digne de protection[9].

---

[7]Ph. CONTE, «*Droit pénal spécial*», Manuels, 2ème éd., Paris, 2005, p.317, n^{0}355.
[8]J. LARGUIER, Ph. CONTE, «*Droit pénal des affaires*», 10ème éd., Armand Collin, Paris 2001, p.100, n^{0}118.
[9]L'illustration la plus frappante qu'on peut en donner est celle du mathématicien Michel Charles, collectionneur d'autographes et de manuscrits anciens, qui a acheté au prix de 140 000 francs à un escroc dénommé «Vrain-Lucas» -qui se présente à lui comme mandataire d'un noble- maintes autographes, lettres et manuscrits fripés, rongés sur les bords écrits en vieux français censés être

Mon mémoire comme l'indique son intitulé «*les lois pénales à l'épreuve des moyens d'escroquerie»* aura pour objectif principal l'étude approfondie de l'évolution de l'élément matériel constitutif de l'escroquerie que sont les moyens ou procédés de tromperie, en allant des plus classiques pour arriver aux plus innovateurs, ainsi que l'examen de leurs différentes modalités de répression.

Nous nous intéresserons plus précisément à plusieurs problématiques que cette étude soulève à savoir: d'une part quels sont les procédés ou moyens classiques d'escroquerie, comment sont-ils sanctionnés et quels sont les particularités de leurs poursuites? Et d'autre part quelles sont les moyens innovateurs d'escroquerie et comment les législateurs des différents pays tendent à les réprimer, essayent-ils uniquement de leur étendre le champ d'application des textes incriminant les moyens classiques ou ont-ils la possibilité de recourir à d'autres solutions pour les prévenir et mettre un frein à leur expansion? Existe-t-il des divergences législatives notables entre le droit français et le droit libanais à ce propos?

Le choix de ce sujet de mémoire nous a semblé des plus intéressants au vu de l'émergence de nouvelles technologies, de nouveaux moyens de communications engendrant de nouvelles infractions, non connues auparavant et auxquels certains pays sont incapables de faire face à cause du manque législatif.

L'intérêt de notre mémoire réside donc dans l'étude comparative des deux systèmes français et libanais et dans les solutions que nous pourrions proposer pour pallier au manque législatif que nous retrouvons en droit français et à fortiori en droit libanais.

Partant de ces problématiques nous verrons dans notre première partie qu'il existe un mensonge dans toute escroquerie mais que tout mensonge n'est pas nécessairement constitutif d'une escroquerie. C'est uniquement le mensonge aggravé, suffisamment persuasif pour tromper, qui l'est. Les manœuvres frauduleuses sont considérées comme l'exemple type de mensonge aggravé étant donné qu'elles viennent ajouter au mensonge un fait extérieur: un acte matériel, une mise en scène ou l'intervention d'un tiers, destinés à lui donner force et crédit et à éliminer chez la victime le sentiment de défiance naturel à l'esprit humain.

En outre, un rapide survol de la jurisprudence nous révèlera d'une part la très grande diversité des différents moyens classiques mis en œuvre par les escrocs pour tromper leurs victimes et en obtenir la remise espérée (tromperie par l'usage

---

faits par les plus grandes postures tels que Pascal ,Galilée, Judas, Marie-Madeleine, César et Cléopâtre, Alexandre le Grand, Aristote, Caïn à Abel….

d’un faux nom, d’une fausse qualité, l’abus d’une qualité vraie ou l’emploi de manœuvres frauduleuses) et d’autre part comment l’escroc adapte ces méthodes classiques à la psychologie, à la méfiance ou à l’intelligence de ces victimes. De là, nous verrons que l’escroc est parfois contraint de mettre en place des mécanismes fort ingénieux et très complexe tandis qu’une mise en scène sommaire suffira à tromper des victimes trop crédules.

Nous passerons ensuite en revue les deux autres éléments constitutifs de l’escroquerie, qui doivent exister à côté de l’élément matériel que sont les moyens frauduleux. Ces deux éléments sont d’une part l’élément moral: l'intention de tromper requise dans tous les délits intentionnels et dont l’appréciation relève des attributions exclusives des juges du fond, et d’autre part la cause déterminante des moyens frauduleux: la remise provoquée d’une chose matérielle ou la fourniture d’un service dont le résultat est préjudiciable pour la victime.

Notre analyse révèlera que les moyens classiques d’escroquerie ne sont malheureusement punissables, tant en droit français qu’en droit libanais, que lorsqu’ils correspondent très exactement aux exigences des articles de lois précis quant à la définition des éléments d’escroquerie.

Dans la seconde partie de notre mémoire nous verrons que si les nouvelles technologies de l’information et de la communication constituent d’une part un outil assez profitable par les bienfaits qu'il procure à leurs utilisateurs, ils génèrent d’autre part la multiplication d’infractions nouvelles dont les traces sont facilement dissimulables sur le réseau et qui mettent en cause, voire même en échec, les méthodes classiques d'incrimination et de répression.

Nous démontrerons par conséquence que la diversité des procédés et moyens frauduleux innovateurs imaginés par les escrocs a conduit les législateurs des différents pays à remettre en question l’efficacité de leur législation. Mais que malgré toutes les tentatives d’incrimination il restera toujours de nombreux procédés innovateurs, sans doute malhonnêtes, qui restent impunis du fait qu’ils ne tombent pas précisément sous le coup des dispositions pénales déjà mis en place.

Nous insisterons en outre sur le fait que l’inexistence de lois nationales suffisamment précises régissant ce qu’on appelle les différentes variétés de «cybers-crimes» demeure l'une des réalités communes à tous les états, d’où la nécessité et l’intérêt de rechercher des solutions, tant sur le plan national qu’international, et de renforcer la coopération internationale pour faire face à ce phénomène nouveau de recrudescence de la criminalité liée à l'outil informatique.

Partie 1: La répression des moyens classiques d'escroquerie:

L'escroquerie est une des infractions les plus classiques que l'histoire a connu et qui ne cesse de se développer et de se multiplier au cours des années et des siècles. Il a été dit en ce sens que tant que nous trouvons des hommes rusés nous pourrions toujours parler d'escroquerie.

L'escroquerie, en la simplifiant, peut être expliquée en quelques mots: c'est une façon de s'approprier la chose d'autrui. Or en réalité, cette infraction est beaucoup plus machiavélique, astucieuse et complexe qu'elle n'apparait. En effet, l'auteur de l'escroquerie doit recourir à des ruses afin de pousser sa victime à lui remettre le bien qu'il convoite. Les moyens utilisés dépendent de l'imagination de l'escroc, tant que l'imagination de ce dernier est poussée tant les manœuvres sont plus développées et difficiles à découvrir.

Selon la science de la criminologie, nombreux auteurs se mettent d'accord que la personnalité de l'escroc est bien différente de la personnalité d'autres auteurs d'infractions. L'escroc dispose en réalité d'une intelligence et d'une capacité plus développée que d'autres de planifier les événements afin d'obtenir la remise volontaire de la chose sans pour autant recourir à la force, il n'utilise que son pouvoir de manipulation pour mieux convaincre sa victime.

Nous traiterons donc dans le premier titre de la première partie de notre mémoire des procédés classiques d'escroquerie (Titre 1) pour exposer sous un second titre les modalités mises en place pour les réprimer tant en droit français qu'en droit libanais (Titre 2).

Titre 1: L'analyse des procédés classiques d'escroquerie:

L'escroquerie est clairement définit dans sa conception classique à l'article 313-1 du CPF comme suit: *«le fait, soit par usage de faux nom ou de fausse qualité, soit par abus de qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, et remettre des fonds, des valeurs ou un bien quelconque, à fournir un servir ou à consentir un acte opérant obligation ou décharge»*.

Cette même conception classique est également adoptée, en droit libanais, où le délit d'escroquerie est réglementé par les articles 655 et 656 CPL (loi du 16 septembre 1983). En effet, ces articles disposent que le délit d'escroquerie est constitué en ce qui concerne son élément matériel par «un fait» consistant en moyens frauduleux bien précis, donnant lieu à «un résultat» préjudiciable avec l'existence bien évidemment d'un lien de causalité entre les deux[10].

Mais même partant de ces définitions préliminaires qui n'englobe que les moyens classiques d'escroquerie, au détriment des moyens innovants que nous étudions dans notre seconde partie, nous pouvons d'ors et déjà affirmer que l'escroquerie, tant en droit français qu'en droit libanais, est un délit original, émanant d'un acte positif, qui consiste à utiliser certains moyens par lesquels *«on trompe une personne physique ou morale»*[11], en le déterminant à une remise avec une intention coupable[12].

L'originalité de ce délit résiderait dans l'appropriation frauduleuse que vise l'escroc sans pourtant qu'il lui soit nécessaire de recourir à l'emploi de la violence.

---

[10] محكمة إستئناف جبل لبنان، قرار رقم ١٢٨، تاريخ ٢٠ / ٣ / ١٩٩٦، القرارات الكبرى ١٩٩٦، عدد ٤٢:"قضي بأن يفترض الاحتيال لتوفر عناصره، وجود أركان ثلاثة، يقتضي أن يقوم عليها وهي :١- وجود فعل خداع يتمثل في إعتماد المحتال على المناورات الاحتيالية التي من شأنها تشويه الحقيقة في ذهن المجني عليه وايقاعه في الغلط . ٢- النتيجة التي تترتب على ذلك وهي حمل المجنى عليه على تسليم المال إلى المحتال. ٣- العلاقة السببية بين الفعلين"

[11] P. GATTEGNO, op. cit., p.217, nº425.

[12] علي عبد القادر القهوجي، قانون العقوبات، القسم الخاص، جرائم الاعتداء على المصلحة العامة وعلى الانسان والمال، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٢، ، ص. ٧٦٢

D'où il s'ensuit que le mécanisme de l'escroquerie consiste pour une personne animée par une intention frauduleuse[13]à utiliser des procédés de tromperie dans le but d'induire la victime en erreur et la pousser ainsi à une remise volontaire[14].

Le droit français[15] ainsi que le doit libanais[16] énumèrent quatre catégories de procédés classiques d'escroquerie. Nous passerons donc en revue sous ce premier titre ces procédés classiques à savoir d'une part la tromperie ayant lieu par l'usage d'un faux nom, d'une fausse qualité ou par l'abus d'une qualité vraie (Chapitre 1) et d'autre part les manœuvres frauduleuses (chapitre 2).

Mais le moins que l'on puisse dire de prime abord c'est que le champ d'application des articles français et libanais a été volontairement voulu très large vu l'emploi de l'expression «*manœuvres frauduleuse*s », qui permet d'incriminer toutes sortes de mises en scène.

Chapitre 1: Faux nom, fausse qualité ou abus d'une qualité vraie

Il est évident que pour qu'un auteur devienne escroc il ne suffit pas qu'il s'approprie la fortune d'autrui de n'importe qu'elle façon, mais encore faut-il que ce dernier ait recours à un moyen de tromperie qui fait naitre *«une croyance fausse dans l'esprit de la victime»*.[17]

Il est indispensable donc de prouver qu'une méthode frauduleuse d'escroquerie ait été utilisée par l'auteur pour qu'il y ait condamnation d'escroquerie. En tout cas quel que soit le procédé utilisé comme moyen frauduleux il est impératif que ce moyen ait été en lui- même déterminant de la remise de la chose ou à la fourniture du service ainsi qu'antérieur à celle-ci[18].

[13]M.VERON, op.cit., éd.2010,p. 286, nº407

[14] القاضي المنفرد الجزائي في طرابلس، قرار رقم ١٩٤٦، تاريخ ١٧/ ٥/ ٢٠١١، كاساندر إلكتروني:"يشترط لتحقق جرم الإحتيال توفر الأركان التالية مجتمعة . أولاً : مناورات احتيالية يمارسها المدعى عليه على المدعي، ثانياً : أن تؤدي هذه المناورات إلى قيام المدعي بتسليم المدعى عليه مالاً منقولاً أو غير منقول أو إسناداً تتضمن تعهداً أو إبراء أو منفعة، ثالثاً: أن يقوم المدعى عليه بالاستيلاء عليها"

[15]CPF art. 313-1

[16]CPL art. 655.

[17]J. LARGUIER, Ph. CONTE, op.cit., p.100, nº118.

[18]J.PRADEL, M.DANTI-JUAN, «*Droit pénal spécial, droit commun, droit des affaires*», 4ème éd., Paris, Cujas 2007-2008, p.616, nº870.

Nous étudierons sous ce premier chapitre trois procédés classiques d'escroquerie en s'attardant sur leur définition (Section 1), leurs caractères communs et les illustrations les plus récentes que nous pouvons en donne (Section 2).

Section 1: Définitions et caractéristiques des trois procédés

Nous verrons que le simple mensonge suffit à lui seul comme moyen d'escroquerie lorsqu'il porte sur le nom ou la qualité, et même pour l'abus de qualité vraie, mais il ne suffit pas à lui seul pour constituer une manœuvre frauduleuse comme nous le démontrerons ci-dessus dans le second chapitre de ce titre premier.

Il est intéressant d'aborder dans un premier paragraphe les définitions et caractéristiques des trois procédés classiques d'escroquerie que sont l'usage d'un faux nom, l'usage d'une fausse qualité, l'abus de qualité vraie. Pour nous attarder dans un second paragraphe à leurs caractères communs et les illustrations que nous pouvons en donner (Paragraphe 2).

Paragraphe 1: L'usage d'un faux nom:

L'escroc usurpe un nom auquel il n'a pas droit pour inspirer confiance et tromper sa victime[19]. L'usage d'un faux nom consiste donc dans le fait d'utiliser un nom autre que le sien et de se faire connaitre par ce faux nom[20].

Le faux nom utilisé peut être celui d'autrui, un nom imaginaire telle l'apposition d'une signature apocryphe sur une carte magnétique volée[21], ou un nom que l'on n'a pas le droit de porter.

La jurisprudence constante considère que l'usage d'un faux nom englobe également l'usage de faux nom patronymique, l'usage d'un faux prénom ou d'un faux pseudonyme, à condition que ces derniers entrainent la confusion dans l'esprit de la victime potentielle de l'escroquerie.

A cet égard, et pour tout genre de faux nom, le simple mensonge par le recours à ce faux nom est punissable, peu importe que cet usage soit verbal ou écrit et que le

[19]M. VERON, op.cit., éd.2010, p.286, nº 409.
[20]J.PRADEL, M.DANTI-JUAN, op. cit., p.617, nº873.
[21]P. GATTEGNO, op.cit., p. 217, nº428.

nom soit le nom réel d'un tiers ou un nom imaginaire, et ceci dès lors que le faux nom en question ait été déterminant de la remise.

Il faut noter d'autre part que l'usage de faux nom peut constituer non seulement le délit d'escroquerie mais aussi une autre infraction, indépendamment de toute recherche de remise, qui est l'usurpation d'état civil par la remise de nom d'un tiers expressément prévue par l'article 434-23 CPF.

Pour autant, on constate que ce premier procédé est rarement utilisé seul dans le monde des affaires, on le trouve cependant souvent accompagné d'autres procédés frauduleux qui viennent renforcer son efficacité et constituent une preuve supplémentaire pour convaincre les victimes plus ou moins douteuses que sont les fausses qualités tel l'utilisation de titres nobiliaires ou professionnels.

Paragraphe 2: L'usage d'une fausse qualité ou l'abus de qualité vraie.

Ce n'est qu'avec l'article 313-1 CPF que le procédé d'usage d'une fausse qualité ou même d'abus d'une qualité vraie est devenu distinct et autonome[22] des autres procédés d'escroquerie.

Pour en donner une définition on dira que la fausse qualité est celle que l'on n'a pas ou que l'on n'a plus. Elle peut s'attacher selon les cas à la nationalité ou au titre professionnel (notaire, avocat…), à l'état civil ou à une activité, ou même à une situation sociale (fausse qualité de chômeur).

L'abus en question consiste à user d'une qualité vraie, qui inspire confiance à la victime, mais en le faisant de mauvaise foi et ceci afin d'obtenir des fonds ou tout autre genre d'avantage. Partant de là, la remise provoquée de l'escroc serait faussement reliée à cette qualité.

A l'instar de l'usage d'un faux nom, le simple mensonge suffit dans le cas d'une fausse qualité indépendamment du fait que cette qualité soit réelle ou imaginaire[23] et peu importe que l'usage de la fausse qualité soit écrit ou verbal.

En l'absence de définition légale expresse du terme «qualité» en droit libanais et même en droit français (article 313-1 CPF), nous passerons en revue les maintes

[22]M.VERON, «*Droit pénal spécial*», 6ème éd., Armand Colin, Paris, 1998, p.206.
[23]J.PRADEL, M.DANTI-JUAN, op. cit., p. 617, n°872.

définitions, tout aussi intéressantes les unes que les autres, qu'en donne la doctrine française :

Selon Michel Veron: la qualité s'identifie aux «*éléments de l'état des personnes: qualités, âge, situation matrimoniale, domicile, nationalité, titres, profession*»[24].

L'opinion de Jean Pradel et Michel Danti-Juan, va dans le même sens puisque ces derniers affirment également que la qualité est constituée des éléments de l'état des personnes, et que les escrocs visent en y recourant aux *«tromperies sur l'âge, la situation matrimoniale, le domicile, l'état de père de famille»*[25].

Patrice Gattegno, vient donner une précision pertinente à ce propos: il précise que si la notion de qualité en droit civil englobe l'âge, la situation de famille et la profession, en droit pénal la notion a un sens beaucoup plus large puisque la fausse qualité peut être constituée par «*tout acte de nature à tromper autrui sur sa situation tel son état civil, profession ou sa situation sociale*»[26].

Les tribunaux, tant français que libanais, conscients de l'importance de l'extension du champ d'application de la notion de «qualité», pour que cette dernière englobe toutes les escroqueries possibles et imaginables, en utilisent une conception extensive. Ils estiment ainsi que toute particularité, tout avantage propre à inspirer confiance et à déterminer la remise est synonyme de qualité.

Citons à ce propos deux affaires intéressantes: l'affaire «Helga de la Brache» c'est une escroc suédoise qui a prétendue être la fille cachée du roi Gustave IV Adolphe de suède, et arrive à obtenir suite à ces prétentions un soutien financier de particulier mais surtout une pension royale importante, et l'affaire «Victor Lustig»\ connue également sous le nom de «l'homme qui a vendu la Tour Eiffel » cet escroc se camoufla en fonctionnaire du gouvernement (directeur général, représentant du ministère des PTT[27]) et envoya aux grandes entreprises des invitations pour négocier la vente de la tour Eiffel en tant que «ferraille».

En ce qui concerne le troisième procédé classique à savoir l'abus de qualité vraie, il est important de signaler l'évolution législative qui a eu lieu le concernant.

[24]M. VERON, op.cit., éd.2010,p.287, nº410.
[25]J.PRADEL, M. DANTI-JUAN, op. cit., p.618, nº875.
[26]P.GATTEGNO, op.cit. , p.217, nº429.
[27] Ministère des Postes et des télégraphes

En effet, Avant la réforme du code pénal français, les textes étaient silencieux sur l'existence de ce procédé, c'était la jurisprudence qui le sanctionnait en le considérant comme manœuvre frauduleuse dès lors que son usage était « *de nature à imprimer à des allégations mensongères l'apparence de la sincérité, à commander la confiance de la victime et à la persuader de l'existence de fausses entreprises* »[28].

La Cour de cassation a rendu une autre décision en date du 8 juillet 1986 dans le même sens dans laquelle elle affirme que : « *l'abus d'une qualité vraie, de nature à imprimer l'apparence de la sincérité à des déclarations mensongères, à commander la confiance de la victime et à la persuader de l'existence d'un crédit imaginaire, constitue une manœuvre frauduleuse*».

On en déduit que la jurisprudence française a indirectement assimilé l'abus de qualité vraie à l'usage de fausse qualité.

Aujourd'hui et depuis 1994, l'article 313-1 CPF, a reconnu l'abus de qualité vraie, rendant ainsi ce procédé un procédé de tromperie distinct et autonome de celui de l'usage d'une qualité vraie. Le droit français ne requière également plus l'exigence de la preuve d'une mauvaise foi de l'auteur, mais exige tout de même que cet abus ait été déterminant de la remise.

Il n'existe malheureusement pas en droit libanais un texte équivalent à l'article 313-1 du CPF qui cite clairement l'abus de qualité vraie comme un des procédés d'escroquerie, on se réfère donc plutôt à la jurisprudence comme c'était le cas en France avant 1994 qui va dans le même sens que le droit positif français.

Il faut noter tout de même qu'il y a certains cas où une fausse qualité ne constitue pas nécessairement un élément d'escroquerie, sauf si le mensonge est confronté par des manœuvres tel l'intervention d'un tiers, c'est le cas par exemple du mensonge sur un droit qu'on prétend avoir, par exemple, se prétendre propriétaire[29] ou se prétendre créancier (lorsque l'auteur obtient une somme d'argent en se disant faussement créancier de sa victime), se prétendre faussement mandataire d'une maison de commerce afin d'obtenir une livraison de marchandises par un fournisseur.

[28] فيلومين يواكيم نصر ، قانون العقوبات الخاص ، جرائم وعقوبات ، منشورات صادر ،بيروت , ٢٠٠٩، ص . ١٦٦

[29] Cass.Crim. 4 février 1898, D.1899.I.584

Or, nous trouvons en droit libanais une notion qui n'existe pas en droit français, celle de disposer d'un bien mobilier ou immobilier sans droit ou qualité, ou par un abus du droit[3031], considérée comme une des figures des manœuvres frauduleuses[32]. En abusant de cette situation, l'escroc mène sa victime à lui remette une somme argent, en contrepartie du transfert de propriété du bien[33].

Apres avoir survolé les définitions et caractéristiques des trois premiers procédés classiques nous mettrons en relief leurs caractères communs et en donneront quelques illustrations sous une seconde section (Section 2).

Section 2: Caractères communs et illustrations

Bien que les trois procédés classiques d'escroquerie se différencient les uns des autres il reste qu'ils ont des caractères communs non négligeables (Paragraphe 1) qui apparaissent en passant en revue les illustrations de ces trois procédés (Paragraphe 2).

Paragraphe 1: Caractères communs

L'escroquerie faite en utilisant un faux nom ou une fausse qualité est considérée comme la plus simple, les caractères communs dans ces deux cas d'escroquerie résident dans le fait que le délit doit impérativement être un délit de commission[34]. L'escroc doit adopter une attitude active pour tromper sa victime et être animer par une intention frauduleuse[35].

---

[30] ع. ع.ق.القهوجي، مرجع سابق، صفحة ٧٨٦

[31] تمييز جزائي، غرفة ٦، قرار رقم ٤٥٦ ، تاريخ ٢٩ / ١٢ / ٢٠١٦ ، كاساندر إلكتروني:" لم يثبت من تحقيقات الدعوى ما يثبت على نحو أكيد أنه في تاريخ ابرام إتفاقية البيع... كانت نية المدعى عليهما متجهة إلى خداع المدعي وإبتزاز أمواله إحتيالاً ولا سيما في ضوء ما تقدم و تشابك الدفعات والنزاع حول مصدرها ... لا تكون عناصر الاحتيال متوافرة، ولا يصح القول أن المدعى عليهما قد اقترفا جنحة الاحتيال وأساءا إستعمال ألحق في التصرف بالعقار ، الذي كان لا يزال مسجل على إسم المالك الأول... أو انهما قد تصرفا فيه من دون أن يكون لهما ألحق في ذلك بموجب أي مستند..."

[32] Art.655, al.3, CPL

[33] تمييز جزائي، غرفة ٧ ، قرار رقم ٢٩١، تاريخ ٢٢ / ٩ / ٢٠١٦، كاساندر إلكتروني:" المدعى عليه أقدم على إستغلال صفته المستمدة من قيود السجل العقاري التي كانت لا تزال تظهره كمالك للقسم لأجل التصرف به... عن طريق تنظيم عقد بيع ممسوح به ممتنعاً ... عن رد الثمن... قاصداً جني ربح غير مشروع ... ثبت توافر عناصر المادة ٦٥٥ فقرة ٣ ... التي وسعت مفهوم الاحتيال الذي نص على صورة جديدة تتمثل بأن يقدم من له ألحق أو الصفة في التصرف بمال منقول أو غير منقول على إساءة إستعمال هذا ألحق توسلاً لإبتزاز المال ... أي إساءة لإستعمال ألحق متزامنة مع نية إبتزاز المال ..."

[34] M.VERON, op.cit., éd.1998,p.286, nº408.

[35] P.PRADEL, M. DANTI-JUAN, op. cit., p. 617, nº872.

La règle est donc claire «pas de commission par omission» il faut par conséquence que l'agent s'attribue par un acte positif un faux nom ou une fausse qualité. Mais ce principe est atténué par la jurisprudence lorsque l'agent omet de signaler qu'il n'a plus la qualité requise afin de bénéficier d'un versement de fonds ou d'une remise.

Le droit libanais va dans le même sens en considérant que l'escroquerie est un délit de commission, qui suppose un acte positif, et il en déduit que le silence même de mauvaise foi ne peut être qualifié d'escroquerie.

La cour de cassation libanaise, ne s'arrête pas là, elle va plus loin et précise, à juste titre, que lorsqu'on est en présence de relations commerciales répétées entre deux parties cela rend la qualification d'escroquerie plus difficile[36] [37].

La cour de cassation tant française que libanaise exige, un examen délicat et minutieux des faits, pour qu'il y ait qualification du délit, la preuve du recours aux moyens frauduleux doit toujours être rapportée.

Voici quelques arrêts dans lesquels la cour a nié l'existence du délit d'escroquerie pour manque de preuve de l'existence de ces manœuvres :

L'arrêt récent de la cour de cassation libanaise[38], dans lequel la cour a jugé que le non remboursement d'une somme d'argent n'est pas considéré en lui-même comme un moyen frauduleux. Une autre décision rendue le 13/2/2012, va dans le même sens en éloignant la qualification de manœuvres frauduleuses pour manque de preuves du recours du défendeur à de telles manœuvres lorsqu'il a obtenu une nouvelle puce de téléphone.

[٣٦] تمييز غرفة ٣ ، قرار رقم ٢٦٠، تاريخ ١٨ / ١٢ / ١٩٩٩ :" وحيث أنه طالما هناك معاملات تبادل تجارية بين طرفين فإن صفة جرم الاحتيال ، تنتفي عن بنود هذه العلاقة التجارية ويكون النزاع مدنياً "

[٣٧] تمييز غرفة رقم ٣ ، قرار رقم ١١ ، تاريخ ١٢ / ١ / ٢٠٠٥ ، كساندر إلكتروني :"و حيث يتبين من مجمل الأوراق أن المديونية التي ترتبت هي نتيجة تعامل تجاري منذ العام ١٩٩٣ ولا مجال بالتالي إزاء التعامل التجاري الناتج في بعضه أو كله عن شراء لسيارات لا مجال للقول بوجود جرم الاحتيال الذي يتطلب مناورات احتيالية يقوم بها شخص يوقع الأخر في الخطأ ويدفعه إلى تسليم أموال في حين أن من الثابت أن الطرفين يعرفان تماماً ما يفعلان وأن علاقة تجارية قامت بينهما منذ العام ١٩٩٣"

[38] تمييز جزائي ، غرفة ٣ ، قرار رقم ١١٥ ، تاريخ رقم ٢٩ / ٣ / ٢٠١٢، كساندر إلكتروني

Les tribunaux sont d'autant plus exigeants lorsque l'une des parties au procès est un professionnel qui est supposé être un expert, et donc supposé être difficile à tromper[39].

Un autre point commun que nous pouvons déduire des législations libanaises et françaises est que le simple mensonge est punissable dans les deux délits de faux nom et de fausse qualité, il n'a pas besoin d'être accompagné de faits extérieurs destinés à l'accréditer tel une production d'écrits ni une intervention d'un tiers. Au cas d'existence d'un écrit le droit libanais opte pour le cumul des deux infractions d'escroquerie et de contrefaçon.

En outre les deux droits conditionnent l'existence de la mauvaise foi pour les deux délits par: 1-l'intention de tromper la victime, 2- le fait que l'appropriation du faux nom ou de la fausse qualité se fasse dans le but d'inspirer confiance chez la victime, 3- le fait que la victime soit tomber dans l'erreur à cause de la confiance que l'escroc lui inspire[40], 4- le faux nom, la fausse qualité et l'abus de la qualité vraie doivent avoir été déterminants[41] de la remise[42] [43].

Mais le plus intéressant reste, sans doute, de donner quelques illustrations frappantes de ces trois procédés (Paragraphe 2).

Paragraphe 2: Illustrations frappantes

Nous pouvons citer parmi les exemples de l'emploi frauduleux du faux nom que les juridictions tant françaises et libanaises ont eu à trancher: L'usage de faux pseudonyme à consonance française pour obtenir des aides publiques[44]; le fait de demander à un tiers, à qui on vient de voler la carte de crédit, le numéro de celle-ci

[39] تمييز جزائي، غرفة ٧ ، قرار رقم ٢٤٨ ، تاريخ ١٢ / ٧ / ٢٠١٢، كساندر إلكتروني

[40] فيلومين يواكيم نصر , مرجع سابق,ص.١٦٧

[41] تمييز جزائي، غرفة ٣ ، قرار رقم ١٣٣، تاريخ ١٨ / ٥ /٢٠٠٥، كاساندر إلكتروني:" المدعى عليه... إنتحل إسم... بدل من إسمه الحقيقي وإشترى عقار من المدعي...وأعطاه شيكاً من دون رصيد، ولكن الانتحال لم يكن له تأثير على قبول توقيع عقد البيع... إذاً لا تتوافر عناير جرم الاحتيال "

[42] تمييز جزائي، غرفة ٧، قرار رقم ١٤٦ ، تاريخ ٥ / ٤ / ٢٠٠١ ، كاساندر إلكتروني : "الكذب واقع على صفة المدعى عليه ... إنتحال صفة مهندس من قبل المدعى عليه لم يكن الهدف منه حمل المدعى على تسليمه أموالاً ليستولي عليها بل يرمي إلى الحصول على عقد مقاولة"

[43] Cass.Crim.14 mai 1990, Bull. nº187

[44] Cass.Crim.12 nov.2006, pourvoi nº05-86.765

et retirer de l'argent[45]; ou le fait de payer des marchandises avec des cartes de crédit volées en apposant des signatures apocryphes sur les documents établis par les commerçants[46].

Les exemples les plus retenus sur l'usage de fausse qualité sont au niveau de l'état des personnes, de la profession[47] et de la qualité de mandataire, ou de propriétaire[48].

En effet, quant à l'état des personnes: les mensonges concernant l'âge, la situation matrimoniale[49] (se faire passer pour célibataire et obtenir un prêt de mariage), l'existence ou la nature du lien de filiation, le domicile et même l'usurpation de titres de noblesse ou les titres honorifiques ou universitaires sont les exemples les plus cités. La cour de cassation française dans un arrêt frappant est même allée jusqu'à condamner pour escroquerie un individu qui a prétendu être aveugle pour obtenir le versement d'une allocation[50], ce qu'elle a considéré comme étant une fausse qualité.

Quant à la profession: la liste des fausses professions utilisées par les escrocs pour inspirer confiance est longue. La jurisprudence admet en effet qu'il peut s'agir d'une profession privée réglementée[51] (médecin) ou non réglementée[52] (antiquaire,

---

[45]C.A. Bordeaux, 25 mars 1987, D.1987,RSC 1988.534

[46]Cass.Crim.19 mai 1987, Gaz.Pal.1988

[47] تمييز جزائي، غرفة ٣ ، قرار رقم ١٩١ ، تاريخ ٣٠ / ٥ / ٢٠٠٧، كاساندرإلكتروني:" المتهم قد حمل المدعية ... على تسليمه أموالاً بعد أن أوهمها أن بإمكانه تأمين عمل لها لدى لدى إحدى النساء السعوديات منتحلاً صفة رجل أمن في السفارة السعودية في بيروت"

[48] تمييز جزائي، غرفة ٧ ، قرار رقم ٩٦، تاريخ ١٨ / ٤ / ٢٠٠٠ ، كاساندر إلكتروني: "المتهم أقدم على إنتحال صفة مالك عقار بكامله، وباعه إلى شخصين مختلفين، وحمل الشاريين على دفع الثمن له بعد أن كدعهمة بأنه مالك للعقار وبذلك ينطبق فعله على المادة ٦٥٥ عقوبات المتعلقة بالاحتيال"

[49] القاضي المنفرد الجزائي في صغبين، قرار رقم ١٨ ، تاريخ ٢٩ / ١/ ٢٠١١، كاساندر إلكتروني :" المدعى عليها استغلت واقعة كونها لا تزال مقيدة عازبة في سجل نفوس... وتستمر دون وجه حق ... عبر حبك مناورة احتيالية واستعملها صفة كاذبة للمخادعة والتأثير وبالتالي الاستفادة من المعاش التقاعدي للمرحوم والدها الذي كان يخدم في سلك قوى الأمن الداخلي وذلك بعد وفاة والدتها ... ونظمت... لقريبها وكالة ليستمر بقبض المعاش التقاعدي وإرساله لها إلى أميركا ...دون أن يثبت...أنه على علم بأن المدعى عليها موكلته متزوجة في الولايات المتحدة ...وهي تعمدت كتم واقعة زواجها ومستعملة صفة كاذبة أنها عزباء في قيود الأحوال الشخصية خلافاً لحقيقة الواقع..."

[50]Cass.Crim.30 avril 2003, Dr. Pénal 2003, comm.119

[51] تمييز جزائي ، غرفة ٦، رقم ٩٩ ، تاريخ ٣ / ٣ / ١٩٩٩، كاساندر إلكتروني:"المدعى عليه تقدم من الشركة المدعية زاعماً أنه محامٍ... رغم أنه كان قد شطب من جدول نقابة المحامين قبل أبعين يوم من ادعائه أمام الشركة أنه محامٍ ، وعلى هذا الأساس وثقت به هذه الشركة، و باعته سيارة وسجلتها على إسمه دون أي تأمين أو رهن رغم عدم دفعه لكامل الثمن. المدعى عليه إستعمل صفة كاذبة للتأثير على الشركة."

salarié pour obtenir des prestations sociales), ou d'une profession publique (fonctionnaire[53], officier public[5455]...)[5657]. Partant de là, la jurisprudence considère comme escroc une personne qui se prétend faussement mandataire d'une entreprise pour obtenir une livraison de marchandises par un fournisseur, une personne qui se dit faussement médecin, Pape, commerçant, concessionnaire exclusif de marque[58], inspecteur du guide Michelin[59] ou faussement diplômée.

A cet égard, un problème se pose au niveau de la qualification, puisque le fait de demander ou d'accepter des remises d'argent par celui qui exerce véritablement sa profession, peut être accusé sur la base d'autres infractions que l'escroquerie à savoir la corruption de fonctionnaire ou de salarié, tout dépend donc de la profession qu'exerce véritablement de l'escroc.

Quant à la qualité dont les escrocs abusent d'une façon très fréquente, il s'agit de la qualité de mandataire: le fait de se présenter faussement comme mandaté par un tiers. L'exemple classique de cette fausse qualité de mandataire est ce qu'on appelle «*l'escroquerie à la charité publique* » qui a lieu lorsque l'escroc se prétend mandaté par une organisation caritative pour recevoir ou distribuer fonds[60]. La

---

[52] جنايات جبل لبنان، قرار رقم ٥١٦، تاريخ ٨ / ١٢/ ٢٠٠٥، كاساندر إلكتروني:"المتهم أقدم على الاستيلاء على أموال المدعي إحتيالاً، بعدما إستعمل صفة كاذبة لمخادعته والتأثير عليه، إذ أوهمه بأنه ملتزم بناء ولديه عمال ومعدات فحمله بمناوراته الاحتيالية تلك على تسليمه مبلغاً من المال من أجل البدء بالعمل، فاستولى عليه و توارى عن الأنظار"

[53] جنايات بيروت، قرار رقم ٣٤٧ ، تاريخ ٢٩ / ١٢ / ٢٠٠٩، كاساندرإلكتروني:" أقدم المتهم على إنتحال صفة جاب في مؤسسة كهرباء لبنان وأوهم والدة المدعي بوجود متأخرات عليها للمؤسسة بعد أن سلمها بطاقة القطع المزورة، مما مكنه من الاستيلاء على مبلغ من المال "

[54] تمييز جزائي، غرفة ٦، قرار رقم ٢٦٥، تاريخ ١٦ / ١١/ ٢٠٠٦، كاساندر إلكتروني :"المدعى عليه أقدم بواسطة المناورت الاحتيالية، المتمثلة بإيهام العريف بأن السيارة مملوكة منه بالرغم من أنها كانت بحيازته على سبيل الاعارة، والزعم أمامه بأنه لم يستحصل على وكالة بيع بإسمه للسيارة حرصاً على عدم زيادة الوكالات... على حمل هذا الأخير على شراء السيارة وتسليمه مبلغ ... واستيلائه عليه... الأمر ما كان ليحصل لولا اتكال المدعى عليه على إنتحال الصفة العسكرية الأمنية التي اتاحت له القيام بهذه الأعمال"

[55] تمييز جزائي، غرفة ٣، قرار رقم ٢٥٥ ، تاريخ ٣ / ١٠ /٢٠١٣ ، كاساندر إلكتروني: "المدعى عليه أقدم على إنتحال صفة جابي كهربا ودخل بهذه الطريقة الاحتيالية أحد المنازل و ايهام ربة المنزل بأنه أتى لتحصيل فاتورة الكهربا منها واستيلائه إحتيالاً على مالها و إبرازه نسخة عن فاتورة طبية، كان قد صورها بشكل يصعب تمييزها عن إيصال كهربا لتسهيل عمليته الاحتيالية ..."

[56] جنايات جبل لبنان، قرار رقم ٦٢٦، تاريخ ٢٠٠٣/١٢/١٨، كاساندرإلكتروني: "إنتحال صفة مسؤول أمني، والاستيلاء من خلال هذا الانتحال على أموال الغير... يشكل الجنحة المنصوص عليها في المادة ٦٥٥ عقوبات"

[57] جنايات جبل لبنان،قرار رقم ١٩٩، تاريخ ٥ / ٤ /٢٠٠٧، كاساندرإلكتروني :" المتهم تردد عدة مرات...منتحلاً صفة مفتش في شركة الكهرباء ، وكان يستلم الأموال والمستحقات لشركة الكهرباء... وقام بالعديد من عمليات الاحتيال على المواطنين... "

[58] Cass.Crim.4 déc.1969, D.1970.114

[59] Cass.Crim.26 juin 1974, Bull.nº 243

[60] Cass.Crim.29 déc.1949, JCP 1950.II.5582 ; 10 juin 1991, Bull. nº247

«qualité» peut donc se manifester dans l'affirmation d'existence d'un lien de droit mensonger.

Pour ce qui est de l'abus d'une qualité vraie on dira que l'escroc utilise une qualité qu'il possède réellement, généralement sa profession[6162] -qualité de notaire, dentiste, directeur comptable, infirmier, négociateur immobilier…- pour donner force et crédit à ses mensonges[63] afin d'obtenir en contrepartie un avantage illicite à raison de la confiance qu'il inspire[64].

Il a été jugé par exemple que l'abus d'une qualité vraie existe dans l'usurpation d'un état consistant par exemple à se prévaloir d'un lien de parenté ou d'alliance imaginaire : fils d'un marquis[65]. Qu'elle existe de même dans le cas de titres usurpés : titre de noblesse[66], titre universitaire[67], titre de commandant dans l'armée, titre d'évêque[68] ou même de pape[69]…Enfin, qu'elle se révèle dans un mensonge portant sur des qualités professionnelles: inspecteur du guide Michelin[70], inspecteur d'assurances, architecte, fausse qualité de médecin[71], conseiller financier…

D'autres exemples retenus par la jurisprudence sont les suivants: un avocat qui abuse de sa qualité pour obtenir le désistement de l'adversaire de son client[72], un notaire qui fait signer un compromis de vente subordonné à l'acquisition d'un autre immeuble par le vendeur en sachant que le propriétaire de l'immeuble convoité

[61] تمييز جزائي، غرفة ٩ ، قرار رقم ٦٤ ، تاريخ ٣٠ / ٦ / ٢٠٠٣ ، كساندر ٢٠٠٣ ، ج ٦ ، ص ١٠٢٩ :" حيث أن المدعى عليه إستفاد من صفته كمعقب معاملات عقارية ومن ظرف معرفة المدعي به وثقته به ومن تمكنه الاستحصال على نماذج أوامر قبض رسوم عقارية لحمل المدعي على تسليمه مبالغ مالية وذلك بأيهمه المعاملة تسير بصورة جدية ، فيكون فعله يشكل جنحة الاحتيال ..."

[62] إستئناف جزاء جبل لبنان ، قرار رقم ٩٨ ، في ٤ / ٨ / ١٩٩٨،كاساندر إلكتروني:"المدعى عليه الذي يعمل موظفاً في الدوائر العقارية... قد قام بمناورات احتيالية حيث لفق الأكاذيب على المدعية بحيث وعدها بإحضار زبون لبيعه العقار الذي تملكه فجعلها تنظم له وكالة بذلك ولكنه لم يبع العقار ... ثم عد وباعه وإحتفظ بثمنه لنفسه"

[63] M.VERON, op.cit., éd.2010,p. 288, nº.412

[64] J.PRADEL, M. DANTI-JUAN, op.cit., p. 620, nº878

[65] Cass.Crim.18 juin 1958, Bull. nº473

[66] Cass.Crim.31 juillet 1884, Bull. n^{0}252

[67] Cass.Crim.29 nov.1838, Bull. n^0 370

[68] Paris, 4 juillet 1989. Dr. Pénal 1990, comm.09

[69] Cass.Crim.11 oct.1966, JCP1966.II.14897.

[70] Cass.Crim.12 juillet 1866, Bull. n^{0}173

[71] Cass.Crim.2 avril 1987, D.1898.I.316

[72] Cass.Crim.6avril.1993, Dr. Pénal 1993, comm.191

refuse de le vendre au prix indiqué[73], le cas d'un dirigeant d'une société de crédit qui recueille des fonds prétendument destinés à des prêts[74], le cas d'un homme d'affaires qui a la demande d'une veuve obtient une indemnité d'une compagnie d'assurance en faisant état auprès de sa mandante de lettres adressées à la justice et en demandant un pourcentage[75].

Toutes ces illustrations d'escroquerie tirées de la jurisprudence françaises sont transposables en droit libanais et la jurisprudence libanaise tranchera sans aucun doute de la même façon si elle était confrontée à l'un de ces cas concrets.

En outre, la jurisprudence française a eu à trancher la question de savoir si les personnes qui prétendent avoir la qualité de chômeur en vue de bénéficier de droits à des prestations financières, peuvent-elles de ce fait être poursuivies pour escroquerie en abusant d'une fausse qualité? La jurisprudence a répondu par la positive, en retenant l'usage abusif de la qualité de chômeur[76]. Cette jurisprudence qui n'est pas des plus récentes peut, sans difficultés aucune, être appliquée à tout individu abusant de sa qualité de membres d'organismes quel que soit l'objet de l'organisme en question tant bien en France qu'au Liban.

Après avoir défini dans le premier chapitre les trois premiers procédés classiques d'escroquerie en relevant leurs caractéristiques et leurs caractères communs, il est intéressant à présent d'examiner sous un chapitre (Chapitre 2) le quatrième procédé classique d'escroquerie que sont les manœuvres frauduleuses.

Chapitre 2: Les manœuvres frauduleuses:

Pour qu'un mensonge soit qualifié de manœuvres frauduleuses et qu'il tombe sous l'incrimination d'escroquerie, il doit être accompagné d'autres éléments matériels qui servent d'appui pour mieux convaincre la victime[77]. D'où le principe d'insuffisance du mensonge et ses atténuations qui feront l'objet de la première section de ce chapitre (Section 1).

[73]Cass.Crim.11 Mars 2009, Dr. Pénal 2009, com.81
[74]Cass.Crim.21 Nov. 1961, Bull. nº473
[75]Cass.Crim.29 Mars 1977, B.C. nº115
[76]C.A. Paris 27 septembre 1978, D.1979, Crim.9 mai 1979.
[77]ع. ع.ق.القهوجي، مرجع سابق، ص. ٧٦٢

En s'attardant sur le principe même, il faudra expliquer et élaborer quels sont les éléments matériels qui viennent s'ajouter au simple mensonge et qui le transforme en une infraction, l'escroquerie. C'est par la suite que nous envisageons sous une seconde section les différents éléments matériels qui viennent s'ajouter au mensonge en donnant plusieurs exemples et illustrations de ce que sont les véritables manœuvres frauduleuses (section 2).

Section 1: L'insuffisance du mensonge

L'expression «manœuvres frauduleuses» utilisée par les législateurs français et libanais, est une notion générale vague, qui vise tous les moyens susceptibles d'être employés ou utilisés par l'auteur de l'escroquerie. C'est ainsi que selon Rassat «*se livrer à une manœuvre frauduleuse c'est avoir une activité quelconque qui est de nature à convaincre quelqu'un de quelque chose de faux* »[78].

Partant de cette définition on dira qu'un simple mensonge banal ne peut, à lui seul, constituer une manœuvre frauduleuse ni en droit français ni même en droit libanais. Le principe consacré dans ses deux droits étant celui de l'insuffisance du mensonge (Paragraphe 1). Mais que ce principe de base connait bien évidemment des atténuations qu'on ne manquera pas de mettre en évidence (Paragraphe 2).

Paragraphe 1: Le principe

La raison qui soutient le principe de base selon lequel le mensonge est insuffisant à lui seul est évidente : une personne avisée est censée être prudente et ne doit pas se laisser tromper par de simples affirmations. Tout au contraire, elle doit être prudente et s'assurer de la véracité des dires de toute personne qui lui est étrangère avant de lui faire confiance[79]. La jurisprudence libanaise affirme clairement qu'au

[78]M-L. RASSAT, op.cit., paragraphe 123
[79]ع . ع . ق. القهوجي، مرجع سابق، ص. ٧٦٣

cas contraire la victime aurait commis une imprudence[80] et ne pourra que se blâmer elle-même de sa propre négligence[81].

Le droit Libanais à l'instar du droit français consacre ce principe[82]. A plusieurs reprises, les jurisprudences française et libanaise l'ont réaffirmé indépendamment du fait que le mensonge en question soit écrit ou verbal, total ou partiel et même dans les cas où le mensonge a été déterminant de la remise.

L'arrêt de la Cour de cassation française[83] a le mérite d'être des plus clair en ce sens: *«un mensonge, même produit par écrit, ne peut constituer une manœuvre frauduleuse s'il ne s'y joint aucun fait extérieur ou acte matériel, aucune mise en scène ou intervention d'un tiers destinés à donner force et crédit à l'allégation mensongère*». Cet arrêt a le mérite d'apporter une précision supplémentaire selon laquelle l'élément extérieur requis doit être indépendant du mensonge.

On pourra soutenir sans hésitation que les manœuvres frauduleuses qui constitue *«le fait matériel et extérieur qui vient à l'appui du mensonge destiné à lui donner force et crédit pour tromper la victime et l'inciter à croire en la véracité de ce mensonge»* sont ainsi indispensables tant en droit libanais[84] qu'en droit français.

Pourtant il faudra bien noter que la jurisprudence libanaise affirme quand même avec rigueur que sans mensonge l'escroquerie n'existe pas. Il a été jugé en ce sens dans un arrêt rendu par la cour d'appel du Mont Liban[85] le 14/4/1999 que l'organisateur qui fait appel à d'autres personnes pour organiser un concert sans remettre à ces deniers les profits auxquels ils avaient droit en contrepartie de leur

---

[80] تمييز جزائي غرفة ٣ قرار رقم ٧١ تاريخ ٢٠٠٥/٣/١٦،كساندر إلكتروني:"الكذب لا يكفي وحده و مهما بلغ مادة وجسامته سبباً للتوهم،وانما يجب تعزيزه أو تأييده بدليل أخر...إذا قصر بتدبر أمره وستسلم لمجرد كلام كاذب مدفوعاً برغبة ملحة وأمل بتحقيق الكسب والنجاح،فلا يعني أنه وقع على الفور،ضحية إحتيال مدبر...وما عليه في هذه الحالة إلا أن يلوم نفسه..."

[81] تمييز جزائي،غرفة ٦، قرار رقم ١٣١،تاريخ ٢٠٠١/٥/٢٢،كاساندر إلكتروني:"المدعى عليه حضر إلى سوق الخضار... وزعم أنه من كبار التجار وأنه ذو ملاءة كبيرة...ومجرد هذا الزعم لا يشكل مناورة احتيالية طالما أن المدعى عليه لم يؤيده بمظاهر خارجية أخرى بشكل مناورات...وعلى المدعي أن لا يستسلم لمجرد زعم..."

[82] تمييز ، غ-٦ - قرار ١٤ ، في ٢٣ / ١/ ٢٠٠١: "الكذب المجرد لا يكفي لإعتباره من قبيل المناورات الاحتيالية بل يقتضي أن يأتي مدعماً بعناصر خارجية كتأييد شخص ثالث ، ولو عن حسن نية ، أو كالظرف الذي مهد له المجرم وإستفاد منه ، بحيث أن تلك العناصر ساهمت في حمل المجنى عليه على تصديق الأكذوبة "

[83] Cass.Crim. 1 juin 2005, Bull. nº167, Dr. Pénal 2005, com.147, Gaz. Pal.13-14 janv. 2006, p.8

[84] تمييز غرفة ٦ ، غرفة ٦ ، قرار رقم ٢٥١ ، تاريخ ٢٦ / ١٠ / ٢٠٠٦ ، العدل ٢٠٠٧ ، ج. ١ ، ص . ٤٢٣ :"إن الكذب وإن كان يشكل عنصراً لازماً من عناصر المناورة الاحتيالية انما ليس العنصر الكافي لوحده وإن أكده صاحبه حتىأقنع به المجنى عليه، بل يجب أن تدعمه عناصر خارجية، فالكذب المجرد لا يستتبع عادةً التأثير الفعال طالما لم تعقبه أو ترافقه أفعال مادية بشكل مناورات "... فإذا أفرط شخص في الثقة فقد تصرف على غير ما يفعل الناس عادةً وكان مقصراً فلا يلومن إلا نفسه , "إن المناورات الاحتيالية لا تقوم على مجرد الكذب أو الاخلال بموجب عقدي ، بل تتحقق إذا كان الكذب مدعوماً بعناصر خارجية من شأنها إيقاع المجنى عليه بالغلط المؤدي إلى تسلم المال "

[85] ع. ع. ق. القهوجي، مرجع سابق ، ص. ٧٦٣

investissement, n'est pas considéré comme un escroc puisqu'il n'y pas eu un mensonge en ce qui concerne le concert et que ce concert n'est pas considéré ni comme une fausse entreprise ni comme un projet imaginaire.

Pour n'en citer que quelques-uns, les mensonges écartés par la jurisprudence concernaient le cas de promesse mensongère de mariage même celle assortie du mirage d'un appartement[86], des mensonges verbaux ou écrits résultant de faux bilans ou de fausses commandes.

Nous en déduisons qu'il n'existe de manœuvres frauduleuses que quand le mensonge est accompagné par d'autres éléments matériels extérieurs destinés à lui donner force et crédit, tel une production d'écrits, l'intervention d'un tiers ou une mise en scène.

Pour ce qui est du caractère frauduleux des manœuvres frauduleuses, ce dernier est déduit du but poursuivi par l'escroc[87].

Un autre principe primordial vient s'ajouter naturellement au principe d'insuffisance du mensonge c'est le principe d'exclusion de la simple omission comme manœuvre constitutive d'une escroquerie. Selon ce second principe, les manœuvres frauduleuses sont des actes positifs de commission ayant pour but d'induire la victime en erreur en vue d'obtenir la remise de la chose convoitée par l'escroc[88]. En d'autres termes les manœuvres ne sont considérées comme frauduleuses que dès lors qu'elles sont des actes positifs antérieurs à la remise, émanant de l'escroc ou d'un tiers complice.

La conséquence de ce second principe réside dans le fait qu'il ne peut y avoir de manœuvres frauduleuses commises par une simple abstention[89], une attitude passive assimilée à une action, ou d'une omission acte négatif par excellence[90].

La jurisprudence est allée dans ce sens en affirmant dans un arrêt très récent rendu en 2015 par la chambre criminelle[91] que «*l'escroquerie est un délit d'action ; que sa commission requiert l'accomplissement d'un acte positif : il faut avoir usé d'un faux nom ou d'une fausse qualité, abusé d'une qualité vraie ou commis une*

[86]M.VERON, op.cit., éd.1998,p.208.
[87]J. LARGUIER, Ph. CONTE, op.cit., p. 105, nº124.
[88]M.VERON, «*Droit pénal des affaires*», Compact, 6ème éd., Armand Collin, Paris, 2005, paragraphe 31.
[89]J. LARGUIER et Ph. CONTE, op.cit., p. 106, nº 124.
[90] ع. ع. ق. القهوجي، مرجع سابق ، ص. ٧٦٥
[91]Cass.Crim, 14 avril 2015, n°14-81.188, Dr. pénal, revue mensuelle Lexis Nexis jurisclasseur juin 2015, p. 30 et 31

manœuvre frauduleuse ; qu'une abstention, une omission, un silence, une réticence, aussi coupables soient-ils, ne constituent pas de manœuvres frauduleuses, celles-ci requérant l'accomplissement d'un acte positif (…)».

Paragraphe 2 : Atténuations jurisprudentielles

Certes le simple mensonge ne peut pas constituer une manœuvre frauduleuse mais tel n'est pas le cas lorsque ce mensonge est conforté par un autre élément extérieur[92] assurant sa crédibilité tel que la production d'un écrit, une mise en scène ou l'intervention d'un tiers[93].

C'est en ce sens que la jurisprudence constante continue de trancher, c'est le cas dans un arrêt très récent de la chambre criminelle rendu en 2015[94] selon lequel *«Alors qu'une affirmation mensongère, non appuyée de faits extérieurs, quelle que soit la forme prise, verbale ou écrite, qui ne porte pas sur l'usage d'un faux nom, d'une fausse qualité ou l'abus d'une qualité vraie, ne constitue pas une manœuvre frauduleuse caractéristique du délit d'escroquerie s'il ne s'y joint aucun fait extérieur ou acte matériel, aucune mise en scène ou intervention d'un tiers, destinés à lui donner force et crédit (…)»*

Le premier élément extérieur qui vient s'ajouter au simple mensonge pour le rendre plus crédible est une mise en scène ou «machination» créée de toute pièce par l'escroc pour tromper sa victime.

Les juges apprécient l'existence de la mise en scène d'une façon subjective en prenant en compte la psychologie, l'intelligence ou même les capacités intellectuelles de la victime de l'escroquerie.

---

[92] تمييز جزائي غرفة ٧ قرار رقم ١١٣ تاريخ ٢٠٠٨/٦/٢٦،كاساندر إلكتروني

[93] تمييز جزائي غرفة ٣،قرار رقم ٢٧٠، تاريخ ٢٠٠٣/١٢/١٠,كاساندر إلكتروني :"إن ايهام المدعي ليس شرطاً وضعه المشرع لقيام جرم الإحتيال وانما هو نتيجة لشرط إتيان المناورات الاحتيالية...إن الكذب لوحده لا يعتبر سبباً للتوهم وانما يجب تعزيزه بدليل أخر ...لا يكفي أن يعمد المدعى عليه إلى ايهام المدعي بأنه في وسعه تنفيذ إلتزامه (كونه لم يركب ألومنيوم من نوع تكنال) بل يجب أن يعزز ذلك بمستندات خطية غير صحيحة...وإما بتأييد شخص ثالث أو غير ذلك من الأدلة...القضاء يقوم على التشدد بتوفر عناصر وشروط المادة ٦٥٥ عقوبات،وإشترط أن تبلغ المناورات حداً من الجسامة والخطورة...وذات أهمية بالغة توصلاً إلى إيقاع المخدوع في الغلط...إذا أفرط المرء في الثقة أو إستسلم لمجعد كلام معسول فيكون قد تعجل الامر أو تصرف على غير حذر..."

[94] Cass.Crim.11 mars 2015, n^0 pourvoi : 13-87558, www.legifrance.fr

D'où, Il pourra s'agir d'une mise en scène au sens théâtral[95] lorsque l'agent installe par exemple des bureaux pour faire croire à l'existence d'une fausse entreprise florissante ou augmentation de capital fictive[96]. Sinon, d'une mise en scène matérielle, technique ou juridique: matérielle quand par exemple la cliente d'un magasin en libre-service a changé l'étiquette du prix d'un produit, juridique lorsque de fausses factures fondant une demande de paiement au crédit sont placés dans une comptabilité inexacte, ou dissimulation d'une partie du contrat que l'on fait signer, ou le cas d'un comparse intervenant pour garantir la valeur de bijoux, ou lors d'une présentation d'un billet dont on demande la monnaie et auquel on substitue un billet de moins de valeur[97], ou faire un maquillage à des objets vendus pour tromper sur leurs qualités véritables[98]. Rentre aussi dans la machination les compteurs kilométriques de voitures de taxi ainsi que les compteurs d'eau, d'électricité…

Pour synthétiser nous dirons que la mise en scène reflète toute manipulation destinée à tromper la victime sur l'exactitude de la situation. Les deux droits libanais et français s'attardent sur l'existence ou pas d'une telle mise en scène pour qualifier les faits in concreto de manœuvres frauduleuses constitutives du délit d'escroquerie ou pas.

Le second élément extérieur attestant, tant en droit français qu'en droit libanais, la véracité d'un mensonge préexistant et le renforçant par la même est la production d'écrits ou de documents souvent fabriqués ou falsifiés par l'escroc lui-même[99], par un tiers ou même détournés de leur finalité. Tel est le cas de faux bilans, d'une comptabilité falsifiée, de déclarations mensongères à des organismes sociaux, de présentation de fausses factures pour l'escroquerie à la T.V.A.[100], de production de titres fictifs: bordereau de cession de créances professionnelles, photographies truquées en matière d'assurance (accident d'automobile, incident), une simple étiquette sur un produit…

---

[95]M-P LUCAS DE LEYSSAC, A. MIHMAN, op.cit., p.54, nº76
[96]Cass.Crim.9 janv.1973, Bull. n ^{0}10, JCP 1974.II.17.674
[97]Cass.Crim.26 juillet 1957, D.1957.677
[98]Cass.Crim.21 mars 1885, Bull. n^0 98, 20 mai 1961, B.167 ; Trib. Corr. Caen 7 mai 1913, Gaz. Pal. 1913.2.253
[99]J.PRADEL, M. DANTI-JUAN, op.cit., p.624, nº882.
[100]M-P.LUCAS DE LEYSSAC, A. MIHMAN, op.cit., p.52, n^0 75

A cet égard, la force de persuasion de tout document utilisé par l'escroc est appréciée par les juridictions françaises et libanaises au cas par cas[101] en prenant compte le degré de confiance attaché à ce document, sa force de probante et le fait qu'il conforte ou non le mensonge[102].

Lorsque les documents présentés à l'appui du mensonge émanent de l'escroc ce dernier sera poursuivi par application des dispositions des deux droits français et libanais pour usage de faux. Alors que si les dits documents émanent d'un tiers de mauvaise foi ce dernier pourra être poursuivi pour faux et complicité d'escroquerie. Pour donner une idée sur les documents émanant de tiers qui ont été retenus par la jurisprudence nous citerons les fausses factures, les certificats médicaux mensongers dans le but de réaliser des escroqueries à la sécurité sociale, les bordereaux dans lequel sont transcrites les créances cédées à un banquier selon le procédé Dailly[103]affirmant l'existence de créances fictives[104], les bilans d'une société certifiés par le commissaire aux comptes et présentés à des banquiers.

La troisième technique de renforcement des mensonges de l'escroc expressément consacrée dans les deux droits français et libanais a lieu par le recours à la publicité: c'est le cas des petites annonces qui attirent les amateurs ou des offres d'emploi qui ne sont bénéfiques que pour l'escroc…

L'intervention d'un tiers afin de confirmer les dires de l'escroc et donner crédit à ses mensonges[105] reste la méthode qui est le plus souvent utilisé en matière d'escroquerie. En effet, il suffit que l'intervention d'un tiers soit déterminante[106] du consentement de la victime pour caractériser la manœuvre frauduleuse surtout lorsque l'intervention en question elle est sollicitée par l'escroc lui-même[107]. D'où l'intervention spontanée d'un tiers, même lorsqu'elle avait pour but de duper la

[101]Ph. CONTE, op.cit. 320, nº559.
[102]J, LARGUIER, Ph. CONTE, op.cit., p. 110, nº127.
[103]M-P LUCAS DE LEYSSAC, A. MIHMAN, op.cit., p. 51, nº 75.
[104]J.PRADEL, M. DANTI-JUAN, op.cit., 625, nº882.
[105] الهيئة الاتهامية في جبل لبنان، قرار ٧٥ ، تاريخ ٤ / ٤ / ١٩٩١ ، العدل ١٩٩٠ -١٩٩١ ، ص ٢٢٦ :" ... وحيث أن العناصر الخارجية المستقلة قد تستمد من تدخل شخص ثالث يؤيد الكذب أو من الاستعانة ... من أشخاص أو أشياء تضفي بتدخلها على الأكاذيب ثقة لم تكن تحملها... وحيث أن تدخل الأشخاص الأخرين لتدعيم الكذب يستوي فيه أن يكون المحتال قد تواطأ معهم على التدخل بعد أن كشف أهم مشروعه الجرمي أو أن يكون قد خدعهم بدوره واستعملهم أدت لخداع المجني عليه ..."
[106] تمييز جزائي ، غرفة ٦ ، قرار رقم ١٣٣ ، تاريخ ٢٦ / ٥ / ٢٠٠٢ ، كساندر ٢٠٠٢ ، ج ٥ ، ص ٥٧٦
[107]M. VERON.éd.1998, op.cit., p.210

victime de l'escroc, est très rarement prise en compte pour caractériser l'élément matériel du délit d'escroquerie.

En outre, il faut qu'il s'agisse d'un tiers véritable c.à.d. d'une personne indépendante de l'agent qui ne soit pas son mandataire, son salarié ou son représentant.

Il importe peu que ce tiers ait un comportement actif en tant que témoin de complaisance d'un accident fictif, ou un comportement passif par sa simple présence, qu'il soit imaginaire ou réel, qu'il soit de bonne foi (trompé lui-même) ou même qu'il soit inconscient de son rôle. Sachant que s'il s'est révélé que le tiers ayant participé au délit d'escroquerie était de mauvaise foi il sera considéré comme tiers complice de l'escroquerie ou tiers certificateur puisque son rôle est d'appuyer les manœuvres de l'auteur principal.

De même il n'importe peu que le tiers soit intervenu en personne dans l'opération ou en qualité d'auteur d'un écrit ou d'un document quelconque. Tel est l'exemple d'un garagiste qui délivre une facture dans laquelle il gonfle le prix d'achat pour permettre à l'acquéreur du véhicule d'obtenir de sa banque un crédit supérieur à celui qu'il aurait dû obtenir de cette dernière[108.]

Tout ce qui précède nous conduis à dire que l'ancien texte français en disposant que *«les manœuvres frauduleuses doivent tendre à persuader l'existence de fausses entreprises, d'un pouvoir ou d'un crédit imaginaire ou faire naitre l'espérance ou la crainte d'un succès, d'un accident ou de tout autre événement chimérique»*[109] était certes plus précis que le nouveau texte, mais que le nouveau texte[110] a le mérite d'être plus large et permet de ce fait d'incriminer beaucoup plus de cas non prévus par l'énumération stricte de l'ancienne version.

Il est important de noter que la jurisprudence française ainsi que la jurisprudence libanaise sont toutes deux très exigeante quant à l'évaluation de l'importance des manœuvres frauduleuses utilisées par chaque escroc. Ainsi ces jurisprudences ne considèrent l'escroquerie constituée que lorsque les actes commis sont *«de nature à surprendre la vigilance d'une personne d'une intelligence normale»*[111]. Cette

[108]M-P. LUCAS DE LEYSSAC, A. MIHMAN, op.cit., p. 50, nº. 74
[109]Ancien CPF art. 405
[110]CPF art. 313-1
[111]M-L.RASSAT, op.cit., p. 145, nº118.

intelligence normale tant intellectuelle que psychologique sera appréciée selon chaque cas d'espèce.

Enfin il est intéressant de souligner que la notion «d'escroquerie au jugement» a vu le jour en droit français mais qu'elle est toujours ignorée en droit libanais. Cette escroquerie spéciale existe, selon la jurisprudence française, lorsque les manœuvres frauduleuses ont pour but *«de surprendre la juridiction saisie soit par l'intervention de tiers effectuant de faux témoignages soit par la production d'écrits falsifiés»*[112]. Cette infraction d'escroquerie sui generis suppose donc selon le dernier état de la jurisprudence française *«d'avoir présenté en justice, de mauvaise foi, des documents mensongers qui, destinés à tromper la religion du juge, sont susceptibles, si la machination n'est pas déjouée, de faire condamner son adversaire à payer des sommes qui ne sont pas dues(…)»*[113].

L'infraction d'escroquerie au jugement n'est toujours pas légiférée en droit libanais la raison est évidente pour une certaine doctrine libanaise qui donne raison à une jurisprudence française récente de 2012 ayant considéré que l'infraction d'escroquerie au jugement «*se borne à remettre en question l'appréciation souveraine, par les juges du fond, des faits et circonstances de la cause, ainsi que des éléments de preuve contradictoirement débattus, ne saurait être admis(…)*»[114].La jurisprudence libanaise a elle-même statué dans ce sens dans un arrêt isolé de 2014[115] où elle rejette la qualification d'escroquerie au jugement. Sa motivation est claire l'escroquerie incriminée par le texte de l'article 655 CPL touche uniquement les délits sur les biens ce qui n'est pas le cas de l'escroquerie au jugement visant l'annulation d'une décision judicaire rendue sous l'ampleur d'une fraude commise par l'une des parties.

Depuis 2004, la jurisprudence française a même admis l'escroquerie d'une sentence arbitrale[116].

---

[112]Cass.Crim.8 nov.1962. Bull. n^{0}312

[113]Cass. Crim.19 mars 2014, n^o pourvoi 13-80970.

[114]Cass. Crim. 21 mars 2012, pourvoi n^0 11-84541 ; Cass. Crim. 20 Avril 2005, pourvoi n^0 04-84828

[115]تمييز جزائي، غرفة ٦، قرار رقم ٤٧٠ ، تاريخ ١٦ / ١٢ / ٢٠١٤ ، كساندر إلكتروني

[116]M.VERON, op.cit., p.296, n^{o}421.

Section 2: Eléments extérieurs propices

Peu importe la manœuvre frauduleuse utilisée par l'escroc cette manœuvre doit impérativement être déterminante de la remise et antérieure à celle-ci. Ces deux conditions sont exigées de façon cumulatives tant en droit français[117] qu'en droit libanais[118].Exceptionnellement, la cour de cassation admet l'escroquerie dans des cas où la remise parfois précède les manœuvres, seulement lorsque les manœuvres ont pour but d'obtenir la continuité des remises[119].

Comme nous l'avons précédemment cité les manœuvres constitutives d'escroquerie sont citées à l'article 313-1 CPF. Le droit libanais énumère à son tour à son art 655CPF (après la réforme de la loi numéro 112 de 1983) d'une façon exhaustive les manœuvres considérées comme frauduleuses: 1- actes frauduleux ayant pour but de persuader la victime de l'existence de fausses entreprises ou un projet fictif ou tout acte faisant naitre chez la victime une espérance de gain ou crainte d'un accident. 2- intervention d'un tiers ou circonstances extérieures desquelles profite l'escroc, 3- disposer des biens (meubles ou immeubles) sans droit ni qualité, 4- recours à un faux nom ou fausse qualité. Un acte matériel peut même être devenir un mode de vie utilisé par l'escroc[120].

Selon Dr. Kahwaji, la réforme de la loi de 1983 est venue énumérer tous les cas possibles des manœuvres frauduleuses à titre limitatif d'une façon claire[121], or une grande partie de la doctrine libanaise ne soutient pas cette idée en consacrant l'idée que la liste énumérée n'est pas limitative, laissant aux juges le pouvoir d'interprétation d'une façon casuistique.

En examinant de plus près la jurisprudence on trouve une diversité dans les moyens utilisés par les escrocs pour tromper leurs victimes afin d'obtenir la remise espérée. Nous citerons ci-dessous la production d'écrits ou de pièces (Paragraphe

---

[117]Cass.Crim.8 Nov. 1988: Bull Crim. 1998, nº 381; Cass.Crim.21 mars 2012, n^0 11-87.453, Dr. pénal 2012, comm. n^0 97

[118]تمييز جزائي، غرفة رقم ٦ ، تاريخ ٢٣ / ١ / ٢٠٠١ ، كساندر إلكتروني

[119]Cass.Crim.31 oct. 1981, (V. *M.VERON, Droit pénal spécial*, 6ème éd, Armand Colin 1998, p.296, nº. 415)

[120] ع. ع. ق. القهوجي، مرجع سابق،ص. ٧٧٢

[121] Ibid. p.769

1) de même que l'intervention d'un tiers et les circonstances extérieurs favorables à l'escroc (Paragraphe 2).

Paragraphe 1: Production d'écrits, de pièces et mise en scène:

La production d'écrits est le moyen le plus fréquent pour justifier l'exactitude des mensonges de l'escroc. Partant de là, les jurisprudences française et libanaise ont adopté une interprétation extensive de la notion d'écrit ou de documents pour faire face aux innovations techniques.

En effet, Il importe peu que l'écrit constate un droit ou non[122], qu'il provienne d'une autorité publique ou d'une personne privée, qu'il s'agisse d'un faux intellectuel ou d'un faux matériel. Il s'agit la plupart de temps de documents fabriqués[123], contrefaits ou falsifiés par l'escroc ou par un tiers.

Toute sorte d'écrit peut servir à établir des allégations mensongères, mais l'écrit le plus utilisé réside dans les fausses factures[124] qui ne correspondent pas à des fournitures ou à des prestations de services réellement effectuées.[125]. Ces factures sont faites souvent par des sociétés fictives ou existantes sans activité réelle, créés seulement pour un besoin fixe, pour faire du chiffre ou de la taxe (ces sociétés sont appelées sociétés taxis). Ces fausses factures servent à obtenir de prêts ou de crédits auprès d'organismes financiers trompés par une apparence d'activité, ceci est considéré une escroquerie.

Un autre procédé fréquent de productions d'écrits, est celui des fausses déclarations de sinistre qui sont utilisés en cas d'escroquerie à l'assurance. C'est le cas quand un escroc vient à joindre à sa déclaration de vol, d'incendie, ou d'accidents, des attestations établies par des tiers experts, pour justifier le sinistre et réclamer une indemnité à l'assurance.

---

[122] تمييز جزائي ، غرفة ٦ ، قرار رقم ٣٠١ ، تاريخ ١٨ / ١١ / ٢٠٠٤ ، كساندر ٢٠٠٤ ، ج ١١ ، ص ١٦٠٣ :" المستدعي ضده، كان عالماً بإيفاء ألدين من قبل المدعي ، ورغم ذلك أقدم على إلقاء الحجز الاحتياطي على عقاراته. يكون فعله في حال ثبوته مؤلفاً مناورة احتيالية وينطبق على المادة ٦٥٥ بند ٣ عقوبات إذ الدليل على أن المستندات التي استعملت لإستصدار قرار الحجز الاحتياطي هي ملفقة وتؤلف إساءة في ألحق بإستعماله وغرضها إبتزاز مال المدعي عن طريق إيقاع القاضي في غلط أدى إلى إصدار قرار الحجز لحمل المدعي على تسديد موال غير متوجبة..."

[123] تمييز جزائي، غرفة ٧ ، قرار رقم ١١٤ ، تاريخ ١٩/ ٥ /٢٠٠٣،كاساندر إلكتروني:"إستيلاء المدعى عليه على أموال من الشركة المدعية بعد أن أوهمها بأنه دفع الأموال التي تسلمها سابقاً إلى صندوق الضمان الاجتماعي مبرزاً اشعارات الاستلام المزورة يشكل الجنحة المنصوص عليها في المادة ٦٥٥ عقوبات ، لأن تسليم المال في هذه المرحلة للمدعى عليه من الشركة المدعية كان بتأثير مناورات المدعى عليه و ايهامه المدعية بأنه سلم المبالغ مبرزاً اشعارات مزورة"

[124] Cass.Crim.12 sept. 2006, Dr. Pénal 2006, comm.157

[125] M.VERON, op.cit., éd.2010, p. 290, nº415.

Mais le procédé le plus efficace reste le recours à une mise en scène. La mise en scène ou machination consiste dans une *«combinaison de faits, l'arrangement de stratagèmes, l'organisation de ruses (...) ayant pour but de donner crédit au mensonge»* de l'escroc[126][127].

La mise en scène requise peut être d'une simplicité extrême par exemple substituer des animaux femelles à des animaux mâles[128], simuler un accident de la future épouse pour émouvoir et escroquer une personne handicapée[129], simuler un vol pour obtenir la prime d'assurance correspondante, ou l'escroquerie au «parcmètre» par laquelle l'escroc met une rondelle[130] sans valeur (à la place de 1 franc) pour déclencher le mécanisme d'un parcmètre de stationnement[131]. En outre, la simple création d'un titre au profit de l'escroc ou la signature d'un contrat d'achat dont il a sciemment dissimulé le texte ou l'étiquetage *«pour y faire apparaitre un prix inférieur que celui réellement fixé* »[132] sont constitutifs de manœuvres frauduleuses. Un autre exemple frappant est celui de l'utilisation de chéquier pour créer l'illusion de moyens financiers que l'escroc ne possède pas dans le but de tromper les commerçants[133]L'escroquerie par l'exploitation commerciale de la charité publique est un également un autre exemple sur lequel la cour de cassation a eu à statuer[134].

---

[126] تمييز جزائي، غرفة ٦ ، قرار رقم ١٤، تاريخ ٢٣ / ١ / ٢٠٠١ ، كاساندر إلكتروني:" الركن المادي المتمثل بفعل الخداع القائم على الكذب المؤيد ... المدعى عليهما اقنعا المدعي...ترغب العمل لديه كخادمة ،وقد انصب فعل الخداع والكذب على واقعة الرغبة في العمل التي صدقها المدعي نتيجة تأييد الشخص الثالث ...عن حسن نيه ... العناصر الخارجية الداعمة للأكذوبة...تظهر جلياً من خلال الظرف الذي إستفاد منه المدعى عليهما والمتمثل في قيام المدعي بالتفتيش عن خادمة...في ما يعود إلى النتيجة الجرمية العبارة الواردة في العقد :إن الجهة قبضت كامل المبلغ, ما يفيد أن المدعي ما كان ليسلم المال لولا فعل الخداع ...توافر الركن المعنوي الذي يتجلى بأن المدعي عليها ...وبإتفاق مسبق مع شقيقها وفور استلامها المبلغ هربت من المنزل"

[127] Cass.Crim.11 mai 1971, Bull. crim. nº145

[128] Cass.Crim.15 mai 1997, Bull.n^{0}189

[129] Cass.Crim.22 oct.1987, Gaz.Pal.1988.114

[130] La rondelle métallique dépourvue de valeur représentait bien l'élément matériel et externe destiné à donner force et crédit au mensonge implicite V. Raymond Gassin, commentaire des arrêts, Jurisprudence (1972), 17277

[131] Cass.Crim.10. Déc.1970, D.1972.155

[132] Cass.Crim.9 Mars 1983, note par Jean Deveze, professeur à la faculté de Droit de Dijon

[133] Cass.Crim,1er juin 2011, pourvoi numéro 10-83.568: «*l'ouverture d'un compte bancaire dans le seul but de se faire délivrer un chéquier destiné à créer l'apparence d'une solvabilité et l'utilisation des chèques ainsi obtenus pour se voir remettre des marchandises avec le dessein formé dès l'origine de ne pas en payer le prix forment un stratagème caractérisant les manœuvres frauduleuses constitutives de l'escroquerie* ».

[134] Cass.Crim.28 novembre 1975(V. P. Bouzat, « *Crimes et délits contre les biens»*, Rev.sc.crim.1978,p.362): constituent des manœuvres frauduleuses : «*l'intervention combinée et l'ensemble des actes de plusieurs personnes agissant en vue du but commun de persuader l'existence de fausses entreprises, d'un pouvoir ou d'un crédit imaginaire ou pour faire naitre l'espérance ou la crainte d'un succès, d'un accident ou de tout autre événement chimérique*».

D'autre part la mise en scène peut être beaucoup plus complexe elle aura alors pour objets: la création de sociétés fictives, le recours aux fausses factures, ou même la distribution de diplômes fictifs. Un premier arrêt intéressant à ce propos est celui rendu par la cour d'appel le 28 mars 2012[135] qui a condamné un administrateur de société professionnel de l'analyse financière pour délit de manipulation de cours entravant le fonctionnement régulier du marché et induisant les investisseurs en erreur.

Un deuxième arrêt illustrant une mise en scène bien réfléchie est celle qui fut l'objet de l'arrêt rendu le 28 février 2012[136].L'affaire était relative à de fausses déclarations de vol de voitures faite par un gérant de garage à sa compagnie d'assurance pour réclamer une indemnité. Alors qu'en réalité le garagiste a procédé au remontage puis à la vente des véhicules en question et en a dissimulé les pièces de rechange

Un troisième arrêt qui va dans le même sens est celui rendu par la chambre criminelle, le 24 mars 2010[137], Il s'agissait d'un escroc qui avec l'aide d'un antiquaire complice vendait des tableaux à des prix supérieurs à leur valeur réelle en recourant à des pseudonymes, à la disposition des tableaux dans des quartiers de luxe et en prétendant que ces tableaux provenaient de collection privée.

L'affaire «Maria Branca dos Santos» a fait également parler d'elle. L'escroc avait créé une organisation de prêts et d'investissements illégaux faisant croire aux investisseurs qu'ils seront remboursés avec des dividendes exceptionnels. Il en est de même pour l'affaire française «Bernard Madoff» et l'affaire libanaise «Salah Ezzedine» où les financiers ont pu détourner des fonds en promettant à leurs clients des intérêts élevés 60 %.

Citons enfin, l'affaire Libanaise très récente de 2015 de «Mourched Daher» a également fait parler d'elle : il s'agissait du propriétaire de deux sociétés financières pour le crédit, qui octroyait des prêts en échange de la conclusion devant notaire de contrats de vente de biens immobiliers appartenant aux

[135]CA Paris, Pole5, ch.12, 28 mars 2012, numéro 10/04868, nº 2: l'escroc avait passé sur le marché plusieurs ordres qu'il avait ensuite annulé afin *de provoquer une hausse du cours, ce qui a déclenché le seuil de réservation de l'action à la hausse*. Les manœuvres utilisées étaient destinées à inciter de potentiels investisseurs à se porter acquéreurs des titres en misant sur une hausse future ou « intérêt artificiel».

[136]Cass.Crim.28 février 2012, pourvoi nº 11-82.953: l'affaire était relative à de fausses déclarations de vol de voitures faite par un gérant de garage à sa compagnie d'assurance. Alors qu'il procédé au remontage puis à la vente des véhicules en question et en dissimuler les pièces.

[137]Cass.Crim.24 mars 2010, pourvoi numéro 08-85.109, HaritiniMatsopoulou, Infractions contre les biens, Chronique de Jurisprudence, Chroniques,Juillet/Septembre 2010 ,p.629 et 630

demandeurs de crédit. Cet escroc s'empressait, une fois les dits contrats dument signés chez le notaire, d'inscrire en son nom les biens faisant leur objet au registre foncier, avant même l'échéance de remboursement des crédits accordés à ses victimes. Par la suite il faisait chanter ses débiteurs qui ne pouvaient plus se faire restituer leurs biens qu'en s'acquittant de sommes faramineuses qu'il leur demandait.

Dans tous les cas de figure que nous venons de relever, on pourrait affirmer que la mise en scène dépend inévitablement de l'imagination de l'escroc, de la crédulité de la victime et du fait que cette dernière soit un professionnel ou pas.

Paragraphe 2: Intervention d'un tiers et circonstances extérieurs

L'escroc peut choisir de faire intervenir un tiers, pour renforcer ses déclarations, et donner crédit à ses mensonges. Le tiers sollicité vient donc certifier l'exactitude des mensonges de l'escroc, d'où l'appellation de «*tiers certificateur* ».

A l'instar du droit français, le droit libanais donne toute son importance à l'intervention d'un tiers dans le délit d'escroquerie.

L'intervention du tiers en question peut être faite, aussi bien en droit français qu'en droit libanais, de façon verbale ou de manière écrite[138].Les exemples d'intervention de tiers auprès des escrocs sont très nombreux : jeux de hasard truqués avec l'aide d'un compère[139], fausse facture permettant d'obtenir un prêt d'un organisme spécialisé[140], le garagiste qui remet une facture pro forma à un acheteur éventuel en haussant le prix réel de la voiture pour permettre à l'acheteur d'obtenir d'une société de crédit un prêt supérieur à celui qu'il aurait pu obtenir[141], ou même celui qui fournit à l'escroc des faux permis de conduite[142].

Le cas retenu par l'arrêt du 1er juin 2005[143] est l'un des meilleurs exemples à citer. En l'espèce il s'agissait d'un prévenu qui, après le décès de son père, avait

---

[138] ع. ع. ق. القهوجي ، مرجع سابق ، ص. ٧٨٠

[139] Cass.Crim.8 juin 1912. Bull.n^{0}308

[140] Cass.Crim.11 jan. 1968, Bull. n^{o}9

[141] Cass.Crim.9 nov.1977, Bull.n^{0}344

[142] تمييز جزائي، غرفة ٧، قرار رقم ٣٣٠ ، تاريخ ٢٧ / ١٠ / ٢٠١٦، كاساندر إلكتروني : أقدم المتهم... على الاستحصال بواسطة شخص ثالث على شيكات مزورة و رخصتي سير مزورتين ... وعلى إستعمال هذه الشيكات والرخصتين... عبر تسليمهما للمدعين بهدف الاستيلاء على اموالهما إحتيالاً ... و لكن الشخص الثالث لم يثبت ارتكابه ...لأي فعل مادي... ولم يرتكب مناورات احتيالية"

[143] Cass.Crim,1er juin 2005 (V. M-P. LUCAS DE LEYSSAC, A.MIHMAN, op.cit.,p.48). Dans ce cas d'espèce, la Caisse d'épargne a été considérée comme un tiers intervenant de bonne foi, dans le délit d'escroquerie commis par le prévenu.

continué à percevoir la retraite versée par la Mutualité sociale agricole tout en étant conscient du caractère anormal de la situation et de la caducité des procurations qu'il utilisait.

Il faudra aussi noter l'arrêt déjà cité du 24mars 2010[144] où un expert qui était intervenu durant un procès pour certifier de la valeur d'œuvre d'arts a été jugé complice du délit d'escroquerie[145].

On peut s'attarder également, sur un troisième arrêt intéressant du 25 février 2004[146] traitant d'un cas d'escroquerie à la TVA puisqu'un groupe de sociétés a organisé, avec la complicité du commissaire aux comptes et de l'expert-comptable[147], des ventes fictives à travers lesquelles il a pu obtenir le paiement d'une énorme somme d'argent comme remboursement de taxes qui n'ont jamais été décaissés. Tout ceci sur la base de fausses déclarations mensuelles de chiffre d'affaires et de documents falsifiés de crédits fictifs de TVA[148]. Cet arrêt montre clairement la position exigeante et ferme de la cour de cassation vis-à-vis d'actes commis par des professionnels, qui se doivent être vigilants en accomplissant leurs missions et doivent opérer un contrôle total sous peine de se voir incriminer comme complices de délits d'escroquerie.

Deux anciens arrêts de la chambre criminelle du 22 mai 1968[149] et du 14 juin 1977[150], dont la motivation est toujours valable de nos jours, ont tranché des cas d'escroquerie à l'assurance en déclarant que le témoignage de complaisance d'un tiers corroborant la demande de celui qui a assigné la compagnie d'assurance en paiement d'indemnité, constitue une manœuvre frauduleuse. Il en est de même pour les déclarations d'accident fictif appuyé par des témoignages de complaisance, la vente de parts sociales mais surévalués grâce au rapport positif

[144]Cass.Crim.24 mars 2010, pourvoi n^0 08-85.109 (V. H.MATSOPOULOU, chronique de jurisprudence, juillet/septembre 2010, p.629)

[145]H.MATSOPOULOU, Infractions contre les biens, Chronique de Jurisprudence, Chroniques,Juillet/Septembre 2010, page 630 et 631.

[146]Cass.Crim.25 février 2004, pourvoi num. 03-81.173

[147]Sur la base du principe selon lequel les comptes et déclarations mensuelles de chiffres d'affaires taxables ne pouvaient échapper à un professionnel non négligent.

[148]H. MATSOPOULOU, Infractions douanières et fiscales, Chroniques, Juillet/Septembre 2005, RSC, page 576 et 577

[149]Cass.Crim.22 mai 1968, note par Pierre Bouzat, Crimes et délits contre biens

[150]Cass.Crim.14 juin 1977, B.215, D.1978.125: «*le témoignage de complaisance qui vient donner forme et crédit aux allégations de la personne qui demande indemnité à la compagnie d'assurance, est considéré comme un commencement d'exécution de la tentative d'escroquerie*»

d'un expert[151], ou le cas d'insertion de documents fantaisistes au milieu des comptes établis par l'expert-comptable de la société[152].

Partant de toute la jurisprudence abondante en matière d'intervention de tiers dont nous venons de citer quelques arrêts marquants, nous pouvons établir une liste de constatations dont l'exactitude a été confirmée de façon constante:

1) Le tiers dont l'intervention est déterminante dans le délit d'escroquerie peut ne pas exister réellement, il est parfois inventé par l'escroc pour les besoins de la cause et connu sous l'appellation «*tiers supposé*». c'est le cas par exemple de l'escroquerie à la publicité dans lequel l'escroc invente de prétendus acquéreurs pour faire monter les prix de celui qui obtient des fonds pour financer un procès relatif à une succession imaginaire. Selon Rassat, vaut mieux considérer en cas de présence d'un tiers supposé que c'est un cas de mise en scène plutôt qu'un cas d'intervention de tiers à proprement dit[153].

2) Le plus souvent, le tiers est vrai et existant, il coopère consciemment avec l'escroc, comme complice de ce dernier avec la même intention frauduleuse de partager avec lui les bénéfices du délit. Tel est le cas de celui qui prétend être intéressé par l'achat d'objets convoités par d'autres personnes dans le but unique d'augmenter les prix[154].

3) le tiers jouit généralement d'une autonomie par rapport à l'escroc. C'est le cas du commissaire aux comptes et de l'expert-comptable qui certifient des comptes permettant une escroquerie[155]. Cette autonomie n'existe pas toujours lorsque le tiers est un mandataire ou un salarié, puisqu'il y a un lien de subordination entre ce tiers et l'escroc.

4) Enfin, le tiers peut être une personne de bonne foi, inconsciente de l'escroquerie[156] ou une seconde victime de l'escroc, mais dont l'intervention sera

[151]Cass.Crim.18 Jan. 1988, Bull.22, Rev.soc.1988, p.576
[152]Cass.Crim.6 déc. 1993, Dr. pénal 1994, comm.84
[153]M-L.RASSAT, op.cit., p.153, nº126
[154]Cass.Crim.17 mai 1993, Dr. Pénal 1993, comm.237
[155]Cass.Crim.25 fév. 2004, Bull.nº53, Dr. pénal 2004, comm.91 ;31 janv.2007, Dr. pénal 2007, comm.56
[156] تمييز جزائي غرفة ٧ قرار رقم ٣٢٣ تاريخ ٢٠٠١/١٠/٢٣،كساندر إلكتروني:"المدعى عليه أقدم عن طريق المناورات الاحتياليه على حمل المدعي على تسليمه الشيك...مقابل تحويل مبلغ يفوق قيمة الشيك...موهماً إياه أن هذا التحويل تقبض قيمته خلال أيام وأيد ذلك شخص ثالث مع أنه تبين أن الحساب المحول عليه لم يكون فيه مؤونة ..."

plus efficace qu'on ne le crois puisqu'il apparait sincère , tel est l'exemple d'un comptable attestant de bonne foi l'exactitude de documents faux, ou un inspecteur du travail autorisant un faux licenciement qu'il pensait valide….

Toutes ces constatations sont valides que l'on soit confronté à de tels cas en droit français ou en droit libanais puisque les mêmes solutions sont applicables dans ces deux droits.

En surplus de tout ce qui précède, le droit libanais fait une référence expresse, qu'on ne retrouve pas aussi clairement en droit français, aux situations dans lesquelles l'escroc est en présence de circonstances extérieures[157] qui lui facilite les choses et dont il a su tirer profit pour tromper sa victime[158] [159].

Il faut bien noter pour conclure ce paragraphe que l'escroquerie n'existe pas, selon une jurisprudence constante de droit français et de droit libanais, lorsqu'il est facile pour l'éventuelle victime du délit de découvrir les manœuvres frauduleuses ou le mensonge de l'escroc avec un minimum de précautions de sa part[160]. En dehors des mises en scène et manœuvres frauduleuses prouvées, pas de qualification d'escroquerie, il ne sera question que d'un litige de nature purement civile[161] .

Une fois que nous avons passés en revue les moyens classiques d'escroquerie en les illustrant d'exemples dans le titre premier ci-dessus, nous étudierons dans le second titre de cette première partie les modalités de répression de ces moyens (Titre 2).

---

[158] إستئناف بيروت، ٤ / ٣ / ١٩٩٦ ، النشرة القضائية ١٩٩٦ ، ج ١ ، ص ٨٠ :" المدعى عليه إستغل ظرف إستفاد منه وهو استيلاءه على مال المدعي بصفته مديراً للمصرف إذ أنه إستلم الشيك من زوجة الأخير موهماً إياه بأنه سيودع قيمته في المصرف ولكنه لم يفعل...

[158] فيلومين يواكيم نصر ، مرجع سابق، ، ص . ١٥٨

[159] تمييز جزائي، غرفة ٦، قرار رقم ١٤٧ ، تاريخ ٢٧ / ٥/ ٢٠٠٤، كاساندر إلكتروني :"المدعى عليه إستغل ظرف وجود السيارة في معرضه(اودعها صاحبها فقط لغاية العرض لا للبيع) فعمد إلى بيعها ،مدعياً بأنها تعود له وأنه بصدد سحب أوراقها من إدارة الجمارك ليقوم بعد ذلك بتسجيلها على إسم (المدعي)، فصدقه هذا الأخير ودفع له الثمن نقداً وبموجب شيكات ،و لكن السيارة أعيدت إلى صاحبها ، في حين إحتفظ المدعى عليه بالثمن لنفسه ... الاستلاء على المال قد تم بالإستناد إلى مناورات احتيالية مورست من قبله على المدعي".

[160] فيلومين يواكيم نصر ، مرجع سابق، ، ص . ١٦٣

[161] تمييز جزائي، غرفة ٦ ، قرار رقم ٧٠ ، تاريخ ١٠ / ١ / ٢٠٠١ ، صادر ١٢٠٧ / ٢٠٠١ : " حضور المدعى عليه إلى سوق الخضار في طرابلس وزعم أنه من كبار التجار وذو ملاءة كبيرة، مجرد هذا الزعم غير كافٍ لأن يشكل مناورة احتيالية طالما أنه لم يعززه بمناورات أو أدلة تؤدي إلى وقوع المدعي بالغلط"

Titre 2: Les modalités de répression des moyens classiques:

L'escroquerie est une infraction intentionnelle accomplie par l'escroc, dans le but de «tromper» la victime et la pousser à lui remettre la chose convoitée.

En effet, l'escroquerie n'est considérée comme accomplie, même une fois l'intention de son auteur parfaitement établie, qu'au moment où la remise est effectuée par la victime.

D'où la nécessité d'expliquer sous le premier chapitre de ce second titre d'une part l'intention qui anime l'escroc et les buts qu'il peut poursuivre et d'autre part la remise provoquée et ses caractéristiques (Chapitre 1).

Nous consacrerons par la suite le second chapitre de ce second titre aux sanctions, prescription et immunités relatives au délit d'escroquerie (Chapitre 2).

Chapitre 1: L'exigence d'une intention et d'une remise

Le premier élément essentiel et indispensable pour conférer à des actes délictueux la qualification d'escroquerie est l'existence d'une intention frauduleuse animant l'escroc. La preuve de cette intention et des motifs poursuivis par l'escroc est donc plus qu'impérative. C'est aux juges de fond qu'il reviendra tant en droit libanais comme en droit français d'apprécier l'existence de cette intention frauduleuse et de révéler les motifs de l'auteur de l'escroquerie. Nous traiterons donc dans la première section de ce chapitre de l'intention frauduleuse et des motifs de l'escroc (Section 1).

Nous consacrerons la seconde section du chapitre à l'étude détaillée du second élément indispensable qui est la remise par la victime de la chose convoitée par l'escroc (Section 2).

Section 1: L'exigence d'une intention frauduleuse

La nécessité de la présence d'une intention frauduleuse est indiscutable (Paragraphe 1). C'est l'indifférence des motifs ou buts poursuivis par l'escroc, aussi variés qu'ils peuvent s'avérer, qui peut être remise en cause (Paragraphe 2).

Paragraphe 1: Nécessité d'une intention frauduleuse

Rien ne peut être accompli sans une intention, surtout pour une infraction aussi grave qu'une escroquerie[162], mais en quoi consiste cette intention?

L'escroquerie étant un délit intentionnel, les deux droits français et libanais[163][164] exigent pour le caractériser que l'élément matériel soit doublé d'un élément moral spécifique: l'intention frauduleuse[165][166]. L'intention frauduleuse exigée[167] n'est rien d'autre que la volonté criminelle de l'escroc de tromper sa victime pour la déterminer à lui remettre la chose convoitée[168].

---

[162] تمييز جزائي، غرفة ٧ ، قرار رقم ٢٦٨، تاريخ ١١ / ٨ / ٢٠١٦ ، كاساندر إلكتروني :" نية إبتزاز الأموال هي شرط لتحقق عناصر جنحة الاحتيال ..."

[١٦٣] القاضي البدائي الجزائي في الدامور (٢١ كانون الثاني في ١٩٦٠)(...) "ولا بد كي تستقيم جريمة الإحتيال من وجود النية الجرمية لدى الفاعل أي أن يعرف أن الوسائل التي يستعملها غير مشروعة وأن تكون لديه في نفس الوقت اردت الحصول على منفعة من غي حق "... وحيث أنه لك تستقيم جريمة الاحتيال لا بد من وجود النية الجرمية لدى الفاعل أي أن يعرف أن الوسائل التي يستعملها غير مشروعة وأن تكون لديه في نفس الوقت اردت الحصول على منفعة من غير حق"

[١٦٤] محكمة إستئناف جبل لبنان، قرار رقم ٧٤، تاريخ ٢٨ / ١ / ٢٠١٠ ، كاساندر إلكتروني:" المحكمة تشدد على ضرورة وجود العنصر المعنوي الذي يتجلى بالنية الجرمية ، وتشير إلى المادة ١٨٨ عقوبات أي القصد الجرمي العام المتمثل بالعلم والارادة وبقصد خاص قوامه نية تملك المال موضوع الاعتداء..."

[١٦٥] محكمة إستئناف جبل لبنان، الغرفة التاسعة الجزائية، قرار رقم ٣٨١، تاريخ ١٢ / ٤ / ٢٠١٠ ، كساندر إلكتروني:" جريمة الاحتيال تفترض عنصر مادي وأخر معنوي ويجب أن يتوافرا معاً... العنصر المعنوي يتجلى بتوافر النية الجرمية لدى الفاعل عند اقدامه على المناورات الاحتيالية، أي أن يتوافر لديه القصد الجرمي المؤلف من العلم بأنه يرتكب جريمة إحتيال ومن الارادة الحرة من أي قيد أو ضغط أو إكراه والمتوجهة إلى إقتراف الفعل الجرمي، هذا إلى جانب القصد الخاص المتمثل في توافر نية تملك الشيء المستولى عليه..."

[166] تمييز جزائي، غرفة ٦، قرار رقم ٥١ ، تاريخ ١٠ / ٢ / ٢٠١٥ ، كاساندر إلكتروني:" يشترط قانوناً من أجل الادانة بالمادة ٦٥٥ عقوبات ، توافر كل مكونات عنصريها المادي والمعنوي مجتمعة، عنصر الاحتيال المادي يتألف من المكونات التالية... موضوع الاعتداء هو ألحق اللذي تستهدفه الأفعال الجرمية... فعل الاعتداء المتكون من واحدة أو أكثر من المناورات... المعددة على سبيل الحصر في الفقرة الثانية من المادة ٦٥٥... النتيجة الجرمية... صلة سببية بين المناورات والنتيجة الجرمية... والعنصر المعنوي يتكون من القصد الجرمي العام أو النية الجرمية كما حددتها المادة ١٨٨ عقوبات... ومن القصد الخاص الذي اشترطت توافره المادة ٦٥٥ عقوبات ..."

[167] القاضي المنفرد الجزائي في طرابلس، قرار رقم ٧٠ ، تاريخ ٣٠/ ١/ ٢٠١٤، كاساندر إلكتروني :"لتحقق عناصر جرم الاحتيال، لا بد وأن يثبت قيام المدعى عليه بمناورات احتيالية ترمي إلى خداع المدعي، وبالنتيجة إلى اقناعه بتسليم المدعى عليه المال تمهيداً للإستيلاء عليه ... ولا بد أن تقوم النية الجرمية لدى المدعى عليه بعنصريها العلم والارادة بحيث يعلم المدعى عليه حقيقة الفعل الماضي الذي يرتكبه وتتجه ارادته إلى تحقيق النتيجة الجرمية : الاستيلاء على مال المدعي"

[١٦٨] محكمة إستئناف جبل لبنان، الغفة التاسعة الجزائية، قرار رقم ٨٧٠، تاريخ ١٢ / ٧ / ٢٠١٠ ، كاساندر إلكتروني:" جرم الاحتيال يفترض لتوافر عناصره قيام عنصر مادي ... مناورة احتيالية المحددة حصراً في الفقرة ٢ من المادة ٦٥٥ عقوبات ...

Partant de cette exigence légale, le délit d'escroquerie n'a pas lieu d'être si l'agent avait pour unique intention de servir sa mégalomanie, ou s'il est de bonne foi croyant vraiment en son pouvoir imaginaire, à son droit au faux nom ou à la fausse qualité qu'il utilise. De là, nous approuvons la décision rendue par les tribunaux français selon laquelle *«il n'y a pas d'escroquerie si l'auteur croit de bonne foi, avoir le droit de porter le nom ou de se prévaloir de la qualité»*[169].

Rappelons à ce propos que les deux droits français et libanais se rejoignent sur le fait que l'intention criminelle ne se confond pas avec le mobile qui anime le coupable. Les deux droits affirme qu'il escroquerie peut avoir lieu même si le mobile de son auteur n'est pas malhonnête[170].

L'intention est la conscience de réaliser un acte qui est défendu par la loi[171]. En d'autres termes l'intention est la connaissance du caractère frauduleux des moyens utilisés par l'auteur et la conscience du préjudice causé à la victime.

Le mobile quant à lui peut uniquement servir de moyen de réduction de la peine d'escroquerie. Tel est l'exemple d'un créancier qui, au lieu de recourir aux voies de droit pour obtenir ce qui lui est dû, s'approprie le bien de son débiteur d'une façon frauduleuse pour se dédommager, ce créancier sera passible d'escroquerie si la preuve de l'existence de tous les éléments de ce délit est rapportée.

C'est toujours à la victime de l'escroquerie qu'il incombe de rapporter la preuve de la mauvaise intention de l'escroc et de l'intention frauduleuse de ce dernier[172]. Étant donné que l'absence de l'intention délictueuse nie l'existence du délit d'escroquerie. Ceci est valable même si le moyen utilisé par l'agent a bel et bien était déclaré comme une véritable manœuvre frauduleuse[173].

إلى جانب عنس معنوي يتجلى بالنية الجرمية كما حددتها المادة ١٨٨ عقوبات ، أي القصد الجرمي العام المتمثل بالعلم والارادة وبقصد خاص قوامه نية تملك المال موضوع الاعتداء..."

[169]Cass.Crim.20 Jan. 1855, S.1855.1.384

[170]Cass.Crim.15 déc.1943, D.1945.131 (Veron Michel, droit pénal spécial. 6ème édition)

[171]J.PRADEL, M.DANTI-JUAN, op. cit., p. 632, nº893.

[172] الهيئة الاتهامية في جبل لبنان، قرار رقم ٣٤٠ ، تاريخ ٥ / ٥ / ١٩٩٨ ، النشرة القضائية ١٩٩٨ ، ج.٥ ، ص. ٥٦٥ : "إن جرم الاحتيال يفترض نية الاستيلاء لدى المدعى عليه على مال المدعي ، بإنكاره عليه أو عدم اعادته بهدف تملكه. أن يكون المدعى عليه قد إعترف للمدعي، بموجب الكتاب المسجل لدى كاتب العدل ، بحقوقه المالية وأقر له بإلتزامه بها وتعهده له بدفعها في مهلة معينة ، بذلك يسقط عن نفسه قصد الاستيلاء على مال المدعي "

[173] القاضي البدائي المدني في المتن، قرار رقم ١١٦ ، تاريخ ٢ / ١٢ / ١٩٥٩ :" " ينتفي وجود جرم الاحتيال إذا انعدمت النية الجرمية لدى الفاعل ولو إستعمل هذا الأخير الأساليب كالكذب المجرد ولو بالكتابة وأعيد وقرر ذلك لأن الكذب العادي لا يحدث تأثيراً فعالاً لتعريه من كل فعل ماضي وعن كل وسيلة من وسائل الاحتيال فلا يوجد في هذه الحالة إلا ما يسمى بالتدليس المدني "

Partant de tout cela, il est évident que les fautes d'imprudence ou de négligence ne tombent pas sous le coup de l'escroquerie et ne peuvent en aucun cas constituer l'élément moral de ce délit.

L'appréciation de l'intention frauduleuse appartient en droit libanais comme en droit français aux juges du fond[174], il leur revient de constater son existence après un examen minutieux des faits de l'espèce. A cette fin, les cours de cassation française et libanaise apprécient le comportement de l'escroc tout en se plaçant au moment de l'accomplissement des manœuvres et de la remise pour exercer par la suite *«son droit de contrôle sur les appréciations des cours d'appel et vérifier si les faits, tels qu'ils résultent des constatations des arrêts, constituent le délit*» d'escroquerie[175].

On citera à ce sujet un arrêt récent de droit libanais 2012[176] qui illustre parfaitement l'exigence de la nécessité d'existence d'une intention frauduleuse: le défendeur avait reçu une quantité de sacs de chips sans en payer le prix immédiatement à condition que le paiement soit effectué une fois que ce marchand vendra les sacs. Le défendeur n'a pas remboursé la marchandise même après avoir reçu un avertissement. La cour de cassation l'a jugé coupable du délit d'escroquerie vu qu'il avait l'intention dès le début de ne pas rembourser l'argent ni le prix et qu'il était «*conscient qu'il était dans l'impossibilité de payer* »

Les événements qui ont lieu postérieurement à la remise n'excluent point l'existence de l'élément intentionnel de l'infraction. De là, la restitution par exemple de la somme escroquée n'efface pas l'intention, cet acte n'est considéré qu'un acte repentir.

L'escroc ne pourra prétendre qu'il est de bonne foi et échapper à une éventuelle incrimination que dans deux cas. L'escroc pourra invoquer qu'il croyait, au moment de l'accomplissement des manœuvres, à la réalité de l'entreprise ou qu'il était inconscient d'avoir utilisé un des moyens frauduleux énumérés par la loi. Par contre, l'escroc ne peut prétendre être de bonne foi lorsqu'il réalise une mise en scène organisée, telle la création d'une société fictive, ou présentation de fausses factures…

---

[174] تمييز جزائي، غرفة ٦، قرار رقم ١٩٣، تاريخ ١ / ٧ / ٢٠٠٤ ، كاساندر إلكتروني :" يعود لمحكمة الأساس تقدير وقائع الدعوى ويعود لها ألحق المطلق في تقدير الأدلة و... مدى توافرها على تحقق النية الجرمية ..."

[175] Cass.Crim.8 Déc. 1955. Bull. crim. nº 553

[176] تمييز جزائي، غرفة ٣، قرار رقم ١٨٦, تاريخ ٢٠١٢/٥/٢٤ ، كساندر إلكتروني

Paragraphe 2 : L'indifférence des motifs

L'ancien CPF fournissait, à son article 405, une liste précise des buts poursuivis par l'escroc. Ces buts énumérés de façon restrictive étaient les suivants: 1- convaincre la victime de l'existence de «fausses entreprises » ce but vise, comme nous le verrons, à tromper la victime sur la situation réelle de l'escroc qui s'attribue par exemple un pouvoir au sein d'une fausse entreprise ou même inexistante ou encore créer l'illusion d'une solvabilité mensongère; 2- l'allégation d'un pouvoir ou d'un crédit imaginaire; 3-la crainte ou l'espérance d'un événement fantaisiste qui lui serait défavorable ou même l'espérance d'un événement bénéfique.

Malgré la disparition de cet article, et son remplacement par le nouvel article 313-1 CPF, on constate que la jurisprudence française a toujours recours à cet ancien article qui couvre tout genre de but.

Le nouveau CPF offre quant à lui un champ d'application beaucoup plus vaste lorsqu'il omet volontairement de reprendre la trilogie des buts visés à l'ancien art 405 CPF et ne fait que préciser que les moyens frauduleux doivent avoir pour but «*de tromper la victime et la déterminer à remettre à l'escroc le bien convoité*». C'est ainsi que la trilogie de buts poursuivis par l'escroc a été remplacée par le seul acte positif de «tromper» peu importe le procédé utilisé par l'escroc.

En s'attardant sur le droit libanais, on notera que les dispositions de l'article 655 CPL sont un mélange de l'ancien article 405 CPF et du nouvel article 313-1 CPF, puisqu'elles énumèrent limitativement les manœuvres frauduleuses tout en permettant une vaste interprétation de cet élément matériel.

Ce manque de précision en droit français et l'énumération large en droit libanais sont voulues par les législateurs tant français que libanais. En effet, l'imprécision et l'énumération extensive donnent aux tribunaux des deux pays la possibilité d'incriminer n'importe quelle tromperie en donnant une interprétation extensive aux deux textes des articles 655 CPL et 313-1 CPF.

Nous passerons en revue ci-dessous les buts poursuivis par l'escroc en adoptant la trilogie des buts telle qu'elle était prévue par l'ancien code pénal français et reprise dans les articles libanais vu que ce sont les trois principaux buts auxquels viennent s'ajouter d'autres buts de moindre importance:

Le premier but de l'escroc pourrait être celui de persuader sa victime de l'existence de fausses entreprises[177].

La fausse entreprise peut être une société fictive[178] ou une entreprise partiellement fausse[179]. C'est le cas lorsque l'objet ou l'activité de cette société ou entreprise est agrandi d'une façon fallacieuse par de fausses commandes[180].

La fausse entreprise peut également être une pure invention de l'escroc qui se procure de faux documents attestant l'existence de locaux loués, d'un personnel embauché, de papiers à en-tête... ou même la distribution de dividendes fictifs par l'emploi de moyens frauduleux. En somme la fausse entreprise prise en son sens large est synonyme de tout projet qui est *«entrepris, organisé et monté de façon fallacieuse sans prendre la forme d'une société »*. Tel est le cas qu'une organisation qui prétend être charitable et qui recueille des dons au profit des handicapés[181].

Nous retenons l'excellente définition donnée par la cour criminelle dans l'un de ses arrêts[182] et qui reflète judicieusement la consistance de la fausse entreprise : «*Est fausse entreprise non seulement celle qui est entièrement chimérique, mais encore*

---

[177]Le terme «entreprise» s'étend à toute société qui exerce une activité industrielle ou commerciale.

[178] القاضي المنفرد الجزائي في المتن، قرار رقم ١٧٣، تاريخ ٩ / ١١ / ٢٠٠٦، كاساندر إلكتروني:"المدعى عليه مارس مناورات احتيالية أقنع نتيجتها المدعي بوجود مشروع يتمثل بتشييد بناء للسفارة في لبنان، ويتوجب في سبيل أن يس التلزيم على المدعي قيام هذا الأخي بتأمين مبلغ مالي، ... وحيث ان مشروع بناء السفارة غير موجود وأن الخائط المبرزة هي وهمية المعطيات تؤكد إنطباق أفعال المدعى عليه على جنحة الاحتيال" ..

[١٧٩] محكمة إستئناف الجناح في جبل لبنان، قرار رقم ٣٤٣،تاريخ ٢٠ / ٦ /٢٠١٢ ، كاساندر إلكتروني :" المدعى عليه أوهم المدعي بوجود مشروع يتمثل ببيع أجهزة لتنقية المياه في المنازل ... وقد انطلت المناورات على المدعي الذي سلمه مبلغ من المال لتمويل الشركة... لكن المدعى عليه إستولى على المبلغ الذي إستلمه من المدعي و راح يستورد الأجهزة ويبيعها لحسابه ...ولم تقم الشركة بأي نشاط تجاري حقيقي... وتبين للمدعي أن المشروع وهمي ولا وجود لبضاعة...وهي تتعاطى الحفلات الفنية... وعرض الأزياء... ولا علاقة لها بأي مشروع تجاري..."

[180]Cass.Crim.20 fev.1974, Bull. nº76

[181]Cass.Crim.10oct.1977, Bull. nº298

[182]Cass.Crim.25 juin 1978, Bull.crim.4.243, R.C.S.1981.393

celle qui, ayant quelque réalité sur certains points, présente dans d'autres parties qui la composent des circonstances entièrement fausses».

Même si le législateur libanais n'en donne pas une définition exacte et précise[183], il reconnait l'existence des fausses entreprises. Mieux encore, il requière l'existence d'actes ou comportements spécifiques révélateurs du caractère fictif de l'entreprise ou du moins la présence de faux bilans ou faux documents attestant son existence. Le droit libanais rejoint le droit français en exigeant que les actes entrepris par l'escroc fassent réellement naitre chez sa victime une confiance certaine qui l'induit en erreur sur l'existence de la fausse entreprise[184]

Le deuxième but de l'escroc consiste à persuader sa victime d'un pouvoir ou d'un crédit imaginaire dont il ne dispose pas en réalité. L'escroc essaye ainsi d'exploiter la naïveté de sa victime en utilisant un pouvoir imaginaire dans les domaines de magies, devins, hypnotise, astrologie…et mène la victime dupée à lui remettre une somme d'argent considérable[185] en lui faisant croire à la possibilité d'obtenir en sa faveur des décisions judicaires favorables. S'agissant de tels cas de charlatanisme la preuve de l'escroquerie est difficile à rapporter puisqu'il faut en premier lieu prouver que le pouvoir que l'escroc s'attribue est imaginaire et que ses «dons» de guérison, de pensée, de pouvoir miraculeux[186] ne sont en réalité que des hérésies.

Il peut également être question d'un crédit imaginaire. C'est le cas quand l'escroc trompe sa victime sur la surface financière [187]ou la solvabilité d'un individu ou d'une entreprise: établissement de fausses factures, ouverture de comptes alimentés par des chèques sans provision, présentation de cartes falsifiées. La jurisprudence

---

[183] فيلومين يواكيم نصر ، مرجع سابق، ، ص . ١٥٥

[184] تمييز جزائي، غرفة ٧ ، قرار رقم ١٧٣ ، تاريخ ٢٠ / ٦ / ٢٠٠٢ ، صادر ١٠٥٣ / ٢٠٠٢: " تحقق جنحة الإحتيال لدى حمل المدعية على تسليمه مبلغاً من المال موهماً ايها بوجود مشروع بناء تبين أنه وهمي "

[185] Cass.Crim.3 Mai 1961. Bull. Crim. nº232: «*le pouvoir imaginaire, l'autorité, la puissance, l'influence contraires à la réalité, est par exemple celui auquel prétend l'individu qui exploite la superstition d'autrui, affirmant guérir certaines maladies*».

[186] M.VERON, op.cit., éd.2010,p.294, nº 420.

[187] محكمة جنايات جبل لبنان، قرار رقم ٣٦٩، في ١٨ /٥/ ٢٠٠٠ ، كساندر إلكتروني :"المتهم ... إستعمل المناورت الاحتيالية بحق... موهماً إياه أنه بصدد جلب مبلغ خمسة وعشرون ألف دولار أميركي، فوقع ضحية هذه المناورة وسلم... ما طلب منه"

française[188] a retenu ce genre de manœuvres dans plusieurs de ses arrêts, et il est évident que la même solution s'impose en droit libanais pour ce genre de cas.
Le troisième but poursuivi par l'escroc est celui de «faire naitre l'espérance ou la crainte d'un succès, d'un accident ou de tout autre événement chimérique» Cette formule englobe les deux hypothèses déjà citées, mais a l'avantage d'incriminer des tromperies qui ne portent ni sur une entreprise, ni sur un crédit ou un pouvoir, tel le cas de réussite à un examen, maladie, décès… Une illustration célèbre est l'affaire «Thérèse Humbert» nom associé à l'affaire de l'héritage Crawford[189].

Un événement est considéré comme étant chimérique lorsqu'il est inexistant: « *l'événement chimérique peut être l'espoir d'un gain en jeu, l'espoir d'un mariage… il s'agit d'une question de fait dont l'appréciation entre dans les pouvoirs souverains des juges de fond* »[190]. N'est pas considéré comme chimérique l'événement irréalisable à cause d'un échec ou une insuffisance dans les moyens mis en œuvre.

Les événements chimériques auxquels recourent le plus souvent les escrocs sont: l'activité des marchands d'objets miraculeux, la vente de pronostics hippiques ou ludiques, les agences matrimoniales fictives, les offres d'emplois fictives... les exemples jurisprudentiels français et libanais sont nombreux[191]: un escroc convainc un vieil homme de lui remettre de l'argent, en lui faisant croire qu'il va lui assurer

[188]Cass.Crim.19 oct. 1957, Chambre criminelle, 6 octobre 1977, chronique de jurisprudence, commenté pat Pierre Bouzat, Crimes et délits contre les biens, page 357: « *le crédit imaginaire existe dans le fait de commettre des escroqueries à la TVA ; des entreprises commerciales obtenant de l'administration fiscale le remboursement d'un crédit d'impôt prétendument versé par des firmes de façade auxquelles elles sont liées par des relations d'affaires purement fictives* ».

[189]En l'espèce Humbert avait prétendu avoir reçu d'un millionnaire americain Robert Henry Crawford une partie de son héritage. Elle obtient par conséquence d'énormes prêts bancaires en utilisant le supposé héritage comme garantie. Or il s'est avéré que le fameux coffre-fort où sont censés se trouver les documents prouvant l'héritage ne contient qu'une brique et une pièce d'un penny.

[190]Cass.Crim.16 Avril 1975.Bull. Crim. nº95

[١٩١] تمييز غرفة ٦ قرار رقم ٢١٤ تاريخ ٢٠٠٥/٧/١٩،كاساندر إلكتروني:"المستدعى ضده لفق أكذوبة على والده واهماً إياه أنه يستطيع تأمين سفره إلى لندن... "

son entretien et son logement jusqu'à sa mort[192]; ou vend des listes d'appartements à louer ou à acheter, malgré le fait que ces derniers sont déjà occupés[193].

Il est intéressant de faire référence à un arrêt rendu par la cour d'appel de Paris le 14 février 1978[194] relatif à un crédit imaginaire hors du commun. Il s'agissait d'une église de scientologie qui avait fait des promesses chimériques, de réussite professionnelle et de guérison de maladies psychosomatiques, alors que son véritable but n'était que la collecte frauduleuse d'un nombre élevé de fonds.

Le droit libanais prévoit lui aussi des cas d'escroquerie nés d'une espérance d'un crédit imaginaire, d'un événement chimérique, ou du fait de persuader la victime de l'existence d'un pouvoir ou d'un crédit imaginaire[195], à la condition que tous ces actes soient antérieurs à la remise faite par la victime. Nombreux arrêts rendues par les différentes cours libanaises en témoigne: guérisons fictives de maladie[196]; procuration de fausses attestations universitaires et de faux relevés de note[197].On citera également un arrêt libanais intéressant de 2012[198] ou une société dont l'objet principal était l'organisation de festivals et de compétitions de beauté a été condamné pour escroquerie car elle avait mis en place une mise en scène avec un projet fictif relatif à des appareils d'entretien et de filtration d'eau.

[192]Cass.Crim.7 mai 1974, Bull. nº160, JCP1976.II.18285

[193]CA Paris, 17 nov. 1983, Gaz.Pal. 1984.2.644 (V. M-P. LUCAS DE LEYSSAC, A. MIHMAN, op.cit., p. 57)

[194]CA Paris, 14 fév.1978, note par Pierre Bouzat, crimes et délits contre les biens, Rev.sc.crim.1978, p.358: en l'espèce les manœuvres de l'église débutent par un test de personnalité gratuit fait à des personnes suivi d'une invitation à des cours qui aident à l'épanouissement et au développement de la personnalité suivis de promesses chimériques, de réussite professionnelle et de guérison de maladie psychosomatique.

[١٩٥] محكمة الاستئناف الجزائية في بعلبك ، قرار ١٣٤ ، ٢٢ / ١٠ / ٢٠٠١ "تعتبر مناورات احتيالية ، الأعمال المادية الملازمة بالإدعائات الكاذبة التي من شأنها ايهام المجنى عليه بوجود مشروع وهمي ، أو التي تخلق في ذهنه أملاً بربح"

[١٩٦] جنايات جبل لبنان، قرار رقم ٤٣٥ ، تاريخ ٢٧ / ١٠ / ٢٠٠٥ ، كساندر ٢٠٠٥ ، ج ١٠ ص ١٩٠٤ :" إن إقدام المتهم على حمل المدعيتين على تسليمه أموال واستيلائه عليها إحتيالاً بعد أن أوهمهن بأنه يشفي من الأمراض عن طريق مناجاة الأرواح يشكل جنحة المادة ٦٥٥ "

[١٩٧] جنايات بيروت غرفة ٧ ، قرار ١٨٦ ، ١٨ / ٣ / ١٩٩٧ : "حيث أنه ثابت بالوقائع والأدلة إقدام المتهمين على الاستيلاء على المال باستعمالهما مناورة احتيالية تمثلت بتعهدهما له بالحصول على شهادة جامعية وبيان بالعلامات ، ولم يؤمنوا له في الحقيقة سوى صورة فوتوكوبية عن شهادة جامعية ، هذه تشكل جنحة الاحتيال "

[١٩٨] محكمة إستئناف الجناح في جبل لبنان، قرار رقم ٣٤٣ ، تاريخ ٢٠ / ٦ / ٢٠١٢ ، كساندر إلكتروني

En tout état de cause, l'appréciation du caractère chimérique relève donc du pouvoir souverain des juges du fond, qui se placent au moment des manœuvres et de la remise sans tenir compte du résultat ou des éléments postérieurs à celle-ci.

Section 2: L'exigence d'une remise

La remise est l'élément clé qui différencie l'escroquerie du vol, l'escroc ne saisit pas directement la chose qu'il désire, elle lui est remise par la victime ou par une personne agissant pour le compte de sa victime[199].

L'escroquerie est considérée comme un délit instantané, qui se réalise au moment de la remise qui est le point de départ de la prescription[200].

La remise peut revêtir plusieurs formes, selon l'objet de l'escroquerie : matérielle en cas de meuble corporel, et exécution de la prestation en cas d'escroquerie portant sur un bien immatériel. Nous passerons donc en revue ci-dessous la spécificité de l'objet de l'escroquerie et les modalités de sa remise (Paragraphe 1) ainsi que la nécessité d'un lien de causalité et d'un résultat préjudiciable (Paragraphe 2).

Paragraphe 1: Spécificités de l'objet

L'escroquerie est considérée consommée dès lors que la remise de la chose convoitée est obtenue. D'où l'existence du bien objet de la remise est une condition préalable, pour qu'un délit soit qualifié d'escroquerie. De là l'importance de savoir quel genre de bien peut-il faire l'objet de la remise frauduleuse ?

Dans l'ancien CPF, l'escroquerie pouvait porter uniquement sur des fonds, des meubles, des obligations, promesses, quittances, décharges... l'escroquerie ne pouvait donc pas porter sur un bien immeuble ce qui est toujours le cas aujourd'hui.

Mais avec le nouveau CPF et conformément aux dispositions claires de son article 313-1, l'escroquerie peut désormais porter sur des fonds (espèces liquide), des

[199] M.VERON, op.cit., éd.1998,p. 213

[200] الهيئة الاتهامية في جبل لبنان، تاريخ ١ / ٤ / ١٩٨٥ ، العدل ٨٦ ، عدد ٤ / ٥٠٩ ، (فيلومين يواكيم نصر، مرجع سابق، ص. ١٧٤)

valeurs (valeurs mobilières, chèque ou ordre de virement et autres valeurs telles les bijoux) ou des biens quelconque corporels et incorporels tel les informations, ainsi que sur un acte opérant obligation ou décharge. Dans tous les cas de figure le bien doit avoir une valeur monétaire. Il s'en suit que l'escroquerie peut porter sur tout élément exploitable, même sans consistance matérielle comme sur l'obtention d'une idée ou une information[201].

Le droit libanais adopte cette même position et considère que l'objet de l'escroquerie peut être un bien quelconque meuble ou la fourniture d'un service[202] à l'exclusion également des biens immeubles insusceptibles de remise. La doctrine libanaise définit les meubles pouvant faire l'objet d'escroquerie comme *«tout objet qui peut être déplacé d'un endroit à l'autre à condition qu'il soit apte à être approprier»*, sachant qu'on n'accorde aucune importance à la valeur matérielle ou morale du bien convoité ni au fait que sa possession ait été faite de façon illégale ou délictueuse[203].

Cependant, il est important de préciser que les deux droits français et libanais admettent que l'escroquerie porte sur les prix des immeubles lorsqu'ils sont augmentés par des manœuvres frauduleuses, ou sur le titre translatif de propriété de l'immeuble ou sur les droit réel sur un immeuble: « *les immeubles sont exclus. Cependant cette règle est de droit étroit car il peut y avoir escroquerie du prix de l'immeuble dont la valeur a été surestimée en raison de manœuvres frauduleuses* »[204].

La jurisprudence française a admis comme nous l'avons déjà signalé plus haut «l'escroquerie au jugement» elle a considéré que l'objet de la remise est un jugement favorable obtenu par des manœuvres ayant pour but de surprendre la juridiction saisie, par le recours à de faux témoignages ou par la production de faux documents ou de documents mensongers. Nous ne retrouvons pas la même solution en droit libanais puisque l'escroquerie au jugement n'y est toujours pas incriminée et qu'un jugement ne peut pas être considéré comme objet de l'escroquerie.

---

[201] M-L. RASSAT, op.cit., p.140, nº.114

[202] فيلومين يواكيم نصر ، مرجع سابق، ص ١٥١

[203] Idem

[204] Crim.15 juin 1992, B.C. nº235, Dr. pénal 1992, comm.281

D’autre part, la fourniture d’un service constitue le second objet pouvant faire l’objet de la remise frauduleuse.

La notion de fourniture de service n’existait pas en droit français avant 1994. En effet, avant cette date, la remise frauduleuse était limitée aux cas de remise matérielle. Les exemples non incriminés sous le coup de l’ancien CPF étaient nombreux nous pouvons en citer: l’utilisation de coupon d’un tiers ou le cas d’un transport avec un billet falsifié, vol d’information, vol d’usage, soustraction par photo copiage, les manœuvres destinées à éviter de payer le cout d’une communication téléphonique[205].

C’est avec le nouveau CPF que les manœuvres frauduleuses tendant à l’obtention d’un service sont désormais punissables. Les escroqueries tendant à la fourniture d’un service consistent pratiquement à obtenir, grâce aux moyens frauduleux, des prestations qui sont gratuites ou même à un prix réduit.

Le champ d’application de l’escroquerie est devenu donc plus étendu en droit français et comprend désormais l’obtention de la fourniture d’un service.

Notons qu’à l’instar de la remise classique matérielle, la remise ayant pour objet la fourniture d’un service, existe même si : 1- elle est faite de façon indirecte[206], 2- elle est faite à un tiers, 3- si l’agent n’a retiré aucun profit de son acte, 4- si la victime n’a subi aucun préjudice réel vu qu’un simple préjudice moral ou éventuel suffit dans ces cas pour l’incrimination.

Quant au droit libanais, ce dernier reste muet sur la possibilité d’incriminer une remise frauduleuse ayant pour objet la fourniture d’un service[207]. Il fait cependant référence à son article 655 CPL à la notion de «*livraison d’un meuble*». Partant de cette référence, rien n’empêche à notre avis que l’incrimination d’escroquerie englobe en droit libanais les cas de fourniture de service.

[205]Cass.Crim.4mai1987,B.C., nº175

[206]Tel un jeu d’écriture, ou une inscription en compte courant

[207] تمييز جزائي، غرفة ٦، قرار رقم ٤٨ ، تاريخ ٢ / ٢ /٢٠١٦ ، كاساندر إلكتروني :االمادة ٦٥٥ عقوبات لا تشمل الخدمات أو الأشغال التي قد يتم حمل المرء على القيام بها أو ادائها بنتيجة أي تصرف قام به المدعى عليه مع توافر نية عدم دفع الأجر، حتى لو اتسم هذا التصرف بسمات المناورات الاحتيالية "

En outre, il est incontestablement admis que la remise, tant en droit français qu'en droit libanais, peut porter sur un acte opérant obligation ou décharge[208]. On vise par les actes opérants obligation ou décharge les titres qui créent, constatent ou éteignent un droit au détriment de la victime et au profit de l'escroc[209]. En d'autres termes sont concernés tous les actes qui forment un lien de droit par lequel on peut porter préjudice à la fortune d'autrui[210].

Pour plus de précision les actes opérant obligations sont ceux qui créent un lien de droit tout en ayant pour effet de rendre la victime débitrice d'une obligation envers l'escroc. Les exemples les plus courants portent sur des contrats de vente ou de bail ou même de promesses de vente, signature d'un chèque …

Par contre, les actes opérant une décharge sont ceux qui annulent un lien de droit au bénéfice de l'escroc et au préjudice de la victime: c'est le cas par exemple d'une remise de dette, dispense de paiement, quittance….

Que les actes portent sur une obligation ou une décharge c'est la conclusion de l'acte qui importe, et ceci même s'il n'y a pas eu de remise matérielle[211].

Ce sont ces mêmes solutions que nous retrouvons en droit libanais[212] : la remise peut porter sur un acte juridique créant un lien de droit ayant des effets négatifs sur les tiers, qui peut être soit une obligation (tel un contrat de prêt ou une promesse d'achat ou de vente), quittance ou décharge, ou un intérêt.

La jurisprudence française affirme que concernant l'escroquerie au jugement le jugement obtenu de façon frauduleuse conduit le tribunal à *«consentir un acte opérant obligation ou décharge»* [213].On relève également un autre arrêt rendu par

---

[208] تمييز جزائي، غرفة ٦، قرار رقم ١٩، تاريخ ١٥ / ١ / ٢٠٠٤، كساندر ٢٠٠٤ ، ج ١ ص ٦٨ :" المنفعة المتمثلة بالحصول على خدمات طبية أو استشفائية لا تكون محلاً أو موضوعاً للإحتيال ما لم تكن موضوع سند أو تعهد مجسدين بصك..."

[209] M.VERON, op.cit., éd.2010,p.295, nº 421

[210] J.PRADEL, M. DANTI-JUAN, op.cit., p.630, nº. 887

[211] J.LARGUIER, Ph. CONTE, op.cit., p.122, nº.138

[212] فيلومين يواكيم نصر ، مرجع سابق، ص . ١٥٢

[213] Cass.Crim.11 janv. 2006, Dr. pénal 2006, comm.48 ; RSC.2006.596, nº2: en l'espèce, une femme a usé de la fausse qualité de professionnelle de l'hôtellerie et de restauration pour tromper la religion des juges durant une procédure de redressement judiciaire et les déterminer à arrêter un plan de cession à son profit. Elle a été condamnée pour escroquerie au jugement.

la cour de cassation française[214] selon lequel : « *celui qui fournit des instructions à l'un de ses salariés pour empêcher un expert judiciaire de remplir sa mission et tenter ainsi de tromper un tribunal est coupable de complicité de tentative d'escroquerie* ».

Apres avoir énumérer les différents objets pouvant constituer la remise frauduleuse, il faut conclure que l'objet de l'escroquerie n'est pas l'*instrumentum* mais le *negotium* lui-même[215].

Quant aux modalités de la remise, elle peut s'effectuer de manière matérielle directement lorsqu'il s'agit de fonds, ou être opérée de manière indirecte par un virement ou par un jeu d'écritures.

Quand il s'agit d'une information ayant valeur patrimoniale la remise se fait par la délivrance de l'information qui peut se faire par n'importe quel procédé.

Quant aux services qui peuvent faire l'objet de remise, cette dernière se consomme quand l'agent a bénéficié de ceux-ci.

Enfin pour les actes opérant obligation ou décharge la remise peut résulter de la simple signature de l'engagement sans aucune autre formalité nécessaire.

Signalons finalement qu'il est indifférent de savoir par qui la remise a été faite. En effet, l'auteur de la remise peut être le propriétaire du bien, un salarié, le mandataire du propriétaire, et même une personne sans aucun lien juridique avec le propriétaire.

Il est également indifférent de savoir à qui elle a été faite: il importe peu qu'elle bénéficie à un tiers, par exemple au père de l'escroc[216], ou à l'escroc, mais pourvu qu'elle soit provoquée par cet escroc[217].

---

[214]Cass.Crim.6 septembre 2000, Dr. pénal 2001, comm.30: en l'espèce Raymond Marquer a été jugé coupable d'escroquerie au jugement pour avoir procéder à une substitution d'étiquettes destinées à empêcher l'expert judiciaire de découvrir que la contamination de l'ensemble des élevages a été causé par des produits qui étaient contaminés par la salmonelle.

[215]Ph. CONTE, op.cit., p.323, nº563.

[216] تمييز جزائي، غرفة ٣ ، قرار رقم ١٦٦ ، تاريخ ٢٣ / ٥ / ٢٠٠٠ ، كساندر ٢٠٠٠ ، ج ٥ ، ص ٥٩٢ :" وحيث أن محكمة الاستئناف إعتبرت أن عناصر المادة ٦٥٥ عقوبات غير متوفرة بالنظر لأن المدعى عليه لم يسحب الأموال من حساب الشركة لنفسه بل لمصلحة والده، إلا أن نص المادة ٦٥٥ لم يميز بين من تصرف بالاموال لصالح نفسه أو لصالح غيره، فيكون الحكم قد خالف القانون وهو يستوجب النقض ..."

Enfin, les deux droits français et libanais, exigent que la remise de la chose escroquée soit inévitablement postérieure aux moyens utilisés vu que cette remise consomme l'infraction[218] c.à.d. que quand elle n'a pas été accomplie on parlera uniquement d'actes préparatoires[219] et non pas d'un délit d'escroquerie[220].La remise doit également être une remise involontaire[221] [222] et qu'elle soit le résultat de la tromperie causé par les moyens frauduleux[223].

Paragraphe 2: Lien de causalité et préjudice

Les droits français et libanais exigent tous deux un lien de causalité entre les moyens frauduleux et la remise du bien convoité. Ainsi, il faut que les moyens frauduleux mènent directement à la remise du bien entre les mains de l'escroc[224].

Partant de cette exigence légale n'est pas considérée comme victime d'escroquerie, la personne qui a volontairement fait une remise sans être influencée par des moyens frauduleux.

De là, l'exigence du lien de causalité est conditionnée par l'emploi des moyens frauduleux qui lui soient antérieurs. Il revient aux juges de fond de constater d'une

---

[217] Ph. CONTE, op.cit. , p.322, nº.561

[218] تمييز جزائي، غرفة ٦ ، قرار رقم ١٣ ، تاريخ ١٧ / ١ / ٢٠٠٦ ، كساندر ٢٠٠٦ ، ج . ١ ، ص. ٩٩ : "لقيام جنحة الاحتيال قانوناً و لإكتمال اركانها ينبغي أن تسبق المناورات الاحتيالية فعل التسليم "

[219] H. MATSOPOULOU, Infractions contre les biens, Chroniques De Jurisprudence, Chroniques, Octobre/Décembre 2012, page 867

[220] Cass.crim.21 mars 2012, numéro 11-87.453: En l'espèce, l'intéressé avait obtenu de sa compagnie d'assurance le remboursement d'une somme d'argent en réparation du dommage qui résulte du vol de son véhicule, en omettant d'informer la compagnie qu'il l'avait au préalablement retrouvé. La cour de cassation casse l'arrêt d'appel qui ne considère pas que ces actes sont des manœuvres antérieures à la remise par l'assureur des indemnités, ni déterminantes de celle-ci.

[221] تمييز جزائي، غرفة ٦، قرار رقم ١٣ ، تاريخ ١٧ / ١ / ٢٠٠٦، كاساندر إلكتروني :"لا تكون عناصر جريمة الإحتيال متحققة إذا كان تسليم المال إلى المدعى عليه قد حصل بنتيجة إتفاق بينه وبين المدعي على إنشاء مشروع تجاري حقيقي بوشر في اقامته من قبل طرفي الاتفاق ونتج عنه تسليم مبلغ من المال إلى المدعى عليه بهدف شراء معدات لتشغيله، لأن التسليم يكون قد حصل في هذه الحالة بصورة إرادية غير مشوبة بأي عيب من شأنه التأثير على المدعي لدفعه إلى التصرف بماله"

[222] "إن جرم الاحتيال لا يقوم إلا بتوفر عنصر الغش ، فشراء تذكرة سفر بالطائرة دون إستعمال الغش وعدم دفع ثمنها يعتبر نزاعاً مدنياً" (راجع . فيلومين نصر، مرجع سابق، ص . ١٦٩)

[223] تمييز جزائي غرفة ٧ ,قرار رقم ١٣٢, تاريخ ٢٠٠٥/٣/٨ ،كاساندر إلكتروني:"المدعى عليه يملك معرضاً لبيع السيارات المستعملة وقد أودع لديه سيارتين لعرضهما بغية الحصول على ثمنهما مقابل عمولة...المستدعي قام بتسليم السيارتين بنتيجة إتفاق إرادي ولم يقم أية دليل على أن المدعى عليه قد توسل المناورات الاحتيالية لحمله على تسليم السيارتين...الكذب لا يشكل المناورة الاحتيالية المقصودة في القانون..."

[224] فيلومين يواكيم نصر ، قانون العقوبات الخاص ، مرجع سابق، ص . ١٧٥

part l'antériorité des manœuvres et d'autre part l'existence d'un lien de causalité entre les dits manœuvres et la remise.

En cas d'absence du lien de causalité, le délit d'escroquerie perdra son élément matériel, considérée le plus important comme le soulève la doctrine libanaise[225].

Il a été jugé tant en droit français qu'en droit libanais[226] que « *le délit d'escroquerie est suffisamment caractérisé lorsqu'il est constaté que les remises de fonds ont été le résultat des moyens frauduleux employés par le prévenu et qu'elles n'ont pas été librement consenties par celui qui l'a trompé* »[227].

Reste à traiter de l'exigence ou pas d'un préjudice subi par la victime de l'escroquerie.

L'ancienne formulation de l'article 405CPF énonçait que l'escroc devait avoir escroqué «*tout ou partie de la fortune d'autrui* », ce qui nous mène à nous interroger si l'exigence d'un préjudice effectivement subi par la victime est l'un des éléments constitutifs du délit d'escroquerie. En d'autres termes, l'escroquerie suppose-t-elle nécessairement que la victime subisse un préjudice, ou existe-t-elle du seul fait de la remise, indépendamment du résultat?[228] L'escroquerie peut-elle exister même si son auteur n'a tiré aucun profit de l'opération?

La jurisprudence française a répondu par la négative: l'existence d'un préjudice subi par la victime n'est pas un des éléments constitutifs du délit d'escroquerie[229], « *le délit d'escroquerie existe indépendamment de tout préjudice éprouvé par les victimes, dès lors que la remise a été extorqué par des moyens frauduleux et non librement consentie* »[230].

---

[225] فيلومين يواكيم نصر، مرجع سابق ، ص . ١٧٥

[226] القاضي البدائي المدني في المتن ، قرار رقم ١١٦ ، تاريخ ٢ / ١٢ / ١٩٥٩ ، : " لكي تتوفر جريمة الاحتيال أن تتكون علاقة سببية بين وسائل الاحتيال وبين تسليم الشيء أي أن يكون التسليم نتيجة طبيعية واكيدة لعمل المدعى عليه الأمر الذي لم يثبت توفره في القضية الحاضرة "..." ينتفي وجود جرم الاحتيال إذا انعدمت النية الجرمية لدى الفاعل ولو إستعمل هذا الأخير الأساليب كالكذب المجرد ولو بالكتابة وأعيد وقرر ذلك لأن الكذب العادي لا يحدث تأثيراً فعالاً لتعريه من كل فعل ماضي وعن كل وسيلة من وسائل الاحتيال فلا يوجد في هذه الحالة إلا ما يسمى بالتدليس المدني "

[227] Crim. 18 Nov. 1969, Bull.crim.362, D.1970.437

[228] M.VERON, op.cit., éd.1998,p. 215

[229] Cass.Crim.19 déc. 1979, Bull. nº369

[230] Cass.Crim.20 Juin 1983, Bull. nº189

Pour ce qui est de la doctrine française, les opinions sont mitigées: alors que Garçon exige un préjudice comme un élément constitutif du délit d'escroquerie, Garraud adopte quant à lui une position contraire en considérant que le préjudice n'est pas un élément constitutif de l'escroquerie. Reste que la majorité de la doctrine française n'exige pas le préjudice comme un élément constitutif du délit.

Qu'en est-il en droit libanais? Est-ce que le préjudice est une condition indispensable pour qu'il y ait incrimination?

La doctrine et la jurisprudence Libanaises ont aligné leurs positions sur l'opinion dominante de la doctrine et de la jurisprudence française n'exigeant pas de préjudice. Il importe donc peu que l'escroc ait réalisé un gain ou pas et que la victime ait subi un préjudice ou pas, l'escroquerie n'existe que si ses conditions sont réunies[231].

La notion de préjudice est indépendante de la personne qui profite de l'escroquerie, on peut donc condamner comme complice d'une escroquerie le tiré d'un effet de complaisance même si ce dernier n'en tire aucun avantage.

Sous le régime de l'ancien CPF, la jurisprudence française considérerait que le préjudice consistait «*à se faire remettre une chose que la victime n'aurait pas remise si elle avait été éclairé sur la situation exacte* »[232].

Le nouvel article 313.1 CPF dispose par contre que les manœuvres doivent avoir déterminé une remise au préjudice de la victime ou au préjudice d'un tiers. C'est ainsi que le préjudice requis parait inhérent à la remise en raison de la nature patrimoniale de l'objet de cette dernière[233].

Cependant il faut noter que le législateur français n'exige pas que l'escroc ait été enrichi par la manœuvre frauduleuse utilisée[234]. La simple tentative d'escroquerie, se vérifiant par le fait que la victime n'ait rien perdu, est punissable en elle-même. L'absence d'appauvrissement de la victime ne nie donc pas l'existence du délit d'escroquerie. Il est évident également que même au cas où l'escroc répare les

[231] فيلومين يواكيم نصر ، مرجع سابق، ص . ١٧٠
[232] Cass.Crim.30 Oct. 1936, D.C. 1936.590
[233] J.LARGUIER, Ph. CONTE, op.cit., p.122, nº.139
[234] J.PRADEL, M. DANTI-JUAN op.cit., p.632, nº.890

conséquences de son délit, l'escroquerie demeure définitivement constituée et est en conséquence punissable.

Une autre question qui se pose est celle de savoir si le préjudice est exclusivement de nature patrimoniale?

La jurisprudence française suivie de la jurisprudence libanaise ont respectivement admis que le délit d'escroquerie est constitué au moment où la remise a été déterminée par les moyens frauduleux indépendamment d'un préjudice patrimonial subi[235] et sans donner d'importance au fait que ce préjudice soit matériel ou moral.

Une fois que nous avons survolé dans notre premier chapitre l'intention frauduleuse, la remise provoquée, le lien de causalité et le préjudice subi sous tous leurs aspects nous exposerons sous un second chapitre la répression des moyens d'escroquerie dits classiques tant bien en droit français qu'en droit libanais (Chapitre 2).

Chapitre 2 : La répression de l'escroquerie dite classique

La particularité du délit d'escroquerie réside dans le fait que sa tentative est punissable et qu'il existe certaines immunités familiales à prendre en considération au moment de la répression (Section 1).

Les sanctions classiques tant simples qu'aggravées du délit d'escroquerie en tant qu'infraction contre les biens feront l'objet de notre seconde section où nous évoquerons également le point de départ de la prescription applicable à ce genre de délit (Section 2).

Section 1: Particularités de la poursuite

La simple tentative est punissable dans le cas d'infraction d'escroquerie, tant en droit français qu'en droit libanais sous certaines conditions bien établies

[235]M-P.LUCAS DE LEYSSAC, A. MIHMAN, op.cit., p. 63, nº. 91: «*le délit d'escroquerie a été retenu à l'encontre d'une personne qui a obtenu des colis de la croix rouge par l'usage d'une fausse qualité, sans qu'un préjudice patrimonial n'existe».*

(Paragraphe 1) avec des spécificités de poursuite quant à la compétence territoriale et aux d'immunités accordées (Paragraphe 2).

Paragraphe 1: Incrimination de la tentative d'escroquerie

La simple tentative d'escroquerie est incriminée en elle-même en droit français[236] et en droit libanais.

Cette tentative a lieu quand le délit n'est pas complètement achevé en raison de circonstances indépendantes de la volonté de son auteur. C'est le cas lorsque la victime découvre les manigances de l'escroc.

Citons à ce propos les exemples suivants: une compagnie d'assurance découvre la surévaluation des factures présentées[237], une demande d'ouverture de compte est assortie de la remise, en connaissance de cause, de chèques sans provision ou frappés d'opposition[238].

La tentative d'escroquerie est punissable en droit français selon les dispositions claires de l'article 313-3 CPF où l'on parle de tentative dans deux cas: en cas de commencement d'exécution, qui consiste à présenter une demande pour obtenir une remise avec l'emploi des moyens frauduleux et que la remise ait été empêchée par des circonstances indépendantes de la volonté de l'agent et le cas d'absence de désistement volontaire, antérieur à la consommation. Ce second cas se pose par exemple lorsqu'une personne a fait une proposition d'assurance avec un faux rapport mais qu'elle retire ultérieurement sa proposition.

---

[236]M-P.LUCAS DE LEYSSAC, A. MIHMAN, op.cit., p.61, nº.88

[237]M.VERON, op.cit., éd.2010,p.298, nº.426

[238]Cass. Ass.Plen. 18 janvier 2006, numéro 02-80-787: «*le prévenu s'est présenté à l'agence de la banque pour se faire ouvrir un compte en remettant quatre chèques émis par des particuliers en règlement d'honoraires de négociations immobilières, ainsi qu'un chèque d'un montant de 300 000 francs tiré en son nom. La banque a découvert que les quatre premiers chèques étaient frappés d'opposition et le dernier était sans provision. L'escroc a été condamné pour tentative d'escroquerie. La cour d'appel a insisté sur le fait que le prévenu connaissait l'opposition vu que les chèques avaient été émis par des clients en contrepartie d'engagements qui à la base n'entendaient pas honorer mais la cour de cassation a cassé l'arrêt de la cour d'appel et trancher dans le sens de l'existence d'une tentative d'escroquerie*».

A l'instar du droit français l'article 655 CPL incrimine à son tour la tentative d'escroquerie. Selon les dispositions de ce texte, La tentative existe si plusieurs cas se présentent : si la remise a été empêchée par des circonstances étrangères et extérieures à la volonté de l'agent , si les manœuvres frauduleuses ont été découvertes avant leur achèvement[239], si les manœuvres ont été accomplies mais que la victime n'est pas tombée dans l'erreur, ou si les manœuvres ont été accomplis mais sans aucune influence sur la victime qui a remis son bien de son propre gré[240].

Dans tous les cas de figures citées, qui s'appliquent indifféremment dans les deux droits français et libanais, la tentative suppose nécessairement un commencement d'exécution.

On en déduit que les moyens frauduleux non utilisés par l'agent, ne seront considérés que comme des actes préparatoires, tant que l'agent n'a pas essayé d'obtenir la remise d'un objet. Tel est l'exemple d'une personne qui a volontairement commis un incendie mais n'a pas demandé un remboursement de son assureur.

Reste que la tentative qui est la plus fréquemment poursuivie, est celle de la tentative d'escroquerie à l'assurance.

A ce propos et avant 1994, la Cour de cassation française jugeait qu'il n'y avait pas escroquerie lorsque l'assuré déclarait à son assureur un sinistre simulé lorsque ladite déclaration n'est accompagnée d'aucune demande formelle d'indemnisation. La Cour voyait en cela un simple acte préparatoire non punissable en tant que tel.

Mais depuis un arrêt de 1994[241] la Cour de cassation française a fait un revirement de jurisprudence en jugeant qu'il y a tentative d'escroquerie lorsque *«la déclaration de sinistre simulé par l'assuré est assortie de productions de documents* » tel qu'une attestation d'un tiers confirmant faussement la réalité du sinistre,

---

[239] فيلومين يواكيم نصر ، مرجع سابق، ص. ١٨٧

[240] تمييز جزائي، غرفة سادسة، قرار ١٩٤ في ٣٠ / ٥ / ٢٠٠١":تحقق جنحة محاولة الإحتيال لدى وضع المدعى عليهم لمشروع الاستيلاء إحتيالاً على عقار المدعية وعدم تحقق جرمهم لإكتشاف مشروعهم من قبل السلطة. فيكون المشروع غير محقق و بقي في طور المحاولة لأسباب خارجة عن إردر واضعيه"

[241] Cass.Crim.6 avril 1994, RSC 1994, p.760, RGDA 1994, p.885

Cette même Cour affirme clairement dans un autre arrêt ultérieur de la même année[242] que « *la seule déclaration d'un sinistre fictif constitue une tentative punissable dès lors que le déclarant a conscience de provoquer l'application du contrat et de déterminer la garantie de l'assureur » et ceci « indépendamment de toute demande expresse d'indemnisation* ».

Il nous parait évident que cette solution logique et constante de droit positif français soit transposable en droit libanais et que les tribunaux libanais qui seront confrontés à un tel cas trancherons dans le même sens.

Au surplus, une tentative d'escroquerie impossible est punissable c'est le cas d'un faux certificat adressé à un organisme incompétent.

La complicité, imputée à tous ceux qui ont participé en connaissance de cause à l'opération, est punissable même si l'infraction d'escroquerie principale est restée au stade de la tentative. Deux illustrations frappantes à citer: celle d'un employé de banque qui photocopie des comptes de clients afin de les remettre à des escrocs qui les utilisent pour commettre une escroquerie au préjudice de cette banque[243] ; et celle d'un tiers qui donne des instructions pour tromper un tribunal et empêcher un expert judicaire de remplir sa mission[244].

Paragraphe 2: Compétence, immunités et excuses

Pour ce qui est de la compétence elle relève en France, en application de l'article 113-2 CP, de toute juridiction dans le ressort de laquelle s'est réalisée un des éléments constitutifs de l'infraction d'escroquerie ou l'ensemble de ses éléments.

Il en est de même pour le droit libanais, la compétence est territoriale et les tribunaux libanais sont déclarés compétents dès lors qu'un des éléments constitutifs de l'escroquerie, ou tous les éléments de l'infraction sont accomplis sur le territoire libanais.

[242]Cass.Crim.1 juin 1994, Dr. pénal 1994, comm.234, Rev.sc.crim.1995.102
[243]J.PRADEL, M.DANTI-JUAN, op. cit., p.615
[244]Cass.Crim.6 sept.2000, Dr. pénal 2001, comm.30

Au cas où l'escroquerie a complètement été réalisée à l'étranger les juridictions tant françaises que libanaises peuvent être déclaré compétentes sur la base de la compétence personnelle[245] lorsque la victime ou l'auteur de l'escroquerie en question est français/libanais.

Même dans le cas de la tentative, la compétence est territoriale, au cas où l'infraction est accomplie sur le territoire français/libanais ou un de ses éléments préparatoires ou un des moyens frauduleux, les tribunaux français/libanais seront compétents pour statuer à condition que la tentative ne s'arrête pas aux actes préparatoires.

En droit libanais, l'article 675 CPL n'a pas exigé l'existence d'une plainte directe de la victime pour poursuivre un individu sur la base du délit d'escroquerie, l'action qui enclenche la poursuite peut donc être une action publique intentée par le ministère public à laquelle pourra se joindre ultérieurement la victime préjudiciée.

Il faut noter enfin qu'en cas de décès de l'escroc au cours de l'instance qui met fin à l'action publique, les tribunaux saisis, français ou libanais, restent compétents pour statuer uniquement sur les demandes civiles et les héritiers de l'escroc seront tenus de rembourser à la victime les montants qui lui sont dus[246].

Notons avant de conclure cette section qu'il existe des immunités familiales, traitées à l'article 311-12 CPF, et à l'article 674 CPL en droit libanais qui s'appliquent aussi bien en cas d'escroquerie ou de tentative d'escroquerie.

Pour en donner une définition l'immunité est une excuse absolutoire conférée à l'escroc lorsque ce dernier commet l'escroquerie contre l'un de ses parents, enfants (même adoptif) ou son partenaire (époux/ épouse) à condition qu'ils ne soient pas divorcés.
Le droit libanais s'attarde également à son article 676 CPL sur les excuses atténuantes, qui s'imposent au juge libanais à chaque fois que ce dernier se trouve confronté à l'un des deux cas suivants: si le dommage éprouvé par la victime est insignifiant ou lorsque le dommage a été supprimé avant le début du procès.

[245] فيلومين يواكيم نصر ، مرجع سابق، ص. ١٧٩
[246] Cass.Crim.8 Avril 1991, Dr. Philomène Nasr, Manuel, p.188

L'existence de l'un de ses deux cas suffit pour permettre aux tribunaux libanais d'atténuer la peine du délit commis à moitié.

En vertu du même article libanais, la peine est atténuée de trois quart dans un seul cas : si le dommage a été retiré en cours de procédure mais avant que la décision sur le fond du litige soit rendue.

Section 2 : **Les Sanctions de l'escroquerie classique**

Les sanctions encourues par l'escroc peuvent être des sanctions simples (Paragraphe 1) mais certaines d'entre elles peuvent s'aggraver à cause de plusieurs circonstances relatives tant à l'auteur de l'escroquerie, qu'à la victime (Paragraphe 2).

Paragraphe 1 : Peines des escroqueries simples et prescription:

Les peines prévues en droit français, à l'article 313-1 CPF pour les personnes physiques, sont de deux genres: d'une part des peines principales d'emprisonnement (5 ans) avec une amende qui peut atteindre 375 000 Euros.et d'autre part des peines complémentaires tel que l'interdiction d'émettre des chèques, interdiction d'exercer une fonction publique ou une activité professionnelle dans l'exercice ou à l'occasion de laquelle l'infraction a été commise, interdiction de séjour, fermeture d'établissement ayant servi à commettre les faits incriminés pour une durée maximale de 5 ans, exclusion des marchés publics pour une durée de 5 ans.

Il faut noter à ce propos que les peines complémentaires posent des problèmes. Cela se vérifie par exemple lorsque les tribunaux ordonnent comme sanction la fermeture de l'établissement où l'infraction a été commise à cause du fait qu'un seul dirigeant ou salarié ait utilisé son activité pour commettre une escroquerie, cette sanction contredit donc en quelque sorte le principe de la personnalité des peines en matière pénale. Il en est de même pour la sanction d'exclusion des marchés publics, il suffit qu'un dirigent ou un salarié soit frappé de cette sanction pour considérer que l'entreprise entière est exclue du marché public.

Les sanctions de droit libanais sont presque calquées sur celles du droit français conformément aux dispositions de l'article 655 CPL. L'escroquerie étant punissable d'une peine d'emprisonnement de 6 mois jusqu'à 3 ans et d'une amende de 100 000 livres libanaises jusqu'à 1 million de livre libanaise.

Les personnes morales peuvent, à leur tour, être déclarées pénalement responsables du délit d'escroquerie. En effet, en droit français et conformément à l'article 313-9 CPF la peine dans sa version antérieure à la loi du 14 mai 2009[247] les sanctions applicables aux personnes morales pouvaient arriver jusqu'à la dissolution de ces entités. Avec l'entrée en vigueur de la nouvelle loi de 2009, la dissolution est devenue interdite, la société ne pouvait encourir que les peines complémentaires à savoir une amende, une confiscation ou interdiction portant sur l'exercice de son activité. Mais une loi du 12 mars 2012[248] a réintroduit par la suite, à l'article 313-9 CPF, la sanction de dissolution qui est désormais applicable.

A leur tour, Les gérants et administrateurs des personnes morales peuvent être déclarés responsables, ou condamnés comme complices des actes commis par les moyens et pour le compte de leur société. C'est la même solution qui peut, sans difficulté aucune, être transposable en droit libanais pour la condamnation des entités morales libanaises et de leurs dirigeants.

Il faut noter qu'en matière pénale, tant en droit français qu'en droit libanais, la preuve de l'escroquerie peut être rapportée par tout moyen sauf au cas où un écrit est requis.

Quant à la prescription de ce délit les deux droits français et libanais adoptent la même position en considérant que le jour de la remise est le point de départ de la prescription de trois ans.

Ce point de départ ne peut être avancé jusqu'à la date des manœuvres, ou même retardé au jour de la découverte par la victime. C'est ainsi que les tribunaux français[249] et libanais[250] affirment tous deux clairement que «*La prescription en*

[247]Loi française n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures.
[248]Loi française n° 348/2012 tendant à faciliter l'organisation des manifestations sportives et culturelles.
[249]Cass.Crim.22 Nov. 1983, Bull. n°307, Rev.sc.crim.1985.309

matière d'escroquerie commence à courir du jour de la remise»[251] *« et non du jour où cet acte aurait été connu de celui qui s'en prétend victime »*[252].

Mais un problème se pose lorsque les manœuvres sont distinctes et répétées provoquant des remises successives. Cela se vérifie notamment en cas de remise déclenchant des versements périodiques.

La jurisprudence française a résolu ce problème en affirmant à maintes reprises que la prescription commence dans de tels cas dès le dernier versement[253], ou dès la dernière remise[254]: «*lorsque des manœuvres frauduleuses répétées sont exécutées et se poursuivent sur une longue période, formant entre elles un tout indivisible, et provoquant des remises successives, la prescription ne commence à courir qu'à partir de la dernière remise ou délivrance*»[255]. C'est cette même solution qu'adoptent les tribunaux libanais[256].

Dans le cas particulier d'un chèque obtenu par des manœuvres frauduleuses, la prescription cours du jour de la présentation du chèque à l'encaissement[257].La prescription diffère dans le cas d'escroquerie qui se réalise par remise d'un billet à ordre, puisqu'elle commence le jour de la remise conformément au principe.

Un autre problème qui se pose au niveau des remises effectuées par virement de compte à compte est celui du moment à prendre en considération. La jurisprudence est également intervenue et a décidé que le moment de la remise en cas de

---

[250] تمييز جزائي، غرفة ٣ ،قرار رقم ٦٥ ، تاريخ ١٦ / ٣ / ٢٠٠٥ . كساندر إلكتروني : "جرم الاحتيال الجزائي ، يبدأ من تاريخ ارتكابها ، وتعد مرتكبة بدءًا من إكتمال التعامل وحصول التعهد أو ابرام التعاقد الذي يليه على الفور تسليم المال ، ولكن يجب التفريق بين تسليم المال إلى الجاني وبين الاستيلاء عليه والتصرف به ،فالمعول عليه هو بدئ التسليم"

[251] تمييز جزائي، غرفة ٣ ، قرار رقم ٦٥ ، تاريخ ١٣ / ٣ / ٢٠٠٥ ، العدل ٢٠٠٦ ، ج ٣ ، ص ١٢٨٤:" إن رأي المحكمة إستقر على أن جرم الاحتيال الجزائي ... هو من الجرائم الأنية يبدأ من تاريخ ارتكابها ، وتعد مركبة بدءًا من إكتمال التعامل وحصول التعهد أو ابرام التعاقد الذي يليه على الفور تسليم المال ، ولكن يجب التفريق بين تسليم المال إلى الجاني وبين الاستيلاء عليه والتصرف به ، فالمعول عليه هو بدئ التسليم ... "

[252]Cass.Crim.20 Mars 1984, D.22.Nov.84.I.R.P.433 ; RSC.85. nº2.p.309 (V.Dr. Philomène Nasr, manuel, op.cit. p.181)

[253]Cass.Crim.20 juin 1994, Dr. pénal 1994, comm.260 ; Crim.18 juil. 1968, Bull. nº234

[254]Cass.Crim.1 fév. 1993, Dr. Pénal 1993, comm.158

[255]Cass.Crim.17 Déc. 1974. Bull. crim. nº371

[٢٥٦] تمييز جزائي، غرفة سادسة،رقم ٧١ في ٢١ / ٢ / ٢٠١٧ ، كساندر الالكتروني: *"الاحتيال (...) جريمة مركبة تتطلب مجموعة من التصرفات والاجراءات التي تندرج في اطار حمل المجنى عليه على تسليم ماله الى الفاعل تحت تأثير الغلط الذي ولدته في ذهنه المناورات الاحتيالية، متى استمر هذا التسليم لفترة من الوقت وكان على دفعات، بحيث تكتمل عناصر الجريمة عند اخر فعل تسليم"* .

[257]M-P.LUCAS DE LEYSSAC, A. MIHMAN, op.cit., p.72, nº.103

virement à un compte courant est celui de l'arrêté de clôture du compte: *«dans le cadre d'une remise effectuée par virement* à *un compte courant, ce n'est qu'au jour de l'arrêté, de clôture du compte que la remise est effectuée et commence à courir la prescription*»[258].

Pour ce qui est de la tentative d'escroquerie en cas de remise sollicitée mais non obtenue, la prescription cours du jour des dernières manœuvres frauduleuses utilisées.

Enfin, en cas d'escroquerie au jugement la prescription commence en droit français le jour où la décision ou sentence arbitrale obtenue est devenue définitive, les procédures d'exécution de la décision n'interrompent pas ce délai de prescription.

Après avoir passé en revue les peines des escroqueries classiques nous nous intéresserons sous un paragraphe 2 aux peines aggravées (Paragraphe 2).

Paragraphe 2: Peines des escroqueries aggravées:

Les sanctions prévues initialement pour les escroqueries dites simples peuvent être aggravées au vu de l'existence de circonstances aggravantes rendant le délit en question encore plus dangereux.

Les peines sont portées en droit français, en application de l'article 313-2 CPF, jusqu'à 7 ans d'emprisonnement et 750000 euros d'amende pour les personnes physiques pour les cas précis énumérés à cet article et que nous passerons en revu ci-dessous.

Le droit libanais[259], prévoit pour les cas d'escroquerie extrêmes s'apparentant à ceux du droit français des peines allant entre 1 et 6 ans d'emprisonnement et une amende entre 200 000 livres libanaises et 2 millions de livres libanaises.

Les circonstances aggravantes rendant le délit d'escroquerie passibles de peines aggravées peuvent tenir ou bien à l'auteur de l'escroquerie ou bien à la victime.

[258]Cass.Crim.4juin 1935, D.1936.1.55
[259]Art. 656 CPL

Le droit français énumère à l'article 313-2 CPF quatre cas aggravés d'escroquerie tenant à la qualité de leur auteur : 1-le cas d'une personne dépositaire de l'autorité publique ou chargée d'une mission de service public ayant agi dans l'exercice de ses fonctions. 2-le cas de personne ayant fait appel au public en vue d'émission de titres (ex : publication de faux bilan) ou en vue de collecte de fonds à des fins d'entraide humanitaire ou sociale. 3- le cas d'escroquerie commise par une bande organisée[260] dont la peine a été modifié à la hausse par une loi française de 2004[261], 4- le cas où le délit est commis par une personne prenant indument la qualité d'une personne dépositaire de l'autorité publique ou chargée d'une mission de service public (faux policiers).

Quant au droit libanais les circonstances aggravées de l'article 656 CPL diffèrent quelque peu de ceux du droit français mais sont conçus dans le même sens: lorsqu'une personne fait appel au public en vue d'émission d'actions, obligations ou de titres quelconques soit d'une société soit d'une entreprise[262], le prétexte d'obtenir un emploi ou une position dans un ministère public, un acte frauduleux accompli par une personne titulaire d'une signature qui lui est confiée par une société ou une association ou institution ou toute autre personne morale.

Au surplus, les circonstances aggravantes peuvent également dépendre de l'état de la victime de l'escroquerie: victimes vulnérables vu leur âge, leur maladie, leur déficience physique, l'état de grossesse et dont l'état est apparent ou connu de l'agent.

Mais avec l'entrée en vigueur de la loi française du 12 juin 2001, ce genre de circonstances aggravantes liées à l'état de la victime tombent désormais sous le coup d'une infraction indépendante celle *«d'abus de la vulnérabilité d'un*

[260]Cass.Crim.16 octobre 2013, D. 2013 p.2399: en l'espèce l'association spirituelle église de scientologie et la société SEL ont été jugées coupables d'escroquerie en bande organisée au préjudice de trois femmes à qui elles avaient proposé un «test de personnalité» sans aucune valeur scientifique.
Il en est ainsi également pour le cas des réseaux constitués pour la fabrication de meubles anciens, ou différents objets volés (V. Pradel Jean et Danti juan Michel, droit pénal spécial, droit commun, droit des affaires, Paris, op.cit, p.614, n°869).

[261]Sachant que dans ce cas précis la peine a été encore plus aggravée atteignant 10 ans d'emprisonnement et 1 million d'euros en application par la loi n 204/2004 du 10 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.

[262]Art. 86 CCL:كل عمل إحتيالي يراد به حمل الناس على الاكتتاب أو دفع المال ، يعاقب عليه بعقوبات الاحتيال

personne» prévue à l'article 223-15-2 CPF. Cet article punit le fait d'abuser de la faiblesse d'une personne pour obtenir d'elle la remise de la chose convoitée.

Cette infraction indépendante d'abus de vulnérabilité n'existe pas, à notre connaissance, en droit libanais qui se suffit de prendre en considération l'état de la victime in concerto pour attribuer la peine adéquate au cas par cas.

Nous noterons toutefois que c'est la même prescription évoquée au paragraphe précédent qui s'applique aux cas d'escroquerie aggravés.

Une fois que nous avons passé minutieusement en revue tous les moyens d'escroquerie dits classiques, que nous les avons défini, illustrer d'exemples, que nous en avons déterminé le champ d'application et préciser les particularités de leur poursuite et les sanctions qui s'y attachent, nous allons dans notre seconde partie voir comment les lois pénales françaises et d'autant plus libanaises sont mises à rude épreuve avec la montée en pic et l'apparition des moyens innovateurs d'escroquerie. Nous nous demanderons également quelles solutions ses deux droits offrent-ils afin de les prévenir, de les combattre sinon d'en diminuer leur nombre et comment, face à ce nouveau genre de délinquance, les Etats ont été plus ou moins obligés d'adapter leurs lois nationales et de ratifier des conventions et accords internationaux (Partie 2).

L'escroquerie est une infraction qui envahit non pas seulement le monde matériel, mais aussi le monde virtuel qui occupe désormais la plus grande partie de nos vies. Du fait que ce mode est en voie de développement continue, on ne peut que remarquer que les infractions commises avec des techniques de plus en plus avancées « cyber-escroqueries »se multiplient sans qu'il ne soit possible de les classifier. Notre seconde partie traitera donc de ces nouvelles escroqueries, de leurs variantes ainsi que des modes de leurs répressions au niveau libanais, au niveau français et même au niveau mondial.

Partie 2: Les lois pénales à l'épreuve des moyens innovateurs d'escroquerie:

De nouvelles formes d'escroquerie sont apparues et se réalisent non pas au niveau de notre monde matériel, mais plutôt au niveau du monde virtuel. Le monde virtuel en question englobe, selon la définition donnée par M-F. Lebert[263], l'ensemble des réseaux commerciaux, publics, privés, d'enregistrement, de services envahis par la nouvelle notion de "cybercriminalité".

La particularité du monde virtuel apparait par la décentralisation de communication, la protection de l'anonymat, la rapidité des informations retenues et enfin l'utilisation fréquente d'identités fictives.

La cybercriminalité regroupe comme nous le verrons les infractions pénales susceptibles de se commettre sur les réseaux de télécommunications et par le biais de l'Internet[264].

Face à cette délinquance, les Etats des différents pays ont été plus ou moins obligés d'adopter des nouvelles lois ou du moins de modifier leurs lois nationales.

Nous passerons en revue dans un premier titre les moyens frauduleux les plus innovateurs qui ont récemment vu le jour (Titre 1) pour nous attarder dans le second titre aux moyens de répression prévus par les différentes législations pour tenter d'incriminer les escroqueries les plus futées (Titre 2).

[263] M. HABHAB, «*le droit pénal libanais à l'épreuve de la cybercriminalité*», SADER, Beyrouth, 2011, p.17

[264] ع. السراج . شرح قانون العقوبات الاقتصادي في التشريع السوري والمقارن ، جامعة دمشق ، ٢٠١٠ - ٢٠١١، ص. ٢٨٣

Titre 1: L'exposé des moyens frauduleux innovateurs:

Les nouvelles technologies de l'information et de la communication ont bouleversé le monde, on trouve de plus en plus de nouveaux modes de communications et d'échanges comme le commerce électronique, qui ne cessent de se développer[265].

Les dernières technologies de l'information et de la communication offrent en effet de multiples possibilités aux utilisateurs, ce qui facilite leur quotidien, ces multiples possibilités ouvrent cependant la voie à la commission de nouveaux moyens d'escroquerie et d'activités criminelles, connus de nos jours, sous différentes appellations qui vont dans le même sens : «*cyber escroquerie*», le « *délit informatique* », les «*cyber-crimes*».

On pourra même arriver à dire, que le nombre des cybercriminalités dépasse le chiffre des délits effectués à la main sans l'utilisation d'ordinateur.

Pour donner une définition première de cette cybercriminalité en vogue nous dirons que c'est l'ensemble des délits illicites commis par l'utilisation des technologies informatiques ou ceux commis contre un système informatique[266].

Par le recours à ces agissements, les internautes recherchent la plupart de temps des informations personnelles sur les internautes: mots de passe, données bancaires, adresses…afin d'en tirer des profits qui sont le plus souvent monétaires.

La cybercriminalité est en fait divisée en deux grandes catégories : la première catégorie regroupe toutes les infractions liées aux technologies de l'information et de la communication, on cite notamment les infractions d'atteintes aux systèmes de traitement automatisée de données, les infractions portant atteinte à la protection des données personnelles. La seconde catégorie regroupe les infractions dont la commission a été facilitée par l'utilisation de ces technologies, en d'autres termes ce sont les infractions qui nécessitent pour leur commission le recours à un

[265]Le chiffre d'affaire du commerce sur Internet, a globalement atteint les dernières cinq années plus de 8,68 milliards. De même le pourcentage d'utilisation de l'internet par les internautes afin de gérer leurs transactions bancaires ne cesse de s'élever (V. M.HABHAB, op.cit., p.23).
[266] M.HABHAB, op.cit., p.21

ordinateur, on cite: les escroqueries par utilisation frauduleuse de carte bancaire, ainsi que les contrefaçons, les loteries frauduleuses…

Partant de là, la *«cyber-escroquerie»* désigne l'activité criminelle ou délictuelle effectuée dans le cyber espace. L'OCDE[267]donne une définition intéressante à relever de ce délit informatique: «*tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne un traitement automatique de données et/ ou une transmission de données*»[268].

Quelques pays, dont notamment le droit français, se sont abstenus de donner une définition globale de l'infraction informatique et se suffisent d'énumérer et de classifier les différentes infractions qui en découlent selon les buts poursuivis par l'escroc. Par contre les Etats-Unis définissent ces délits au niveau fédéral ainsi qu'au niveau de chaque Etat, on cite les *«computer crimes*» au niveau de l'Etat de Texas, définissant le délit informatique[269].

Le droit libanais est quant à lui totalement silencieux sur la définition des infractions informatiques, il n'en donne ni énumération précise ni classification claire. L'état actuel de la législation libanaise est loin de pouvoir s'adapter à la survenance de ce genre de délits hors du commun comme nous le verrons et il a besoin d'être reformé dans son intégralité pour les englober dans l'état actuel de sa législation

Aujourd'hui, les escrocs peuvent commettre leurs cybers-escroqueries depuis n'importe quel pays où ils se trouvent et de façon presque instantanée. C'est ainsi que ces derniers modifient des sites web, intègrent un réseau informatique, copient des informations confidentielles, opèrent des virements bancaires… à longue distance.

Nous allons passer en revue les moyens les plus innovateurs auxquels les escrocs ont récemment recours en étudiant d'une part les cyber-escroqueries visant les

[267]Organisation de Coopération et de Développement Economique

[268]N. El CHAER, «*la criminalité informatique devant la justice pénale*», Sader, 2004, Beyrouth, p. 18

[269] م. عبد الرؤوف ألحن، جريمة الإحتيال عبر الانترنت، الأحكام الموضوعية و الأحكام الاجرائية، منشورات الحلبي، بيروت، ٢٠١١ ، ص.١٠٤

personnes physiques (Chapitre 1) et d'autre part les cyber-escroqueries visant les entreprises et banques (Chapitre 2).

Chapitre 1: Les cyber-escroqueries visant les personnes physiques

Le réseau d'internet, qui est en voie de développement au cours des dernières années, mène à un développement de la délinquance et à la multiplication des victimes croyant faire de bonnes affaires sur les réseaux de communications.

La France est un pays où l'activité cybercriminelle est très excessive, notamment depuis 2001. Il devrait être de même pour le Liban même si la plupart de ses infractions ne sont pas rapportées aux services concernés pour que ces derniers ouvrent une enquête les concernant.

L'hameçonnage, l'escroquerie à la nigériane (Section 1) et les arnaques sur internet (Section 2) que nous allons voir tout de suite sont les techniques vedettes qui s'effectuent de plus en plus à travers les nouvelles technologies liées à la montée en puissance de l'informatique.

Section 1: L'hameçonnage et les courriers électroniques frauduleux :

Les nouvelles technologies de l'information et de la communication provoquent des bouleversements majeurs, et laissent naitre une nouvelle menace: la cybercriminalité, notion polymorphe née de l'essence de ces nouvelles technologies[270].

L'hameçonnage (Paragraphe 1) et les courriers électroniques frauduleux (Paragraphe 2) qui ont lieu par l'usage des nouvelles technologies constituent les deux genres de cybercriminalité les plus connues comme nous le verrons tout de suite.

[270]D. SERRES, A. CLUZEAU, Maitrise en droit de l'entreprise, Uuniversité Laval-, mémoire, 2008

Paragraphe 1 : L'hameçonnage ou «phishing»:

L'hameçonnage, connu en anglais sous le nom de «phishing», est un procédé de vol d'identité par courriel[271] à l'aide de l'internet.

Les escrocs «hackers» recourent à ce procédé afin d'obtenir des renseignements personnels sur leur victime. C'est ainsi que les hackers envoient de faux courriels- qui apparaissent comme authentiques- et utilisent l'identité d'institutions financières ou de sites commerciaux connus dans lesquels ils demandent aux destinataires de mettre leurs coordonnées bancaires ou personnelles. Les utilisateurs cliquent sur un lien leur menant sur un faux site, qui est une copie conforme du site de l'institution ou de l'entreprise, et fournissent leurs informations personnelles qui seront retenues par les pirates pour détourner des fonds à leurs avantages[272].

La pratique du «phishing» consiste en d'autres termes à *«collecter des informations en créant un site miroir ayant l'apparence d'un site officiel, afin de réaliser une collecte des données personnelle»*[273].

Cette technique ne vise pas directement les institutions ni les entreprises, mais leurs clients personnes physiques qui seront eux même les victimes potentielles d'escroquerie. Le client subira le vol de ses renseignements personnels et perdra sa confiance envers l'entreprise et peut même aller jusqu'à engager la responsabilité de cette dernière pour le préjudice subi[274].

Une variante de l'hameçonnage classique réside dans «les propositions de travail non sérieuses». Ce sont des offres de travail portant sur des activités illégales notamment de blanchiment d'argent qui sont émises sur les sites internet. Le processus est le suivant: les victimes reçoivent un e-mail contenant une proposition de travail en contrepartie de laquelle on leur offre un profit de grande envergure. Les manœuvres frauduleuses consistent, une fois que la victime accepte le travail fictif proposé, de la convaincre d'effectuer un transfert de fond .

[271]D. SERRES, A. CLUZEAU, op.cit.
[272] م. عبد الرؤوف ألحن، مرجع سابق ، ص٦٤
[273]M.HABHAB, op.cit, p.81
[274]Les frères «Stevens», de Houston, ont commis une escroquerie de phishing, en créant un faux site de l'armée de sauvegarde (Salvation Army), et ont pu obtenir une somme de 48 000 dollars, sous le nom de société d'entraide suite à l'ouragan Katarina (V. Mohammad alhenn, p.65).

Une deuxième variante de l'hameçonnage se vérifie lorsqu' une victime reçoit des messages lui indiquant que son compte a été désactivé et que sa réactivation ne sera possible qu'une fois ses renseignements personnels fournis. En réalité ce message électronique fournit un hyperlien qui dirigera l'utilisateur vers une autre page web qui ressemble au vrai site, et la victime étant inconsciente que cette page est falsifiée, fournira ses informations personnelles qui seront enregistrées par l'escroc[275].

Une troisième variante de l'hameçonnage qui prend de plus d'ampleur est celle du «net phishing». Les attaques du net phising se font ou bien par le biais de manipulations sociales[276] ou bien par des manouvres technologiques (technical subterfuge), ayant tous les deux pour but la soustraction des informations personnelles et financières des victimes.

Les tribunaux français, recourent à une ancienne loi de 1978[277], afin d'incriminer les attaques d'hameçonnage, considérées comme des attaques aux données stockées. Cette loi a pour but *«de reconnaitre des droits nouveaux au profit des citoyens à l'égard des grands systèmes centralisés d'informations dont les divers secteurs privés et publics commençaient à se doter»*[278]. L'article 39 de ladite loi donne aux personnes un droit de s'informer sur les données enregistrées, leurs origines et leurs destinataires[279]. Les victimes françaises disposent d'un site pour signaler tout hameçonnage, c'est le site www.internet-signalement.gouv.fr.

Au niveau des Etats-Unis, où la FTC[280] reçoit les plaintes ayant pour objet le phishing[281], on trouve les lois «Anti-Phishing Act»[282], «Federal Trade Commission

---

[275] م . الغول، جرائم شبكة الانترنت والمسؤولية الجزائية الناشئة عنها ، دراسة مقارنة، مكتبة بدران الحقوقية، ٢٠١٧ ، ص . ١٧٠

[276]Les méthodes de «social engineering» se font à l'aide de courriers trompeurs envoyés pour diriger les consommateurs vers de faux sites sur internet qui poussent les internautes à donner leurs informations financières: numéro de carte de crédit, mots de passe, numéros de sécurité sociale…

[277]Loi française n° 78-17, du 6 janvier 1978 relative « *à l'informatique, aux fichiers et aux libertés* »

[278]M. HABHAB, op.cit, p.81

[279]Idem

[280]Federal trade comission, a signalé en septembre 2003, que 9 millions résidents aux Etats-Unis, sont tombés victimes du «phishing», (V. J.A.HITCHCOCK, Net crimes and Misdemeanors, outmaneuvering Web spammers, stalkers, and Con artists, Medford, New jersey p.137)

Act» et le « Gramm-Leach-Bliley Act[283]» dont les peines ont été renforcées par la loi «Identity Theft Penalty Enhancement Act»[284]. L'Etat du Texas dispose d'une loi spéciale[285] de lutte contre le *phishing*: la «House Bill 1098», intégrée au «Texas Business and Commerce Code»[286] qui prévoit des peines allant jusqu'à de 2 ans d'emprisonnement et 100,000 dollars d'amende.

La Grande Bretagne dispose elle aussi d'une loi spécifique réprimant l'usurpation de l'identité numérique, la «Fraud Act»[287] de juin 2006[288].

Les tribunaux libanais n'ont pas par contre une loi spécifique ayant pour but de protéger les données personnelles et sur la base de laquelle les attaques d'hameçonnage peuvent être incriminées. Certains auteurs libanais préconisent d'appliquer l'article 571 du CPL[289] qui protège la vie privée. Mais selon l'avis de la majorité de la doctrine cet article ne fait référence à aucun moyen de communication, d'où il ne peut pas être appliqué pour réprimer les atteintes aux données personnelles réalisées par le biais d'Internet[290].

Selon le bureau de lutte contre la cybercriminalité au Liban si l'on s'attarde sur la situation actuelle libanaise on ne trouve pas un nombre très élevé de cas

---

[281]La FTC a condamné en 2004 pour phising, sur la base des deux lois: Federal Trade Commission Act et le Gramm-Leach-Bliley Act, un escroc qui a Houston crée des faux sites imitant ceux de «American Online» «PayPal» en incorporant les logos de ces deux institutions afin d'extirper les données personnelles des victimes. (V. Justin Vaughan, Texas's new e-consumer protection acts: A (PH)ARWELL to phishing and spyware, Texas Wesleyan law review, 2006, p.6)

[282]« A bill to criminalize Internet scams involving fraudulently obtaining personal information, commonly known as phishing» de 2005 (V. J. Vaughan, op. cit., p.5)

[283] Connu aussi sous le nom « *Financial Services Modenization Act of 1999* », le 12 novembre 1999

[284]Loi numéro 108-275, du 7 juillet 2004

[285]Loi du 1 septembre 2005

[286]J. VAUGHAN, Texas's new e-consumer protection acts: A (PH)ARWELL to phishing and spyware, Texas Wesleyan law review, 2006, page3

[287]A son article 2, la loi incrimine le «phishing»

[288] م . عبد الرؤوف ألحن، مرجع سابق، ص. ١٠٧

[289] «*Tout individu qui se sera introduit dans le domicile ou l'habitation d'autrui, ou dans les dépendances de son domicile ou de son habitation, contrairement à sa volonté… contrairement à la volonté de celui qui a le droit de l'en exclure encourra la peine d'emprisonnement …* »

[290] M.HABHAB, op.cit.p.85

«phishing»[291]. Cela n'empêche pas pour autant le législateur libanais de suivre l'exemple français en prévoyant une loi spéciale incriminant l'hameçonnage et des sites de signalement de ce délit.

Outre l'hameçonnage classique plusieurs nouvelles méthodes connus désormais sous l'appellation de «*courriers électroniques frauduleux*» ont vu le jour.

Paragraphe 2: Courriers électroniques frauduleux

Les courriers électroniques frauduleux ont récemment envahit les réseaux sociaux.

Un premier genre de courrier électronique frauduleux est celui de *«l'escroquerie au mariage ou à la relation»*. Les escrocs commencent par la Romance scam, méthode utilisée pour prendre contact avec une personne vivant seule en lui envoyant des emails ou en communiquant à travers des sites pour célibataires. Les escrocs peuvent aussi bien promettre le mariage ou bien simplement entretenir une relation pour gagner le cœur de la victime. Peu de temps après, l'escroc déclare sa flamme envers sa victime et lui fait part de ses problèmes financiers[292] pour obtenir des sommes d'argents[293]. Un de ces exemples d'arnaque est celui du «Bezness», réputé pour les destinations de vacances orientales telles que la Turquie ou l'Egypte ou Tunisie… Les femmes célibataires tombent pendant leur voyage sous le charme d'escrocs qui commencent à inventer des histoires émouvantes pour susciter la pitié chez leurs victimes afin d'escroquer leur argent.

Un exemple célèbre est celui de «Robert Mc Coy», qui se présentait à ses victimes, par des publicités publiées sur différent sites électroniques, comme une femme russe en recherche de l'amour, et publiait des photos appartenant à une belle femme. Une fois que les victimes tombaient sous son charme, l'escroc leur demande d'envoyer une somme d'argent pour acheter un ticket d'avion afin de les rencontrer. Dès que l'escroc reçoit l'argent, il explique à ses victimes piégées qu'il a subi un accident et réitère sa demande de somme d'argent, plus tard il cesse de

[291]Suite à une interview que nous avons effectuée avec Commandant el Hage, qui était toujours à la tête du bureau de lutte contre la cybercriminalité au Liban, le 10 décembre 2016.
[292]Tel que le besoin de payer le téléphone ou l'accès à internet ou même le besoin de médicaments, le prix d'un billet d'avion…
[293] م. عبد الرؤوف ألحن، مرجع سابق ، ص ٦٧

répondre et disparait. Cet escroc a avoué d'avoir trompé 250 hommes, et retiré plus d'un million de dollars[294].

Le deuxième moyen innovateur d'arnaque sur internet est celui des faux comptes «PayPal». Les clients escrocs se présentent pour acheter des objets sur internet et prétendent qu'ils préfèrent payer la transaction au moyen du site PayPal, la vendeuse accepte et ouvre un compte sur ce site Paypal, le client prétend alors être à l'étranger et convainc sa victime que pour finaliser le paiement via PayPal elle avait besoin d'utiliser 5 cartes PCS, il demandera à la vendeuse de les acheter lui promettant de rembourser tout le montant lors de la réception des marchandises[295].

On rapproche les arnaques PayPal au «phising» puisque le contact entre l'escroc et sa victime se fait via internet, la victime reçoit la plupart de temps un faux mail où il lui est demandé de fournir le numéro de suivi du colis(afin de débloquer les fonds), et puis cela sera suivi par un autre courrier dans lequel l'acheteur prétend être à l'étranger, et demandera à son vendeur que le compte PayPal soit activé au niveau international. En réalité une vraie adresse PayPal permet le paiement dans toutes les monnaies du monde contrairement aux croyances des victimes escroquées.

Il en va de même pour les cas d'achats en ligne qui ne sont pas beaucoup plus sûrs. En effet, *«L'e-commerce»* s'est, de plus en plus développé au cours des dernières années ce qui multiplie les escroqueries faites lors des achats en ligne ou même dans le cadre de vente aux enchères. Les escrocs font croire aux victimes que les agents vendeurs sont situés à l'étranger et propose ainsi un service de paiement connu pour inspirer confiance tel que Western Union pour le virement du prix des objets vendus[296]. Il s'avère en fin de compte que le produit acheté n'arrive pas à destination, que ce soit un produit imité ou que la vente aux enchères ne soit rien de plus qu'une arnaque bien menée par son auteur pour escroquer les acheteurs.

Ce genre d'escroquerie est le plus répandu, selon les statistiques de la commission fédéral du commerce[297].

---

[294] www.russian-detective.com/scams

[295] J.A. Hitchcock, « *Net Crimes and Misdemeanors, outmaneuvering web spammers, stalkers and con artists*», second edition, Medford, New Jersey, p.94

[296] م. عبد الرؤوف ألحن، مرجع سابق ، ص ٥٠

[297] Idem.

Une célèbre vente aux enchères frauduleuse a eu lieu aux États-Unis. Il s'agissait de la vente sur le site «e-Bay» d'une affiche «authentique» du film Indiana Jones avec la signature de Harisson Ford et Sean Connery. La victime de cette escroquerie a acheté l'affiche non authentique, vendu à plusieurs personnes, en envoyant un chèque, sans jamais la recevoir[298] [299].

On citera également d'autres exemples notoires: Un escroc Daniel Katelsen a été condamné en Colorado le 10 Mai 2001 pour avoir commis une cyber-escroquerie, Il avait eu recours à un faux nom pour publier sur le site « eBay » des pièces d'ordinateurs à vendre, nombreux clients les ont achetés mais n'ont jamais reçu ces pièces[300]. Un autre escroc en Géorgie, avait mis à vendre sur le site «eBay» des roues de voitures, et ses clients environ 215 personnes qui lui ont transféré, dans un intervalle de 3 ans, 539,000 dollars, n'ont rien obtenu en contrepartie[301].

Nous évoquons aussi le cas de jeunes escrocs qui ont envoyé, depuis la Californie, 50 millions de courriers de publicité aux étudiants et personnes âgées, proposant d'accomplir des travaux dans les maisons en contrepartie d'une somme d'argent en faisant croire que ces courriers étaient envoyés par le site «www.Bigbear.net». Les récepteurs, tombés victimes de cette ruse, ont transférés des sommes à ce groupe de jeunes sans obtenir aucun service[302].

Un dernier exemple est celui d'une société appelée «*E.A.A.S Lottey Watergate, inc*», située à Johannesburg, qui envoi des courriers informant d'éventuelles victimes qu'elles ont gagné une somme de 2 millions de dollars, et qu'il faudrait pour l'obtenir donner à la société ses informations, son numéro de compte ou le numéro de sa carte de crédit[303].

Les législateurs des différents pays tendent, comme nous allons le constater dans notre second titre, à chercher un juste milieu, un équilibre entre d'une part la liberté, la célérité, la facilité qu'offrent les nouvelles technologies et d'autre part les exigences de sécurité des transactions, de protection de tout genre de données, de la vie privée mais surtout de mettre un frein aux courriers frauduleux mais également aux arnaques et manipulations frauduleuses.

---

[298] J.A.Hitchcock, op.cit., p.95

[299] Il en est de même pour le cas d'affiches du film Pretty Woman, avec la signature de Julia Roberts sur l'affiche (V. J.A.Hitchcock, op.cit.,p.95)

[300] Online fraud and crime: Are consumers safe? Hearing before the subcommittee on commerce trade and consumer protection, 2001, p. 33

[301] IC3, Internet crime report 2007, p.15

[302] م . عبد الرؤوف ألحن، مرجع سابق، ص. ١٥٩

[303] Ibid. p.67

Section 2: Arnaques par internet

L'Internet est le lieu de prédilection des escrocs. Ces derniers y promettent les choses les plus incroyables (Paragraphe 1) et y exercent les arnaques les plus imprévisibles dont «l'escroquerie à la nigériane» (Paragraphe 2). On essayera dans ce paragraphe de donner quelques exemples en ce qui concerne le vol des informations et les arnaques par internet.

Paragraphe 1: Promesses et loteries frauduleuses

Une des techniques d'escroquerie pouvant être exécuté par internet est celle dite *«la prisonnière espagnole»*. Cette technique remonte au XVIème siècle, durant ce siècle, les seigneurs recevaient un message réclamant des rançons pour libérer les princesses détenues.

Le concept aujourd'hui est beaucoup plus élaboré. Il consiste à faire croire à la victime en lui envoyant des emails, texto ou autres qu'elle obtiendra une récompense en contrepartie d'une certaine somme d'argent qu'elle a à avancer et qu'elle se fera rembourser. Ou même à faire croire aux victimes qu'une personne est en détresse, qu'elle se fait continuellement maltraitée par ses kidnappeurs, la victime aura alors tendance à apporter son aide et proposer le paiement de sommes aux prétendus «kidnappeurs» qui ne sont en réalité que des complices de l'escroc...[304] La preuve de ce genre d'escroquerie est difficile à rapporter puisque les relations entre la victime et l'escroc ne pourront pas toujours être établies.

Une autre méthode plus ou moins nouvelle est celle de «*la vente en cycle court*», qui se réalise par une manœuvre frauduleuse consistant à faire signer à la victime, à la va vite, un contrat de vente qui se révèle n'être en réalité qu'un contrat de location ou une licence d'exploitation par lequel la victime ne devient en aucun cas propriétaire du produit/objet du contrat[305].

Les loteries frauduleuses prennent elles aussi de plus en plus d'envergure. De nombreuses personnes deviennent victimes d'escroquerie dans l'emballement

[304] J.A.Hitchcock, op.cit.p.7

[305] م. عبد الرؤوف ألحن، مرجع سابق ، ص ٦٧

d'avoir gagné un lot surprise, un concours ou une loterie[306]. Le processus est simple les victimes reçoivent un appel, un courriel électronique, un message sur leur portable, dans lequel les escrocs prétendent qu'ils ont été sélectionné pour gagner et que l'offre est tout à fait légale, mais qu'il faudra payer quelques faibles frais pour réclamer le prix[307]. Ainsi, pour l'envoi des gains promis les escrocs réclament le renvoi d'un bon de commande ou de frais de dossier en rétribution des services pour récupérer son lot.

L'exemple mondial le plus notoire est *«l'escroquerie à la loterie Microsoft»* fraude qui commence par des courriers électroniques informant leurs destinataires qu'ils ont gagné la loterie Microsoft qui n'est en réalité qu'une loterie purement fictive. C'est suite à l'annonce faite par Bill Gates à propos de donation qu'il entend consentir, que les escrocs ont envoyé des e-mails intitulés «gains de la loterie Microsoft» annonçant le gain d'une somme d'argent. Les escrocs utilisent donc les marques de grandes entreprises et de personnalité connues tel que Bill Gates pour donner plus de crédibilité et d'authenticité à leurs courriels électroniques. En réalité, la loterie Microsoft n'est qu'une illusion, cette escroquerie n'a pour but que soutirer de l'argent ou des informations personnelles.

---

[306]Nous trouvons aux Etats-Unis, le cas de « Green Card Lottery Program », en 1990 ce système a été créé par le Congress Americain mais gratuitement or nombreux sites l'ont utilisé mais en imposant un tarif à payer. Les internautes, voulant à tout prix obtenir la citoyenneté américaine, tombent victimes et payent de sommes énormes (V. J.A.Hitchcock, p. 47).

[307]Voici l'exemple de ces messages envoyé généralement par une adresse «Microsoft loterie» dont le sujet est «félicitation» :

« *Fondation Internationale Bill Gates*
Direction de la promotion de l'internet et du jeu
La direction de loterie cristal Internationale BillGates
Loterie américaine pour la promotion de l'internet partout dans le monde
Réf Nombre : ------
Numéro du lot : 497 00 1527-AB66
Numéro du gain : AB 164 C
Monsieur/Madame,
Nous sommes heureux de vous informer du résultat des programmes internationaux de gagnants de loterie tenus il y a deux jours de cela a notre siège sis à New York.
Votre adresse d'E-mail attachée au billet numéro ----- avec le numéro de série ------ vous avez été donc approuvés pour percevoir la somme forfaitaire hors taxe de 100.000 Euro.
FELICITATIONS !! FELICITATIONS !! FELICITATIONS !!En raison du mélange vers le haut de quelques nombres et noms, nous demandons De garder l'information confidentielle de votre gain jusqu'à la fin de vos réclamations (…) »

On notera que les e-mails semblent cibler la victime elle-même, puisque la promesse s'adresse à elle en particulier, même si en réalité ils sont envoyés à une masse. De plus, les sommes promises par l'escroc pour séduire ses victimes sont irraisonnables puisqu'elles s'élèvent à plusieurs millions d'euro.

Parfois les victimes sont même invitées à appeler un numéro de téléphone précis surtaxé, pour recevoir une somme d'argent qui serait transférer à leurs comptes bancaires. Les victimes en appelant ce numéro ne faisait qu'augmenter leurs factures de téléphone sans rien y gagner en contrepartie[308].

Malheureusement, beaucoup de consommateurs s'exécutent aussitôt sans réfléchir et payent les frais demandés ou transmettent les informations personnelles requises. Mais aucun d'entre eux ne reçoit les gains promis, ni récupère les sommes avancées.

La position de la législation européenne est claire à l'égard de ces loteries commerciales déloyales: ces pratiques sont définitivement interdites et punissables. A cet égard, la Cour de justice de l'union européenne a rendu un arrêt clair et ferme à ce propos[309]: *«le droit de l'Union interdit les pratiques agressives qui donnent l'impression au consommateur qu'il a déjà gagné un prix, alors qu'il doit verser de l'argent ou supporter un certain coût afin d'être informé de la nature du prix ou accomplir les actes permettant d'en prendre possession».*

Soulevons également la précision rapportée par la Cour précitée selon laquelle: *«de telles pratiques sont interdites même si le cout, imposé au consommateur est négligeable (comme celui d'un timbre postal par exemple) par rapport à la valeur du prix, ou même s'il ne procure aucun bénéfices au professionnel»*

Nous soutenons cette position et aimerons la voir appliquer non seulement par les tribunaux français ou elle est facilement transposable mais également par les tribunaux libanais.

Ce genre d'escroquerie connait donc deux aspects. Tout d'abord le vol d'identité grâce aux informations personnelles extirpées a la victime, puis le fait de lui

[308] م . عبد الرؤوف ألحن، مرجع سابق، ص. ٧٢

[309]Cour de justice de l'Union européenne ,Arrêt C-428/11, du 18 octobre 2012, Communiqué de Presse n^0 133/12, Luxembourg , www.curia.europa.eu

soutirer de l'argent. La prudence, la méfiance et la vigilance sont d'autant d'armes efficaces pour lutter contre cette cybercriminalité.

Paragraphe 2: L'escroquerie à la «nigériane»

L'escroquerie à la «nigériane» est elle aussi en vogue. Ce genre d'escroquerie, connu sous le nom «*Advance Fee Scam*» aux Etats-Unis, repose sur un scenario, une mise en scène plus ou moins convaincante qui est présentée à la victime, et qui a pour conséquence le versement de sommes d'argent[310]. Elle ressemble de très près au système de loteries frauduleuses que nous venons de passer en revue. Le point de départ de cette escroquerie est la plupart de temps, un pays connaissant des troubles, ceci donnera un aspect tragique à l'histoire de l'escroc, pour mieux convaincre sa victime de la situation, on cite parmi les pays : Pays d'Afrique noire, Afrique de l'Ouest (Cote d'Ivoire, Gambie, Ghana, Guinée, Liberia, Sénégal, Togo Nigeria).

Cette escroquerie commence, comme pour les loteries frauduleuses, par un e-mail envoyé par un inconnu. La particularité de ce courriel réside dans le fait qu'il est général impersonnel ne s'adressant pas à une victime en particulier contrairement aux loteries frauduleuses.

Dans ce courrier, une somme importante, s'élevant souvent à des millions de dollars, est proposée à la victime en contrepartie d'une «aide» qu'elle devra fournir à l'escroc. L'aide en question consiste en une avance d'une somme d'argent pour couvrir certains frais (frais de douanes, frais de transfert bancaires, taxes fiscales, taxes de dévolution successorale…) afin que l'escroc puisse lui-même percevoir un héritage ou une somme d'argent qui lui est revient d'un parent défunt ou d'un tiers[311]. En réalité lorsque la victime effectue ce paiement elle s'apercevra rapidement qu'elle n'aura aucune somme en retour.

Ces e-mails qui promettent, pour la plus part d'entre eux, le partage d'un héritage futur contiennent des histoires émouvantes ou touchantes développées par l'escroc. Dans la majorité des cas de figure, les parents ou tiers à qui l'escroc fait référence ont ou bien été tués ou ont subi un accident, et ont laissé une somme ou un héritage, qui ne peut lui être remis qu'après le paiement de frais qu'il n'a pas la

[310] م. عبد الرؤوف ألحن، مرجع سابق ، ص ٦٥
[311] J.A.HITCHCOCK, op.cit., p.118

possibilité d'avancer lui-même. L'escroc promet donc à la victime susceptible de lui apporter une aide une part ou un pourcentage de la somme ou de l'héritage qu'il devrait percevoir ultérieurement[312].

On donnera quelques exemples de ce gendre d'escroquerie, le cas de Clémence Bare qui prétend être la veuve de l'ex-président de la république du Niger qui a promis à sa victime 20% de 38 millions de dollars. Le cas d'Eric Biara Marie Braman qui prétend être le fils unique d'un riche négociant de cacao d'Abidjan, promettant à sa victime 15 % de 8 millions. Enfin, le cas de Mrs. Felicia Kabila qui prétendait être l'épouse du président du Congo assassiné en 2001 et qui a promis à sa victime 25 % de 22 millions de dollars[313].

En Europe, une association des victimes d'escroqueries à la nigériane a été créée en février 2009[314] (en vertu de la loi du 1er juillet relative au contrat d'association) pour lutter contre ce genre d'escroqueries[315].

Par contre, en France, le seul moyen de réprimer ce genre d'escroquerie s'avère le recours à l'ancienne loi numéro 78-17, du 6 janvier 1878 qui a besoin d'être remise au goût du jour.

La législation libanaise est quant à elle tout à fait lacunaire. Elle n'apporte aucune protection pour les victimes d'escroquerie à la nigériane pour les mêmes raisons que nous avons invoquées plus haut en ce qui concerne l'application insuffisante des dispositions de l'article 571 CPL. D'où la nécessité d'organiser au moins des forums pour mieux informer les internautes des dangers de ce genre d'escroquerie est toujours accrue.

Il faudra bien noter tout de même que, selon le bureau de lutte contre la criminalité au Liban, le peuple libanais est familier avec cette méthode d'escroquerie et les libanais sont conscients des dangers qu'elle représente. Ainsi, malgré le fait que

---

[312] م. عبد الرؤوف ألحن، مرجع سابق ، ص ٦٦

[313]De même, pour le cas de Stan Stabelski, habite à Washington, il a versé 200,000 dollars, en espérant obtenir 2 millions de dollars, et pour un autre américain, habitant à Florida a versé une somme de 300,000 dollars (V.J.A.Hitchcock, op.cit., p.119)

[314]AVEN Europe (Association des victimes d'escroqueries à la nigériane en Europe, et d'usurpation d'identité sur Internet).

[315]21 millions d'euros sont dépensés par les victimes de ces arnaques,selon le site www.avenfrance.org.

les libanais reçoivent des milliers d'e-mails frauduleux, peu d'entre eux en tombe victime. En effet, le bureau de lutte contre la criminalité au Liban n'a traité pendant l'année 2017 en cours, selon les dires de son commandant, que cinq cas d'escroquerie à la nigériane.

Il est intéressant de relever en conclusion de ce premier chapitre relatif au cyber-crimes visant les personnes physiques que les Etats-Unis ont imposé, à ces personnes, l'obligation de déclarer l'infraction dont elles auraient été victimes à une organisation spéciale crée pour cette cause, sous peine d'une sanction[316]. Mais les cyber-escroqueries ne visent pas pour autant uniquement les personnes physiques, ces délits ciblent également, et de plus en plus, des entreprises et banques comme nous le verrons ci-dessous sous un second chapitre (Chapitre 2)

Chapitre 2: Les cyber-escroqueries visant les entreprises et banques

La cyber escroquerie ne vise pas seulement les particuliers, mais aussi les sociétés, entreprises et banques.

Ces entreprises et établissements financiers fournissent en effet des blocs d'informations, qui donnent naissance à des mafias et à des «*marchés noirs*».

Une enquête faite par le Computer Security Institute, montre qu'aux Etats-Unis les pertes issues d'escroquerie visant les entreprises ou banques ont atteint 455,8 millions de dollars en 2002 (170,8 millions pour le vol de données, 50 millions pour intrusion et détournement d'accès à Internet, et 115,7 millions de fraude)[317]. Plus récemment les pertes s'estiment de 10 milliards chaque année[318] [319].

Pour ce qui est du cas Français, les pertes s'estimaient déjà en 1996 selon les chiffres du CLUSIF[320] à 7,6 millions de francs[321]. Au Liban les chiffres ne sont pas précis mais il est sûr qu'ils sont également très élevés.

---

[316] فريد منعم جبور، حماية المستهلك عبر الانترنت، ومكافحة الجرائم الالكترونية ، دراسة مقارنة ،منشورات الحلبي الحقوقية ، طبعة ٢٠١٢ ، ص. ٢١٣

[317] N. El CHAER, op.cit, p. 22

[318] ف . جبور ، مرجع سابق ، ص ١٨٨

[319] En septembre 2003, aux Etats-Unis, la «*U.S. Federal Trade Comission*», a signalé que les institutions financières ont subi une perte de 48 millions de dollars (V. J.A.Hitchcock, op.cit., p.137)

[320] Club de la sécurité informatique français

Nous examinerons sous deux sections les genres d'escroquerie qui visent le plus les entreprises et banques à savoir d'une part les escroqueries aux informations sensibles, dépôts et titres financiers (Section 1), et d'autre part les escroqueries liées aux cartes bancaires et «fraude au président» (Section 2).

Section 1: Escroqueries aux informations sensibles, dépôts et titres financiers

Les escroqueries qui se multiplient de plus en plus et sortent de l'ordinaire sont celles relatives à l'usage frauduleux des informations sensibles d'une entreprise ou banque (Paragraphe 1), mais également celle relatives à l'usage frauduleux des dépôts et titres financiers (Paragraphe 2).

Paragraphe 1: Escroquerie par vol d'informations sensibles

La plupart des entreprises possèdent des données sensibles qui sont relatives aux innovations de l'entreprise ainsi qu'aux données personnelles des clients (numéros de téléphone, numéros de carte bancaire).

Ces données peuvent faire elle-même l'objet d'escroqueries spécifiques connues sous le nom de « vol d'information sensibles»[322].

En effet, toute entreprise dispose de deux réseaux: le réseau Internet et le réseau Intranet. Le réseau Internet est l'interface en ligne et le réseau Intranet est un réseau fermé et interne à l'entreprise[323] qui contient le plus souvent les informations sensibles qui seront accessibles à un nombre précis et restreint d'employés. Mais il existe entre ces deux réseaux, des passerelles dangereuses. Les informations sensibles recueillies dans les failles du système peuvent donc faire l'objet d'une attaque.

C'est ainsi que le vol d'informations s'effectuera par les pirates ayant, par des portes laissées ouvertes dans le réseau, un accès aux informations ou pouvant répliquer ou facilement s'infiltrer dans les autorisations d'accès et falsifier les certificats échappant ainsi aux mesures de sécurité imposées par l'entreprise[324].

---

[321]N. EL CHAER, op.cit.,p.22-23
[322]Appelé aussi « in-house offence » (V. M.ALHEN. p. 69)
[323]D. SERRES et A. CLUZEAU, op.cit.
[324] N. EL CHAER, op.cit, p.58

Ces attaques peuvent aussi bien s'opérer par des personnes étrangères à l'entreprise que par des personnes travaillant au sein de la dite entreprise. En effet, il est fréquent que les salariés d'une entreprise opèrent eux même des attaques de vol d'information sensibles stockés sur le réseau surtout lorsqu'ils ont un accès plus ou moins facile aux codes et mots de passe mise en place.

S'ils ne piratent pas eux-mêmes le système informatique de leur entreprise, les salariés auront tendance à délivrer les codes d'accès et mots de passe aux pirates informatiques en échange d'une somme d'argent. C'est le motif de vengeance qui anime le plus souvent les salariés licenciés ayant quittés l'entreprise mais possédant toujours leurs autorisations d'accès à commettre ce genre d'escroquerie[325].

On peut aussi invoquer les cas d'espionnage industriel[326], comme nouvelle technique d'escroquerie. Cette technique a lieu lorsque les pirates ont l'intention de voler des informations relatives à une innovation afin de la doubler. Ils procéderont à la vente des informations relative à cette innovation à un concurrent ou à celui qui paye le plus en lui faisant croire que cette innovation est l'innovation dans sa copie originale.

Les pirates informatiques peuvent en outre exploiter les données personnelles relatives aux clients de l'entreprise, telles que leurs adresses de courriel pour leur envoyer des spams, ou même s'infiltrer dans leurs ordinateurs et les infecter par un virus qu'il contrôle…

Mais il reste que les données bancaires sont les informations sensibles les plus convoitées dans ce genre de délit puisque les escrocs arrivent par leur biais à escroquer des sommes d'argent aux victimes. Tel est l'exemple de l'opérateur de télécommunications américain AT&T, victime du piratage d'informations sensibles relatives aux données personnelles et bancaires de ses clients (à peu près 19,000 clients)[327]. Un autre exemple notable est celui du piratage de 40 millions de numéro de cartes de crédit bancaires Visa et Mastercard en 2005 , les hackers ayant trouvé une faille dans le système «*Cardsystems*» et l'on exploiter.

[325] م. عبد الرؤوف ألحن، مرجع سابق ، ص ٦٩
[326] ف.جبور، مرجع سابق، ص. ١٩١
[327] D. SERRES et A. CLUZEAU, op.cit.

Pour ne pas éveiller les soupçons, les pirates agissent silencieusement et discrètement, ce qui rend leurs attaques difficile à repérer. De plus, on notera que ces escrocs ont tendance à attaquer les organismes privés (les entreprises commerciales) plutôt que les organismes publics.

Nous croyons que les entreprises tant françaises que libanaises doivent renforcer la protection de leurs données privées et recourir aux systèmes les plus sûrs et les plus fiables afin d'éviter tout genre d'attaque indésirable nuisible à leur réputation et les préjudiciant.

Outre le vol d'informations sensibles on note une augmentation sensible des escroqueries visant des dépôts et titres financiers de banques (Paragraphe 2).

Paragraphe 2: Escroquerie aux dépôts et titres financiers

Maintes atteintes peuvent viser les dépôts bancaires et les titres financiers.

En effet, en ce qui concerne les dépôts financiers chaque client d'une banque peut avoir accès, via internet, à son compte bancaire et opérer, à distance, les transactions bancaires qu'il souhaite effectuer.

Mais cette facilité offerte aux clients bénéficie par la même la tâche aux «hackers», qui assez agile pour avoir accès aux sites internet des banques accèdent aux comptes des clients, et opèrent des transferts en leur faveur à leurs comptes personnels.

L'affaire célèbre à citer à ce propos est celle de la «Security Pacific National Bank»[328], qui a eu lieu aux Etats-Unis[329].

Il en va de même pour le cas de l'escroc russe, Vladimir Levin (29ans), fameux pour l'intrusion au serveur de la banque «City Bank », situé au New Jersey, aux Etats-Unis. Cet escroc a pu obtenir 12 millions de dollars en effectuant des transferts des comptes de clients à ses propres comptes tout en surveillant toutes les transactions et accords effectués par la banque[330].

---

[328] م. عبد الرؤوف ألحن ، مرجع سابق ، ص ٤٨

[329] En l'espèce, l'américain Stanley Mark, avait découvert le code de transfert des comptes des clients d'une banque, et a pu opérer un transfert de 4 millions de dollars à un compte ouvert dans une banque suisse. Cette escroquerie n'a pas été découverte jusqu'au jour où lui-même a dévoilé son secret.

[330] م. عبد الرؤوف ألحن، مرجع سابق، ص ١٥٨

Un troisième exemple à citer est celui d'un adolescent de moins de vingt ans, qui a trouvé les failles dans le système de la banque «City Bank», et à opérer un énorme transfert à son compte. Les autorités américaines ont découvert cette escroquerie suite à une plainte déposée à l'encontre de cet escroc par les autorités douanières qui a soupçonnée l'achat d'une voiture chère par un adolescent[331].

Pour ce qui est des titres financiers, nombreux investisseurs, effectuent également leurs opérations relatives à leurs titres financiers via internet : ils achètent et vendent leurs actions et obligations sur le marché financier.

Les escrocs anonymes profitent de ce moyen d'échange via internet pour tromper les éventuels investisseurs, en créant des fausses rumeurs qu'ils rependent sur le marché financier sur la «rentabilité» de certaines actions ou obligations. Le but de ces escrocs est de doubler les achats d'actions et d'obligations et d'augmenter par la même, leur prix de vente vu que ces actions appartiennent le plus souvent à l'escroc lui-même. Ainsi, lorsque les escrocs organisent la vente de ces actions ils les vendront à un prix élevé qui n'est pas le prix réel.

On cite à cet effet l'exemple d'un courtier en bourse, qui a fait croire à ses clients qu'en utilisant un programme secret du «Wall Street » il était capable de faire fortune. Il a pu obtenir grâce à cette manœuvre frauduleuse une somme de 100,000 dollars de ses clients[332].

Donnons également l'exemple d'un autre escroc qui a usurpé un site électronique appartenant à une société de courtage licenciée en bourse, en utilisant la dénomination sociale de cette dernière, les numéros de ses contacts et autres informations pertinentes, ce qui a induit plusieurs victimes trompées par ce genre de stratagème à investir dans la société fictive de l'escroc. Cette escroquerie a duré pendant 10 mois, sans que les victimes suspectent ces manœuvres[333].

A l'escroquerie se rapportant au vol d'informations sensibles et à celle relative aux dépôts et titres financiers, viennent s'ajouter les escroqueries commises par fraude aux cartes bancaires et BEC que nous exposerons sous une seconde section (Section 2).

[331] م. عبد الرؤوف ألحن ، مرجع سابق ، ص ٤٩
[332] Ibid. p.52
[333] Ibid. p.53

Section 2 : Escroqueries liées aux cartes bancaires et à la fraude au président

Il s'avère de tout ce qui précède et de ce qui va suivre sous cette seconde section que les délits les plus dangereux sont commis par des spécialistes, connus sous le nom de «hackers», «crackers», «phreakers» ou «carders»[334], poussés par des motivations et des buts très différents. Ces buts comprennent entre autres: le fait de relever un défi technique pour prouver les failles de certains systèmes, l'envie d'un gain, la vengeance ou une simple célébrité, ou même l'obtention d'une reconnaissance…

Deux genres d'escroquerie qui requièrent sans aucun doute que leur auteur soit un spécialiste dotée d'une intelligence supérieure sont les escroqueries commises au moyen de cartes bancaires (Paragraphe 1) et celles connues sous le nom de «fraude au président» (Paragraphe 2) que nous exposerons tout de suite.

Paragraphe 1: Escroquerie par cartes bancaires

Les cartes bancaires de crédit ou de débit, peuvent être utilisées pour la commission de plusieurs escroqueries[335], puisque de nos jours, elles remplacent l'argent liquide. Ces cartes contiennent en effet toutes les informations personnelles de leur détenteur ainsi que les coordonnées bancaires de son compte.

Les escrocs créent de plus en plus de faux sites sur le réseau Internet, similaires aux vrais sites appartenant à des vraies sociétés commerciales. Sur ces faux sites, les escrocs reçoivent les transactions commerciales ou financières passées par leurs victimes et s'approprient les données des cartes de crédit des clients pour les utiliser par la suite à l'insu de ces derniers.

L'exemple type de ce genre d'escroquerie est la création d'un site similaire voir identique à celui d'une banque renommée à travers lequel les escrocs envoient des courriers aux clients, leur demandant de fournir leurs coordonnées bancaires afin de procéder à une transaction ou afin de sécuriser le changement de leur mot de passe électronique. Vu que les banques inspirent confiance aux clients, ces derniers

[334]Le hacker prend connaissance du système et se l'approprie, le cracker exercera une influence sur les données ayant pour but de porter atteinte au processus de communication ou bien porter atteinte directement au système. Le phreaker vise à obtenir des informations et enfin «le carder» s'approprie les informations bancaires pour obtenir l'argent des victimes(V. N. ELCHAER, op.cit., p. 26).

[335] ع. السراج، مرجع سابق، ص ٢٩٥ - ٢٩٦

ne suspectent pas généralement de telles escroqueries et envoient instantanément à l'escroc leurs informations bancaires[336].

De même, le délit d'escroquerie peut avoir lieu à l'occasion de la substitution de la carte bancaire du client au distributeur automatique.

Cette sorte d'escroquerie nécessite pour son accomplissement la modification préalable par l'escroc du distributeur automatique (ATM) par le recours à la technique dite *«technique du collet marseillais»*. L'escroc devra introduire dans la fente du distributeur une petite machine, qui retient toutes les informations de la carte introduite par le client de la banque. La victime en utilisant le distributeur, croira à un problème technique et s'en ira pour consulter ultérieurement sa banque, l'escroc lui aura ainsi en sa possession la carte magnétique. La plupart du temps, l'escroc sera caché quelque part à côté de la machine, pour pouvoir obtenir en plus de la carte le code confidentiel de la victime, de cette façon il pourra utiliser instantanément la carte qui lui a été frauduleusement remise, jusqu'à ce que la victime s'en aperçoive et appelle sa banque pour faire opposition.

Une autre technique d'escroquerie liée à la carte bancaire est celle du «Skimming».

Le skimming consiste à copier toutes les informations qui existent dans la bande magnétique qui se trouve au dos des cartes bancaires, en faisant passer ces dernières sur des machines spécialisées[337].

En copiant ces informations, l'escroc obtient le PAN qui est le numéro de reconnaissance du titulaire de la carte, la date d'expiration de celle-ci ainsi que toutes les autres informations qu'il juge pertinente pour pouvoir l'utiliser dans toutes sortes d'opérations faites sur Internet.

Le mot «skimming», vient de «skimmer», qui est une machine que la banque installe sur les machines de distribution automatique de billets. Le client de la banque fait généralement passer sa carte dans cette machine afin que cette dernière obtienne les informations et les enregistre. Les escrocs ont pu créer une machine similaire qu'ils utilisent sans que la victime ne prenne conscience, pour obtenir les informations et coordonnées bancaires des cartes magnétiques.

Ce genre d'escroquerie, a lieu fréquemment aux restaurants, lorsque le client paye par carte le montant de la facture. Le serveur ou même le propriétaire du restaurant peuvent à cette occasion faire passer la carte de crédit sur une machine de «skimmer», sans que le client ne sache.

---

[336] م. عبد الرؤوف ألحن، مرجع سابق، ص ٨٢

[337] Ibid.p.84

En 2005, quatre escrocs anglais, on eut recours à la méthode de «skimming» et ont pu escroquer une somme s'élevant à 200,000 pounds, après avoir obtenu les coordonnées des cartes de plusieurs victimes[338].

Au surplus des escroqueries liées aux cartes bancaires, un autre genre escroquerie en vogue ces dernières années est celui désormais connu sous le nom de «fraude au président» (Paragraphe 2).

Paragraphe 2: Escroquerie par «fraude au président»

La «fraude au président» ou «Business e-mail compromise» (BEC) est l'une des escroqueries les plus subtiles. Elle sévit depuis 2010 partout dans le monde et cause de réels dommages aux entreprises qui en sont les victimes directes.

Cette méthode consiste à convaincre un employé ou collaborateur d'une entreprise d'effectuer un virement d'argent, généralement vers un compte à l'étranger, sur ordre supposé d'un dirigeant de l'entreprise ou de l'un de ses fournisseurs, derrière lequel se cache en réalité l'escroc malveillant[339]. En définitif, ce genre d'escroquerie a pour objectif de provoquer un transfert de fonds non autorisé.

Malgré le fait que cette escroquerie frauduleuse est une arnaque qui vise toute sorte d'entreprise, de n'importe quel secteur et de toute taille[340]. Les escrocs veillent la plupart du temps à choisir, des entreprises d'envergure internationale, ou bien celles qui travaillent avec des fournisseurs étrangers, vu que ces entreprises sont très habituées à effectuer des virements bancaires à l'étranger.

Les escrocs procèdent de la manière suivante[341]: ils mènent tout d'abord une enquête visant l'identification des «employés-clés» occupant des postes importantes au sein de l'entreprise cible de l'escroquerie. Ils recherchent par exemple les employés qui s'occupent de la comptabilité de l'entreprise et qui opèrent les virements de cette dernière. Une seconde enquête est également nécessaire. Elle aura pour but de s'informer de façon minutieuse sur l'identité d'un dirigeant, d'un partenaire ou d'un fournisseur de l'entreprise afin que l'escroc adopte un comportement cohérent similaire à l'idéologie stratégique du

[338]Idem.
[339]A.GRONDIN, *«le boom inquiétant de la fraude au président»*, art. publié le 8/4/2016, les echos. Fr, www.lesechos.fr.
[340]A-S LECHEVALIER, «*Fraude au président: des milliers d'entreprises escroquées»*, art. publié le 17/12/2016, Paris Match, www.parismatch.com
[341]A. GRONDIN ,art. préc.

dirigeant/fournisseur de l'entreprise visée et suive le processus interne des demandes de virements habituellement utilisé[342]. Notons à cet égard, que les escrocs, préfèrent ordonner de petits virements successifs pour ne pas éveiller les soupçons des commissaires aux comptes. Il faudra également que l'escroc créé une fausse adresse email[343] et choisisse avec soin le moment propice de l'attaque[344] tout ceci pour inspirer plus de confiance et convaincre ses victimes.

Les manœuvres frauduleuses utilisées peuvent même aller beaucoup plus loin on parlera alors d'une variante à la classique «fraude au président» désormais connu sous l'appellation «fraude au changement de coordonnées bancaires»[345] . Lorsque l'escroc recours à cette nouvelle variante, il se présentera comme le nouveau comptable d'un fournisseur de l'entreprise ciblée ou le fournisseur lui-même et demandera à l'employé-cible de modifier les coordonnées bancaires qu'il lui avait, soit disant, précédemment communiquer. Partant de là, toutes les transactions effectuées aux nouvelles coordonnées seront récupérer par l'escroc. Pour inspirer plus de confiance, le fraudeur enverra ultérieurement à l'entreprise par courriel email une copie de la facture pour appuyer sa demande puis un faux reçu attestant réception de la somme versée.

La «*fraude au changement de coordonnées bancaires»* a vu le jour en France, en mars 2015, lorsqu'une société asiatique s'est fait passer pour le fournisseur, et a contacté une entreprise française l'informant d'un changement de domiciliation bancaire. Selon le site le parisien, l'inventeur de cette escroquerie est un franco-israélien, appelé Gilbert Chikli[346], qui a été condamné en 2015 par le tribunal correctionnel de Paris pour avoir fraudé 33 banques et sociétés entre 2005 et 2006, causant une perte d'environ 8 millions d'euros[347].

---

[342]Les escrocs visitent donc les sites officiels en ligne des entreprises et y puissent suffisamment d'informations en se renseignant sur la nature du travail de l'entreprise, les noms des dirigeants, leurs photos, quelques informations personnelles… pour usurper de la meilleure manière qu'il soit l'identité d'un dirigeant/fournisseur/avocat/commissaire aux comptes.

[343]Adresse email similaire à celle du président de l'entreprise, de son fournisseur voire même de son avocat.

[344]Il s'agira la plupart du temps, de la veille des vacances, suite à un long week-end, et de préférence en l'absence de la personne dont il usurpe l'identité.

[345]Connue également sous le nom de l'arnaque aux FOVI (faux ordres de virement International)

[346]J. CONSTANT, *«arnaques au «faux président»: l'escroc Gilbert Chikili arrêté en Ukraine»*, art publié le 19 aout 2017, Le parisien, www.leparisien.fr.

[347]L'escroc se faisait passer selon les circonstances pour le président de la société ou un agent des services secrets qui luttent contre le blanchiment ou le terrorisme. Ses victimes sont des

A en croire la police fédérale américaine (FBI), cette méthode d'escroquerie, connait un accroissement spectaculaire et a déjà causé une perte de plus de deux milliards de dollars aux entreprises américaines entre octobre 2013 et février 2016[348]. En France, les tentatives de fraude au président par usurpation d'identité ont lieu chaque jour de sorte que les entreprises françaises sont quotidiennement ciblées[349]. Le ministère d'affaire français, a expliqué qu'en cinq ans, 2300 plaintes ont été déposées[350] par des entreprises victimes de cette escroquerie. Selon les statistiques du bureau de lutte contre la cybercriminalité au Liban ce bureau traite de plus de 120 cas de «fraude au président», ce qui représente, par rapport aux autres cas d'escroqueries, un nombre élevé.

Donnons quelques illustrations frappantes de «*fraudes au président*» dont les victimes sont des entreprises de grande envergure: La société KPMG, victime de ce genre de fraude en Mai 2012[351]. A leur tour les sociétés Eurocopter, Groupe Zannier, Saint-Gobain, le groupe Coca-Cola en 2013, ainsi que la chaine d'hôtel Hilton, le groupe Virgin et Nestlé et enfin le fameux fabricant de pneumatiques Michelin[352] ont été visés.

Les moyens offerts aux entreprises afin d'échapper à ce genre de fraude réside dans la nécessité de mise en place de mesures de sécurité assez efficaces. Tout d'abord, il est indispensable de mieux informer les employés-clés des entreprises de l'existence de ce genre de fraude et de les avertir contre leurs dangers pour qu'ils soient plus vigilants. De plus, les entreprises, devraient instaurer un

---

sociétés et banques de grande renommée: HSBC, le Crédit Lyonnais, la société Alstom, ainsi que Thomson Technicolor...

[348]A. GRONDIN, art. préc.

[349]A-S. LECHEVALIER, art. préc.

[350]A.GRONDIN, art. préc.

[351]Le comptable en charge des règlements fournisseurs, reçoit un appel d'une personne prétendant être le président du directoire de KPMG SA, et lui demande sous le sceau d'une confidentialité absolue, de procéder à un virement de 232848 euros, qui seront nécessaires pour l'accomplissent d'une étude de «consulting». Sachant que l'escroc avait créé un courrier électronique similaire à celui du vrai président de la société pour lui envoyer la demande d'ordre de virement officielle. Sous le prétexte d'achat de filiales, ces manœuvres ont été répétées 8 fois, et le montant de la perte est devenu environ 7 millions d'euros. (V. Denis Lafay, *« KPMG: à Lyon, les dessous d'une escroquerie à 7,6 millions d'euros»*, art publié le 27/6/2014 à la tribune toulouse, www.toulouse.latribune.fr).

[352]Un individu s'était fait passer pour le président ou l'un des directeurs de la société Michelin et avait contacté un comptable d'un niveau très inférieur, lui demandant un virement urgent de 1,6 million d'euros vers un pays étranger (la république tchèque), pour accomplir une opération confidentielle. (V. Grondin Anaelle, art. préc).

formulaire de demande de «virement urgent» soumises à un contrôle accentué de la part des commissaires aux comptes. Depuis le développement de cette escroquerie, plusieurs entreprises ont aussi déjà modifié leurs sites officiels en éliminant les informations relatives à l'identité de leurs présidents.

Pour les banques, la *«fraude au président»* a longtemps été l'affaire de leurs seuls clients c.à.d. des entreprises[353]. Mais les entreprises victimes de telles fraudes se retournent de plus en plus souvent contre leur banque leur réclamant les versements indus aux escrocs. A cet égard, un arrêt rendu par le tribunal de commerce de paris le 30 octobre 2015[354] a condamné un établissement bancaire à rembourser, pour défaut de vigilance, à la société victime l'intégralité du montant du virement frauduleux.

Depuis Les banques agissent de façon préventive pour éviter toute condamnation future[355]: *«des protocoles de communications électronique offrent un niveau plus de sécurité très important»*[356]. La Société Générale planche même sur des solutions de reconnaissance vocale biométriques pour éviter à ses conseillers de se laisser tromper par les fraudeurs qui utiliseraient le même numéro que leurs clients.

Nul doute qu'une loi spéciale tant en France qu'au Liban, voire même le durcissement de la position de la jurisprudence française et libanaise, conduirait à une efficacité renforcée de la protection à la fois des entreprises mais également des banques.

Après avoir exposé, tout au long du premier titre de cette seconde partie, les moyens les plus innovateurs auxquels recourent les escrocs en les définissant et les illustrant d'exemples, passons sous un second titre à leurs modes de répressions qui s'avéreront être des plus primitifs vu que les législateurs des différents pays se retrouvent impuissant face à la montée de tous ces nouveaux procédés d'escroquerie et à leur caractère transnational. Partant de ces constats, la nécessité

[353]C'est dans des cas très rares, que les sommes seront récupérées par les sociétés victimes de cette fraude. C'est notamment le cas lorsque la banque soupçonne la véracité de la transaction effectuée vu son montant anormalement élevé et qu'elle la bloque un certain moment afin d'appeler le client et de s'assurer si le virement effectué est normal en demandant une confirmation du donneur d'ordre.

[354]B. GRAULLE *« «fraude au président»: les banques menacées»*, art. publié le 2/1/2015, les échos.fr, www.business.lesechos.fr.

[355]E. LEDERER, *«les banques en première ligne face à la «fraude au président»*, art. publié le 29/1/2015, les échos.fr, www.business.lesechos.fr.

[356] Idem.

d'une coopération internationale pour faire face aux infractions d'escroquerie transnationales s'avéra donc être plus que souhaitable (Titre 2).

Titre 2: L'impuissance du législateur face aux moyens frauduleux innovateurs:

Les nouvelles technologies de l'information et de la communication sont essentielles dans notre société et présentent de nombreux avantages au niveau du commerce et de l'échange. Mais leurs développements continuels s'accompagnent malheureusement d'un développement de la criminalité informatique, d'où la nécessité d'imposer des limites afin de freiner cette cyber escroquerie en légiférant des normes sur le plan national et international.

Notons à ce propos que la manipulation informatique est considérée unanimement par tous les pays comme l'élément matériel extérieur au mensonge qui constitue en lui-même les manœuvres frauduleuses exigées pour incriminer les comportements frauduleux des escrocs.

Mais la grande difficulté de légiférer de nouvelles lois réside dans le fait que l'internet ne connait ni de limites, ni de frontières à cause de son caractère transnational. En effet, les informations circulent sur l'Internet plus rapidement que jamais et les délinquants se trouvent dans des endroits éloignés des pays où leurs infractions produisent des effets.

Partant de là, Il s'avère difficile, voire impossible, de retrouver les auteurs des cyber-crimes, de les identifier, pour ensuite les sanctionner, vu que la plupart d'entre eux se présente sous des pseudonymes, noms imaginaires ou en usurpant l'identité d'autres.

Face à ce constat de multiplication des cyber-crimes il s'est avéré nécessaire de trouver des moyens pour y lutter. La lutte efficace que doit rechercher chaque pays ne peut en réalité être faite, eu égard les spécificités de ces nouvelles escroqueries en plein essor, qu'à travers une législation bien formée et non pas par une simple interprétation extensive des dispositions déjà existantes incriminant les

escroqueries dites classiques comme nous le verrons ci-dessous sous le premier chapitre (Chapitre 1).

Nous passerons en revu sous un second chapitre la nécessité d'une coopération internationale pour faire face aux infractions d'escroquerie transnationales (Chapitre 2).

Chapitre 1: Volonté de réglementation

Les infractions connues sous le nom de «cyber-crimes» sont considérées comme de nouvelles infractions très spécifiques. De ce fait, il s'avère en principe difficile voire même impossible de réprimer ces cyber crimes en ayant recours aux dispositions traditionnelles prévues dans les codes pénaux de droit français comme de droit libanais. C'est ce que nous étudierons d'une façon détaillée sous la première section de ce chapitre (Section 1).

Cela nous mènera à relever la nécessité de prévoir des sanctions spéciales réprimant les nouvelles formes d'escroquerie ce que nous appréhenderons sous la seconde section de ce chapitre (Section 2).

Section 1: Répression par assimilation à d'autres infractions incriminées

La délinquance informatique est associée à l'évolution technologique et à l'utilisation quotidienne de l'internet et des réseaux d'informatiques.

Face à cette délinquance informatique en voie de développement, et qui se multiplie de plus en plus au cours des dernières années, les deux codes pénaux français et libanais connaissent des limites que nous exposerons ci-dessous (Paragraphe 1).

Les tribunaux français et libanais tenteront donc d'étendre le champ d'application de quelques textes traditionnels aux nouveaux procédés d'escroquerie pour pallier le vide législatif dont souffrent leurs législations respectives (Paragraphe 2).

Paragraphe 1: la déficience des textes français et libanais

Les dispositions des codes pénaux, ayant comme but de punir les auteurs d'actes interdits par la loi et considérés comme dangereux, devrait régir tout genre d'infraction quel que soit son degré, sa complexité et les moyens qui sont utilisés pour l'accomplir.

Malheureusement le CPF, et encore plus le CPL, sont toujours déficients à l'égard de la délinquance informatique. Tous deux ne traitent pas spécifiquement de cette délinquance. Le CPF se suffit d'aborder les délits «*d'accès ou de maintien frauduleux dans un système de traitement automatisé de données, d'introduction, de modification et suppression de données contenues à l'intérieur du système*»[357].

Une des causes de déficience de ces deux codes pénaux est l'inconscience des dangers que la délinquance informatique peut engendrer. Les limites de ces codes se situent soit au niveau de la connaissance de la délinquance informatique ou bien au niveau des nouveaux actes mis en place par les délinquants et qu'ils n'incriminent pas.

Ainsi, plusieurs crimes informatiques qui peuvent, en principe, être qualifiés d'escroqueries échappent à cette qualification à cause des nouveaux procédés utilisés comme manœuvres frauduleuses.

Du fait de cette déficience et de ces limites, les dispositions «classiques» des codes pénaux ne sont plus suffisantes pour incriminer la multitude des nouvelles fraudes informatiques, d'autant plus que le principe d'interprétation stricte de la loi pénale[358] s'y oppose fermement[359].

Cela est très palpable en droit libanais où les juges libanais font face à une absence totale de législation spéciale en rapport avec les crimes informatiques et n'ont aucun choix que le recours aux dispositions traditionnelles du CPL et par suite opérer une interprétation analogique de la loi pénale[360].

---

[357]Art. 323-1 CPF

[358]«*Nulle infraction ne peut être sanctionnée par une peine, ou par une mesure de sureté ou d'éducation, si elle n'était prévue par la loi au moment où elle fut commise*» (V. M. HABHAB, op.cit.p.27)

[359]N. ELCHAER, op.cit., p. 34

[360]Ibid. p.38

En droit Français la situation est plus nuancée. Le droit français dispose, pour faire face à quelque «cyber-crimes», de la loi Godfrain que nous évoquerons dans le second paragraphe ci-dessous. Nonobstant cette loi, la législation française souffre quand même de plusieurs autres lacunes. Ces lacunes persistantes concernent un nombre d'actes en rapport direct avec l'informatique mais qui ne rentre malheureusement pas dans le champ d'application de cette loi. Ce code est dépassé et ne joue plus son rôle dissuasif face à la prolifération des cybers crimes. La révision du CPL est difficile à concevoir à cause de l'impossibilité de trouver un remède efficace et adapté aux cyber-crimes proliférés de manière ininterrompue.

Par suite, un recours aux dispositions pénales traditionnelles générales, telles que celles prévues pour la protection de propriété littéraire artistique et industrielle[361] ou même celle incriminant d'autres infractions classiques, semble un passage inévitable pour les tribunaux français.

La jurisprudence française a, comme premier pas, différencié entre les délits où l'informatique est un moyen de fraude auxquelles peuvent s'appliquer les incriminations traditionnelles et les fraudes consistant en une manipulation ou création de données ou altération de programme de traitement de ces données qui échappent à ces incriminations[362]. La France a donc tenté d'adopter une législation spéciale spécifique à cette criminalité sui generis en voie de développement continue. Nous soulignerons cela sous le second paragraphe ci-dessous.

A cela s'ajoute un autre problème dont souffrent les deux pays: les procédures pénales de poursuite des délinquances informatiques sont très couteuses et nécessitent une police bien formée et spécialisée ainsi que le recours à des experts en informatique

Partant de là nous nous poserons la question de savoir quelles lois traditionnelles les tribunaux français et libanais peuvent-ils appliquer pour incriminer les délits informatiques non prévus par leur lois nationales respectives? Comment ces tribunaux pourraient-ils concilier l'expansion des dispositions classiques avec le principe d'interprétation stricte qui s'oppose à toute interprétation large des textes de loi?

[361]Les informations peuvent être protégées par le droit de la propriété intellectuelle et artistique, tel la protection des marques, brevets… (V. N.EL CHAER, op.cit. p. 61)
[362]N. El CHAER , op.cit.,p.35

Paragraphe 2 : les textes aptes à extension

Tout d'abord les tribunaux peuvent penser à appliquer les dispositions de l'infraction de vol, le vol étant « *la soustraction frauduleuse de la chose d'autrui* »[363]. Or il est évident que la chose, élément constitutif de l'infraction de vol est de nature matérielle, mais est-il possible d'admettre la soustraction d'une chose immatérielle telle qu'une information ?

Si on examine les termes de l'article 311-1 du CPF, on conclut que les dispositions de cet article peuvent s'appliquer sans aucun problème si le vol est un vol de l'ordinateur en soi ou même lorsque les données ou information volées ont un support matériel (disques, bandes magnétiques, papier…). En effet, la soustraction de données ou information ayant un support matériel nécessite un déplacement matériel ce qui permet l'application des dispositions du vol.

Par contre, lorsque la soustraction a pour objet une information insusceptible de déplacement il s'avère difficile d'appliquer l'article 311-1CPF vu qu'aucune soustraction matérielle n'a lieu dans ce cas.

Les tribunaux confrontés à ce cas d'espèce ont en premier lieu opté pour une interprétation extensive de la notion de soustraction frauduleuse pour pouvoir incriminer les soustractions d'informations. C'est ainsi que le tribunal correctionnel de Montbéliard[364], suivi par la cour d'appel de Reims[365] et la cour suprême le 12 janvier 1989 ont consacré le principe de vol d'information .Mais cette position n'a pas été adoptée par la cour de cassation qui a déclaré, depuis 2008[366] , qu' «*en absence de toute soustraction de documents appartenant à une entreprise tierce, le simple fait d'avoir copié des données informatiques, qui n'en a jamais été dépossédée, puisque ces données, éléments immatériels, demeurent disponibles et accessibles à tous sur le serveur, ne peut constituer la soustraction*

[363]Art. 311-1 CPF, Art. 635 CPL
[364]T. corr. Montbéliard, 26 mai 1978, AJPI 1983, 533 (Ar cité par N. EL CHAER, op.cit.p.59)
[365]C.A. Reims, 27 février 1987, Patrick B. et Didier G. le procureur de la république et la société d'imprimerie Bourquin, Expertises 1987 (V.N.ELCHAER,op.cit.p.59)
[366]Cass.crim.4mars 2008, Dalloz 2008, p.2213, Rev.sc.crim., p.131

frauduleuse de la chose». Cette jurisprudence de la cour de cassation française est devenue de droit positif en droit français.

Au Liban, les tribunaux libanais ont aligné leur position sur celle de la cour de cassation française. Ils n'appliquent pas[367], à un cas de copiage des données enregistrées sur un disque, les dispositions de l'article 365 du CPL relatives à l'infraction de vol[368].

Une idée est sûre en droit français et en droit libanais: on ne pourra pas parler de possession de l'information mais plutôt d'un monopole et d'une exclusivité de celle-ci[369] [370].

Pourtant il faudra bien noter que la jurisprudence française consacre une valeur à des forces immatérielles telles le gaz ou l'électricité, et a admis la notion de vol de ces «forces» lorsqu'elles sont mesurables[371].

Outre le délit de vol dont les dispositions s'avèrent insuffisantes pour incriminer toute sorte de délits informatiques, on peut se demander si les tribunaux peuvent avoir recours aux dispositions classiques relatives à l'infraction d'escroquerie classique pour punir et incriminer les comportements informatiques illicites?

Il a été jugé que l'utilisation frauduleuse de l'ordinateur en tant que simulateur où les interventions sur les programmes informatiques sont considérées comme une escroquerie informatique par utilisation de moyens frauduleux[372].

La jurisprudence française a eu l'occasion à ce propos de trancher la question de savoir si l'information est considérée comme une chose, et si elle peut en conséquence faire l'objet d'une remise? La jurisprudence a tendance à étendre la

[367]Juge d'instruction de Beyrouth par sa décision rendue le 1er novembre 1999 (V.N.ELCHAER.op.cit.p.60)
[368]N. El CHAER, op.cit., p.60
[369]N. El CHAER, op.cit.,p. 61
[370]Selon M.HABHAB, le concept de soustraction reconnu dans la loi et accordé dans la doctrine et la jurisprudence ne peut être appliqué dans le cas des atteintes aux informations. Le concept consiste à supposer que la soustraction s'accomplit dans le cas où on peut enlever la chose, et la transporter d'un lieu à un autre (V. M.HABHAB, op.cit. p. 55).
[371]N. EL CHAER, op.cit p.68
[372]Ibid. p. 76 et 77

notion de remise d'une chose en abandonnant la notion traditionnelle de remise[373]. Cette tendance s'appuie en France sur la réforme du code pénal de 1994 ayant introduit la nouvelle définition de la «chose» objet de l'escroquerie en intégrant le terme de «*bien quelconque*»[374] et en ajoutant aussi l'expression «fourniture de service».

On aurait pu imaginer que cette même solution puisse être transposée en droit Libanais. Certains auteurs libanais étaient favorables à cette transposition s'appuyant sur l'idée que les romains reconnaissent que les choses incorporelles sont des biens susceptibles d'appropriation. D'autres auteurs libanais s'y opposaient excluant les informations de la catégorie des biens. C'est l'omnipotence du concept traditionnel « d'objet corporel matériel » qui a prévalu à cause du caractère immatériel des informations[375]. Tout ceci montre l'insuffisance de l'incrimination par le recours aux délits traditionnels d'escroquerie classiques.

Qu'en est-il pour l'application des dispositions régissant le délit d'abus de confiance en droit français et en droit libanais?

L'article 314-1 du CPF[376] et son équivalent l'article 670 du CPL incriminent l'abus de confiance qui consiste à dissimuler, détourner, dissiper, dégrader ou détruire un titre contenant obligation ou décharge, ou tout autre objet mobilier qui lui aura été confié.

Partant de cette définition nous nous demanderons si les fraudes informatiques peuvent être qualifiées d'un titre contenant obligation ou décharge? Remplissent-elles les conditions d'incrimination du délit d'abus de confiance?

L'auteur de l'abus de confiance ne soustrait pas la chose, au contraire, elle lui est remise par la victime sans avoir recours à des manœuvres frauduleuses. Cet abus suppose la remise d'une chose en vertu d'un contrat de détention précaire et un détournement volontaire au préjudice du propriétaire. Cette infraction est

---

[373]Ibid.p.81

[374]La remise n'a pas forcement à être matérielle puisque rien ne l'exige dans la loi (V. N. ELCAHER, op.cit.p.83)

[375] م. عبد الرؤوف ألحن، مرجع سابق، ص.١٣٨

[376]«*L'abus de confiance est le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé*».

considérée être réalisée lorsque le propriétaire de la chose ne pourra plus exercer ses droits sur cette chose, sachant que le détournement est « *le fait de donner à une chose une destination autre que celle prévue lors de la remise* »[377].

De même, l'objet de tout abus de confiance se résume à : des Effets, deniers, marchandises, billets, quittances ou tout autre écrit contenant ou opérant obligation ou décharge. Echappe à cette liste le terme de «meubles» qui fut remplacé par le terme « bien quelconque » qui peut aussi bien designer les objets incorporels[378].

Un arrêt de la cour de cassation française[379] a eu à résoudre un cas de fraude informatique en retenant la qualification d'abus de confiance.

Cette solution ne peut pas trouver sa place en droit libanais par application des dispositions des deux articles 670 et 671 CPL vu que l'abus de confiance ne peut pas s'appliquer aux choses incorporelles. L'objet de ce délit ne peut être jusqu'à ce jour n'être que matériel.

La doctrine libanaise soulève si bien la position classique du droit libanais en affirmant qu' «*il est difficile d'appliquer à un environnement immatériel des textes qui s'appliquent dans un environnement matériel* »[380].

Il faudra que le législateur libanais intervienne, comme il l'a fait le législateur français, en intégrant le terme de «bien quelconque» pour qu'il y ait extension des articles 670 et 671 CPL aux biens incorporels.

En définitif, nonobstant l'avancée quelque peu de la jurisprudence française que nous venons de citer plus haut, il reste que, comme pour les autres délits, la qualification d'abus de confiance même si elle peut s'appliquer à quelques

[377]N. El CHAER, op.cit., p. 85
[378] Ibid. p.86
[379]Cass.Crim,14 novembre 2000, Juris-Data numéro 007519: En l'espèce une entreprise a conservé le numéro de carte bancaire d'une cliente sans droit ni permission de cette dernière. Le président de l'entreprise a été condamné par la cour d'appel pour abus de confiance. Le président se pourvoi en cassation et invoque l'idée selon laquelle le détournement n'est punissable que s'il porte sur une chose corporelle or en l'espèce le détournement s'il a eu lieu a porté sur un numéro de carte bancaire par suite sur une information incorporelle. La cour de cassation confirme l'arrêt d'appel en insistant sur le fait que l'article 314-1 CPF s'applique à tout bien quelconque et non seulement aux biens corporels.
[380]M. HABHAB, op.cit, p.29

infractions informatiques, ne recouvre pas toutes les infractions commises dans le domaine informatique.

Il se révèle donc nettement de tout ce qui précède que l'extension des textes classiques de vol, d'escroquerie ou d'abus de confiance n'est pas la solution de secours adéquate. Mieux vaut donc réprimer les nouvelles formes d'escroquerie par des sanctions spéciales plus adaptées à la spécificité de chacune d'elles (Section 2).

Section 2: Répression par des sanctions spéciales adaptées

Il s'avère de plus en plus nécessaires pour tous les Etats de multiplier les organismes spécialisés en matière de cybercriminalité (Paragraphe 1) mais surtout de légiférer en premier lieu au plan national des lois spéciales spécifiquement adaptées à tout nouveau moyen d'escroquerie (paragraphe 2).

Paragraphe 1: Mesures préventives et organismes spécialisés

L'évolution technologique est un phénomène insaisissable qui ne pourra jamais, à notre sens, être contrôlé à cent pour cent. Mais il s'avère tout de même nécessaire de lui mettre des limites en imposant des lois spécifiques adaptées qui couveront le plus grand nombre d'infractions liées à cette évolution continue mettant un frein radical à ce nouveau genre de délinquance non-surveillée. A cette fin, il faudra que les législateurs nationaux des différents pays trouvent le juste équilibre entre la liberté qu'offre la technologie innovatrice d'une part et la nécessité de lui imposer des limites pour freiner les abus d'autre part.

En effet, les législateurs de par le monde ont tous l'obligation de protéger les données et informations de la même façon qu'ils ont déjà imposé le respect des droits d'auteur, des marques, des brevets d'inventions…et cela partant du fait que ces données ou information constituent une valeur sociale dont l'atteinte doit faire l'objet d'une incrimination spéciale spécifique.

Le gouvernement français a tenté de prévoir plusieurs moyens de prévention. Il a créé entre autre en 2009, un site internet : www.internet.signalement.gouv.fr pour

lutter contre les pratiques de cybercriminalité[381] et mis en place un service téléphonique pour répondre aux questions et plaintes des internautes ce qui permet d'éviter aux victimes potentielles d'être trompées.

La police nationale française a adapté les enquêtes pour qu'elles deviennent plus efficaces. Par la suite, le ministère intérieur français a établi plusieurs organismes spéciaux de lutte contre la criminalité informatique.

Pour n'en citer que les plus importants nous citerons: la BEFTI[382] qui est saisi suite à une plainte pour contrefaçon de logiciel ou intrusion frauduleuse dans les sites d'internet faites par les hackers et qui dispose de méthodes classiques de recherches et perquisitions; l'OCLCTIC[383] qui assure le travail des enquêtes judiciaires en regroupant trois équipes spécialisées: un groupe chargé des intrusions sur les réseaux Internet, un autre chargé des systèmes de transmission et télécommunications et un troisième a un rôle d'assistance et de collecte des preuves informatiques. L'OCLCTIC a même un rôle au niveau international puisqu'il est le point de contact central des échanges en matière de coopération policière au niveau européen[384]; enfin la DST[385] qui recherche et prévient les activités d'espionnage et de terrorisme et a créé une section qui lutte contre la criminalité informatique[386].

D'autres services français renommés pour leur efficacité sont les suivants: L'IRCGN[387](institut de recherches criminelles de la gendarmerie nationale), qui effectue les missions d'expertise et d'assistance pour l'établissement des preuves

[381]Ce site recueille toutes les plaintes faites contre les contenus illicites de l'internet et alerte immédiatement les pouvoirs publics en ce qui les concerne

[382]Brigade d'enquêtes sur les fraudes aux technologies de l'information créée le 22 février 1994, et le SEFTI (Service d'enquêtes sur les fraudes aux technologies de l'information) ou la BCRCI (Brigade centrale de répression de la criminalité informatique), V. J-F. CASILE «*le code pénal à l'épreuve de la délinquance informatique*», éd. Presses universitaires d'Aix Marseille, PUAM, 2002, p. 37.

[383]L'office central de lutte contre la criminalité liée aux technologies de l'information et la communication créée le 15 mai 2000 (V. M. HABHAB, op.cit., p. 137).

[384]N. El CHAER, op. cit., p.207.

[385]Direction de la surveillance du territoire créée en 1994, mais ses attributions sont fixées par le décret n^0 82-1100 du 22 décembre 1982.

[386] N.ELCHAER, op.cit., p. 207.

[387]Créé le 24 octobre 1990 (V.N. ELCHAER, op.cit. p. 210).

scientifiques; La DCSSI[388] qui évalue les menaces pesant sur les systèmes d'information et alerte les organismes[389]; Le SGDN[390], L'IHESI[391] et la CISSI[392] qui ont pour mission de proposer les mesures pour garantir la sécurité des informations ; Le CERTA[393] qui a pour objet de détecter et résoudre les atteintes à la sécurité des systèmes informatiques.

Il existe en outre des organismes français privés de plus en plus présent sur le terrain comme: le CLUSIF[394]qui constitue un point de rencontre et d'échange des évolutions de travail contre la criminalité informatique, et aide les entreprises à mettre en place des mesures de sécurité pour faire face aux cyber-crimes, son rôle est éducatif ; et le RECIF[395] qui lutte contre toutes les formes de criminalité informatique, et informe les entreprises sur les menaces qui y sont relatives.

Enfin des structures judiciaires spécialisées dans la délinquance informatique ont été établies en France qui sont le SEFTI[396] et la BCRCI[397]. Ces deux structures ont pour objet de mener les enquêtes judicaires sur tout le territoire national et de gérer le Bureau Central National d'Interpol.

Les Etats-Unis ont adopté, en 1986, une loi relative au système de télécommunication[398] et ont créé des organismes spécialisés[399]: le NCCS[400] qui a

[388]La direction centrale de la sécurité des systèmes d'information instituée par le décret du 31 juillet 2001.
[389]N.EL CHAER, op.cit. p. 212
[390]Le secrétariat général de la défense nationale (V.N.ELCHAER, op.cit. p. 212).
[391]L'institut des hautes études de la sécurité intérieure créé en 1989 (V.N. EL CHAER, op.cit. p. 213).
[392]La commission interministérielle pour la sécurité des systèmes d'information créée par l'Arrêté du 3 mars 1986 (V. N. EL CHAER, op.cit.p.214).
[393]Le centre de recensement et de traitement des attaques informatiques (V.N. ELCHAER, op.cit. p. 214).
[394]Le Club de la sécurité informatique des systèmes d'information français fondé en 1984 (V.N. EL CHAER, op.cit.p.216).
[395]L'institut de recherches et d'études sur la criminalité informatique, l'association créé en juin 1993 (V.N. EL CHAER, op.cit., p. 217).
[396]Le service d'enquêtes sur les fraudes aux technologies de l'information.
[397]La brigade centrale de la répression de la criminalité informatique.
[398]En application de cette loi toutes les informations ou données transmises mais non stockées sont recueillies plus particulièrement *« toute transmission, en totalité ou en partie, de signes, signaux, écrits, images, sons, sonnes ou renseignements de toute nature, par câble, radio, système électromagnétique, photo-électrique ou photo-optique »* (V. N. El CHAER, op.cit, p.251.)

pour rôle d'enquêter sur les fraudes informatiques (intrusions par les réseaux téléphoniques, les réseaux d'ordinateurs, piratage…)[401]; le CCIPS[402], constitué par des juristes spécialisés dans le droit informatique, qui a le rôle d'information et la responsabilité des poursuites[403].

L'Angleterre a de son côté, instaurer la « *National Hi-Tech Crime Unit* » qui est une unité spéciale de lutte contre la criminalité informatique[404].

Si le droit français a fourni des efforts palpables d'adaptation grâce aux organismes que nous avons mentionné plus haut, le constat en droit libanais est beaucoup plus amer.

En effet, le Liban souffre non seulement d'un manque législatif absolu, comme nous le soulèverons sous le second paragraphe, mais il n'a même pas tenu à proliférer les organismes spécialisés lui permettant de lutter contre la cybercriminalité. Les enquêteurs et organismes libanais ne sont pas familiers à la criminalité informatique, à cause du manque de formation. Ils ne sont pas non plus dotés de moyens efficaces pour recueillir les éléments de preuve dans le monde numérique.

Le seul organisme libanais qui a vu le jour est le *«bureau de lutte contre les cyber-crimes»*[405] crée en 2006. Ce bureau fait partie des forces de sécurité intérieure et de

---

[399]Au niveau de l'Etat Maine, nous trouvons une unité «The Maine Computer Cimes Task Force » qui mène des investigations contre tout genre de cyber-escroquerie et lutte contre les crimes et ont mis en œuvre un site www.mcctf.org pour alerter l'IFCC (internet fraud complaint center) V. J. A. HITCHCOCK, op.cit.p, 299). Pour l'Etat de Massachussetts nous trouvons la « High Technology and Computer Crimes Division » créé en 1997. Pour ce qui est de San Diego, Californie on trouve le SDCDA (San Diego County District Attorney) pour toute enquête. En juin 2000, le CATCH (Computer and Technical Crime High-Tech) a été créé (V.J.A.HITCHCOCK, op.cit. p. 304). De plus nous trouvons plusieurs sites afin que les victimes informent leurs gouvernements des attaques : www.IC3.gov (internet crime complaint center) créé par le bureau du FBI en 2000, ainsi que le site www.IFCC.gov (internet fraud complaint center) V.M.ALHENN.op.cit.p.232.

[400]National Computer Crime Squad

[401]N. ELCHAER, op.cit., p.204

[402]Le "Computer crime and Intellectual Property section" créé en 1991 (V. N.EL CHAER, OP.CIT.P. 209, M.ALHEN, op.cit.p.232)

[403]Nous trouvons aussi le USDOJ (United States Department of Justice) (V.J.A. HITCHCOCK, op.cit.p. 307)

[404]N.EL CHAER, op.cit.p.209

la police judiciaire libanaise. Pour faire face aux nouvelles méthodes d'escroquerie, le bureau organise des forums pour familiariser les individus et grandes sociétés et mieux les éclairer sur leurs effets.

Malheureusement ce bureau doit être mieux équipé et les policiers le constituant doivent être mieux formés, Il est également indispensable de lui prévoir un budget plus élevé afin de mieux lutter contre les cyber-escroqueries dont le nombre augmente d'au moins 5% annuellement[406]

Les pertes éprouvées par les victimes libanaises des cyber-escroqueries sont très élevées. Elles atteignent annuellement, selon les renseignements que nous avons pu nous procurer du commandant Suzanne El Hajj, 18 millions de dollars.

Tout ceci nous mène à conclure qu'il y a un décalage extrême en droit libanais entre le développement des domaines de la délinquance informatique et les moyens mises en place pour lutter contre cette délinquance qui est en voie de développement.

Pour ce qui est du droit français, il nous semble que les moyens de préventions entrepris ne sont pas suffisants et doivent à leur tour subir de modifications continuelles pour être de façon permanente au gout du jour. Les organismes spécialisés français devraient disposer d'encore plus de moyens et de matériel adéquat.

Après avoir expliqué l'impuissance des organismes de préventions face à la criminalité informatique, il s'avère indispensable voire même essentiel pour tous les pays de légiférer un droit spécifique en la matière, pour mieux adapter son droit positif aux délits informatiques.

---

[405] مكتب مكافحة الجرائم المعلوماتية.

[406]Ces informations ont été obtenues suite à l'interview, que nous avons déjà évoqué, avec le commandant Suzanne EL HAJJ.

Paragraphe 2: Recours à des lois spéciales adaptées

Légiférer des lois spéciales, claires et simples pour faire face à la cybercriminalité, est devenu une nécessité absolue puisque comme nous l'avons constaté, le droit pénal traditionnel est la plupart du temps impuissant voire inefficace face aux nouvelles méthodes de cybercriminalité.

La France était un des premiers pays à lutter contre les nouveaux dangers de la cybercriminalité à travers la loi de 1978[407]. Cette loi a mis en place un organisme ad hoc «la Commission Nationale de l'Informatique et de Libertés» qui a pour rôle de contrôler les opérations informatiques ainsi que les données personnelles en imposant certaines sanctions pénales[408].

Une seconde loi de 1985[409] fut ajoutée à celle de 1978. Cette nouvelle loi a pour objet d'étendre le champ d'application de l'ancienne loi pour mieux protéger le droit d'auteur, les phonogrammes et les logiciels.

Par la suite et précisément en 1988, une troisième loi a été adoptée: la «loi de Godfrain»[410](modifiée en 1994). Cette loi, intégrée aux articles 323-1 à 323-7[411] NCPF, a l'avantage d'être beaucoup plus spécifique que les deux précédentes réprimant précisément les fraudes informatiques visant tout système de traitement automatisé de données[412].

[407]Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[408]N.EL CHAER, op.cit, p.16
[409]Loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle.
[410]Loi n° 88-19 du 5 janv. 1988 relative à la fraude informatique
[411]CPF Art. 323-1 al.1, se réfère à l'accès ou au maintien frauduleux dénommé «intrusion non autorisée» dans tout ou partie d'un système de traitement automatisé de données, alors que le second alinéa fait référence à l'atteinte au système mais exige l'existence d'une influence exercée sur les données ou sur le système lui-même sans pour autant prévoir l'atteinte au dispositif de sécurité. CPF Art. 323-2 lui sanctionne l'altération du fonctionnement d'un système informatique. CPF art. 323-1 à 323-3 protègent eux les systèmes de traitement automatisé de données contre toute atteinte.
[412]Intrusion, altération, atteinte aux systèmes, atteinte aux données, association de malfaiteurs.

Nous constatons que les articles 323-1 à 323-7 NCPF ne traitent que d'un seul aspect de la délinquance informatique. Ils ne punissent que les atteintes[413] portées au système de traitement automatisé[414] de données[415], à l' exclusion des données non issu de tels systèmes. D'autre part le système de données doit nécessairement être en fonctionnement[416] pour que les dispositions de ces articles lui soient applicables. Autre que les délits d'accès et de maintien, l'article 323-1 NCPF sanctionne tout autre comportement ou délit informatique, dépourvu de toute qualification à condition de l'existence d'une intention frauduleuse caractérisée[417]. D'où l'on dira que le champ d'application de cet article est en principe assez large pour punir toute fraude informatique que cette dernière soit qualifiée ou non. La sanction de ce genre de délits est clairement mentionnée à ce même article[418].

En application de l'art. 323-4 NCPF[419] et de l'art 323-6 NCPF[420] les personnes morales peuvent à leur tour être poursuivies pour les délits informatiques de l'art

[413]L'atteinte au système a lieu dans deux cas : le cas d'accès à un système et le cas de maintien dans un système. L'accès incriminé consiste à pénétrer partiellement ou totalement dans un système informatique par une opération de manipulation informatique ou tout autre moyen. On exige dans ce cas que l'accès soit effectué d'une manière frauduleuse par une personne n'ayant pas le droit d'accéder au système. Pour ce qui est du maintien dans un système, il est punissable, lorsqu'il se prolonge au-delà du temps autorisé. Le maintien est ainsi un délit d'abstention «*consistant dans le fait de ne pas mettre fin à son branchement dans le système dès que l'on se rend compte de son erreur*». (V. N. El CHAER, op.cit., p.96).

[414]«*Ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité* » (V. N. El CHAER, op.cit., p. 96)

[415]La donnée étant *«la représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement*» (V. N. El CHAER, op.cit., p.96)

[416]Notons à cet égard que le réseau Internet est assimilé à un système de traitement automatisé de données,

[417]Un dol général: l'auteur doit avoir accompli l'accès ou le maintien au système sans droit, sans aucune autorisation et qu'il soit conscient de l'irrégularité de ces agissements faussant et entravant le fonctionnement de ces systèmes.et un dol spécial: l'auteur doit avoir agi frauduleusement.

[418]CPF Art. 323 al 2 impose la sanction consistant « *soit dans la suppression ou la modification des données contenues dans le système, soit une altération du fonctionnement*».

[419]CPF Art 323-4:«*la participation à un groupement ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 a* à *323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* ».

[420]«*Les personnes morales peuvent être déclarées responsables pénalement dans les conditions prévues par l'article 121-2, des infractions définies.. »*

323 NCPF. L'élément matériel est la participation à un groupement composé d'au moins deux personnes qui coopèrent pour commettre un délit. L'élément moral doit également être prouvé: il faut que l'entente entre eux ait été formée pour préparer l'infraction informatique[421]. L'Etat et les collectivités territoriales sont les seules personnes morales qui ne peuvent être poursuivies et déclarées pénalement responsables.

Le 13 juin 2001, le gouvernement français a adopté une quatrième loi spéciale pour lutter contre les cyber-crimes, intitulée « *de la sécurité dans la société de l'information* »[422]. Puis en 2003 une cinquième loi spéciale du 18 mars 2003[423]est venue régir les règles de perquisitions en ce qui concerne les nouvelles technologies.

Notons finalement que pendant l'année 2003, une proposition de loi française[424] a été présentée intitulée *«la lutte contre la cybercriminalité* ». Cette proposition de loi visait à protéger toute victime des virus, et réprimer «*le fait de détenir, d'offrir, de céder ou de mettre à disposition un équipement , un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée»*[425]. Suite à cette proposition de loi c'est une loi française datant de 2014[426] qui a été adoptée. Cette loi met en place, à travers 41 articles, un cadre juridique approprié permettant de traiter efficacement des délits relatifs aux systèmes informatiques.

[421]D'où la seule volonté ne suffit pas pour condamner la société et les associés, on exige l'existence d'éléments concrets qui marquent la volonté de commettre le délit tel: l'établissement d'un plan du système informatique ou l'achat des fournitures spécialement en vue de la commission de l'infraction… De même il faut que les personnes formant le groupement aient la conscience que leur activité est illicite.
[422]N.EL CHAER, op.cit.p.168
[423]Loi n^0 2003-239
[424] Projet de loi n^{o}905 déposé le 11 juin 2003
[425]N. EL CHAER, op.cit., p.155, CPF art. 323-3-1 donne un cadre juridique aux actions frauduleuses et aux outils qui servent à les commettre.
[426]Loi n^{o}2014-006 relative à « la lutte contre la cybercriminalité»

Quant au délit d'hameçonnage, un premier projet de loi a été proposé en France[427] et déposé en mai 2006. Ce projet avait pour objet *« l'obtention de renseignements indicateurs par fraude ou par faux semblant »,* et par le mot « faux » il visait directement l'hameçonnage. Mais ce projet de loi n'a pas été adopté. Un second projet de loi intitulé «*Vol d'identité et inconduites connexes*»[428] a été également proposé introduisant, à son article 10, une nouvelle infraction incriminant directement l'hameçonnage: le *«le vol d'identité et fraude à l'identité*». Mais malheureusement jusqu'à nos jours ce second projet de loi n'a été adopté.

Toutes ces lois et projet de loi français sont évidemment un grand pas vers le vote de multiples lois spéciales françaises supplémentaires contre les cybers-crimes.

Le législateur français a en outre modifié les incriminations des textes pénaux existants pour faire face aux délinquances informatiques. Les nouvelles moutures de quelques textes français se réfèrent d'une façon implicite à l'exploitation du système informatique. On trouve tout d'abord les infractions de faux: l'article 441-1 NCPF, englobe désormais non seulement les écrits mais *«tout autre support d'expression de la pensée*»[429]; l'article 222-18 CPF intègre les supports informatiques *« la menace, par quelque moyen que ce soit, de commettre un crime ou un délit contre les personnes*»[430].

Pour ce qui est du droit libanais, ce droit est toujours très lacunaire. Il est encore loin d'avoir une législation qui confère une protection minimale contre l'usage frauduleux des nouvelles technologies ou même contre l'accès ou l'intrusion dans le système informatique et la détérioration des données. Notons tout de même

[427]Projet C-299.
[428]Projet C-27.
[429] J-F. CASILE, op.cit.p.41
[430]Mais il faudra bien noter à cet égard que la loi française n° 200-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique n'a pas admis l'assimilation totale entre un écrit au sens traditionnel et un écrit au sens électronique. Le droit pénal congolais, considère à son tour que l'information, même à valeur immatérielle, peut constituer un écrit sachant que cette loi n'exige aucune condition quant à la forme de l'écrit (V. la convention sur la criminalité et le droit pénal congolais, Christophe KaweKasango, mémoire université de kinshasa, RDC-licence en droit 2003). Il en va de même également en droit suisse, « *les données informatiques peuvent constituer des écrits propres ou destinés à prouver des faits ayant une portée juridique* » (arrêt de 1970).

l'existence d'une loi libanaise de 1999[431] relative à l'interception des communications privées[432].

En outre, un projet de loi libanaise relatif à la cybercriminalité a été proposé par le ministère de l'Economie et du commerce ECOMLEB, en 2005 mais n'a pas été adopté par le parlement libanais jusqu'à nos jours. Ce projet de loi propose d'ériger en infractions pénales les actes suivants : accès illégal à tout ou partie d'un système informatique ; l'interception illégale de transmission non publiques ; atteinte à l'intégrité des données, atteinte à l'intégrité d'un système ; abus de dispositif ; la falsification informatique et la fraude informatique[433].

Nous pensons que l'adoption de ce projet de loi, ainsi qu'une loi sur le commerce électronique seraient de bons points de départ pour la lutte contre les infractions informatiques. Ces deux lois une fois adoptées viendront combler le vide législatif et pourront ultérieurement être mise à jour de façon continue pour offrir la plus grande protection possible.

La doctrine libanaise propose à son tour des solutions supplémentaires: Dr. M. Habab, propose la technique de co-régulation, de coopération entre les pouvoirs publics, les usagers et les entreprises pour mettre en œuvre une régulation par laquelle *« ni l'Etat ou le juge à travers la réglementation, ni les entreprises, ne peuvent réguler seuls Internet, les risques d'impuissance ou de déviation seraient trop importants… ils peuvent se compléter, collaborer, chacun dans leur rôle respectif »*[434].

Au niveau des pays arabes, quelques-uns ont déjà légiféré des lois spéciales contre «les crimes informatiques», on cite par exemple la loi Jordanienne[435]de 2001, la

[431]N^0 140 du 27 octobre 1999

[432]Cette loi est intéressante puisqu'elle oblige, en application de son article 5, les opérateurs libanais d'aider les autorités publiques d'enquêtes. En France, les acteurs privés coopèrent avec les organes spécialisés, pour faire face à la cybercriminalité, et une nouvelle loi du 15 novembre 2001, est venue renforcer les pouvoirs d'investigation des enquêteurs dans le domaine des nouvelles technologies (V.N.EL CHAER, op.cit.p.183).

[433]Le projet a le mérite d'expliquer chacune de ces infractions, et de proposer des sanctions adéquates à chacun d'elles. De plus, le projet s'attarde sur la notion d'intention frauduleuse condition exigée pour l'incrimination de tout genre de délit informatique.

[434]M. HABHAB, op.cit., p.280

[435]Loi n^o 58 du 31 décembre 2001 (V.M.ALHENN, op.cit.p.112).

loi Tunisienne de 2000[436] régissant le commerce électronique, et la loi de Dubaï[437] de 2001[438] enfin, la loi égyptienne numéro 15 en 2004[439]. A notre avis il serait grand temps que le droit Libanais aille lui aussi en ce sens et vote une loi spéciale régissant le plus grand nombre de cyber crimes tout en s'inspirant de toutes les lois spéciales déjà prévues tant par les pays occidentaux qu'orientaux[440].

Aux Etats-Unis, on trouve des lois spécifiques[441], tels que le «Counterfeit Acces Device and Computer Fraud and Abuse Act » [442] de 1984[443], ou la loi fédérale «Computer Fraud and Abuse Act » [444] de 1984, en 1997 « the consumer Internet privacy act » a été adopté, et en 2010 la loi « The Protecting Cyberspace as a National Asse Act » a été adopté[445]. Sachant que l'Allemagne[446], la Suisse[447] et le Danemark[448], l'Etat Philippin[449] ont eux aussi élaborés des lois spécifiques[450]. A la nécessite de légiférer au plan national s'ajoute l'impératif de prévoir des mesures préventives afin d'échapper à ce genre d'infractions tels que : des forums de

[436]Loi n^0 83 du 9 mai 2000(V. M. ALHENN, op. cit. p.112)
[437]Loi n^0 2, en 2002 قانون امارة دبي الخاص بالمعاملات و التجارة الالكتروني (V.F.ALJABBOUR, op.cit.p.186)
[438]Loi no 2 du 12 février 2001.
[439]م. عبد الرؤوف ألحن، مرجع سابق، ص. ١١٢
[440]Nous citons de même, Oman le premier pays arabe à légiférer une loi contre les infractions informatiques, en 2001, un décret numéro 72, est entré en vigueur, incriminant ces infractions commises par les ordinateurs ainsi que celles relatives aux cartes, et l'Arabie Saoudite en a fait de même en adoptant le 21 mai 2007 une loi pour lutter contre ces infractions informatiques (V.M.ALHENN, op.cit.p.112-113)
[441]Le 1 décembre 2005, le Congress Américain a adopté la loi du CANSPAM, pour incriminer toute atteinte faite par le biais des « scams ». (V.J.A.HITCHCOCK, op.cit. p 56)
[442] Amendé en 1986, 1988, 1989, 1990, 1994 et enfin en 2001 par the «Patriot act»
[443] م. الغول ، مرجع سابق ، ص ٣٣٣
[444]م. عبد الرؤوف ألحن، مرجع سابق، ص ١٠٤
[445]Loi n ^{0} 773, du 18 juin 2010, qui élargit la compétence du président des Etats-Unis et ses pouvoirs en Etat d'urgence pour mieux contrôler ce monde virtuel. Il pourra même ordonner l'arrêt de fonctionnement de sites internationaux tels «Google» ou «Yahoo» pour des raisons d'urgence nationale (V.M.ALGHOUL, op.cit.p.335).
[446]Art. 263 A code pénal allemand (V.M.ALHENN, op.cit.p.p.101)
[447]Art.147 du code pénal suisse (loi de 1995), incriminant l'escroquerie par le biais de l'internet, ainsi que le détournement électronique frauduleux des biens (V.M. ALHENN, op.cit. p. 103)
[448]En 1985, la loi de lutte contre les délits portant atteinte à d'ordinateur et les délits informatiques (V.M. ALHENN, op.cit. p.103)
[449]Le seul Etat à avoir totalement mis à a jour sa législation (N.EL CHAER, op.cit. p. 274)
[450]Le législateur grec a adopté une loi incriminant le cyber-escroquerie : art.386 code pénal grec (V.M.ALHENN, op.cit.p. 102)

formations des internautes et utilisateurs de technologie pour les sensibiliser aux dangers de ces cyber crimes, la mise en œuvre d'un centre d'alerte et de secours sur l'Internet tel le CERTA qui détecte et résolut les incidents informatiques...

L'impératif de légiférer des lois nationales adaptées aux modes innovateurs d'escroquerie doit nécessairement aussi se doubler, pour plus d'efficacité et de protection, d'une coopération internationale essentielle pour mettre un frein radical à ses infractions transnationales[451] (Chapitre 2).

Chapitre 2: La nécessité d'une coopération internationale

Les cybercriminels envahissent progressivement le monde de l'Internet et vu que l'internet ne connait pas de frontières, les cybers-crimes commis par ces derniers dépassent les frontières, pour endommager plusieurs pays ou plusieurs entreprises multinationales.

Les problèmes émergent du fait que les délinquants se situent dans un pays tandis que les effets de leurs actes délictueux ont lieu dans un autre pays. Ceci fait que plusieurs tribunaux pourront se déclarer compétents et voudront voir leurs lois nationales s'appliquer. Or les lois nationales, dont le champ d'application s'arrête aux frontières nationales d'un certain pays, ne peuvent régir ces infractions transnationales dont les effets dépassant les dites frontières.

Il est vrai que quelques pays industrialisés disposent, comme nous venons de le voir sous le premier chapitre, de législations spécifiques. Mais le problème réside dans le fait que ces législations nationales sont très disparates vu que chaque pays a répondu d'une façon différente à la criminalité informatique: Certains ont élaboré de nouvelles dispositions, d'autres ont modifiés leurs anciens textes, tandis que d'autres n'ont rien légiférer jusqu'à ce jour.

[451]F.JABBOUR propose lui une intervention législative au niveau des pays arabes pour imposer une coopération des organismes spéciaux avec les secteurs privés spécialisés en matière informatique.

فريد منعم جبور، ، مرجع سابق ، ص. ٢١٣

L'adoption d'instruments juridiques internationaux adéquats s'avère par conséquence un outil indispensable de lutte contre les cybers-crimes. L'effort requis, au niveau national en adaptant des lois nationales spéciales devra être doublé au niveau international par des conventions, pour une meilleure coopération entre les pays.

Les membres du G8[452] ont déclaré à ce propos dès 1997 qu'il est : **«***impossible pour un pays, compte tenu de la nature des réseaux modernes de communications d'agir seul pour répondre à ce problème nouveau de la criminalité liée aux technologies de pointe»*[453], une coopération internationale est donc indispensable et impérative.

Nous verrons que la bonne solution serait l'harmonisation des différents droits nationaux et la coopération entre les différents états, coopération qui prend le plus souvent la forme d'accords ou de conventions bilatérales ou multilatérales (Section 1) dont les recommandations et mesures de préventions doivent être suivies (Section 2).

Section1 : Conventions internationales réprimant les infractions liées à l'informatique

Le droit pénal international ne traite pas des crimes informatiques, mais se contente de renvoyer aux lois internes. Or la diversité des lois nationales peut causer des problèmes et empêcher l'incrimination de maintes infractions informatiques.

Partant de là, la solution idéale serait l'harmonisation des lois nationales par l'adoption d'accords et de conventions bilatéraux et multilatérales entre les différents pays. Ces accords ou conventions visent des solutions à plusieurs problèmes dont notamment l'extradition, l'entraide judicaire, les problèmes de compétences.

A cette fin, plusieurs mécanismes de coopération ont été instaurés au sein de l'Union Européenne, et maintes recommandations ont été émises par les Conseil de l'Europe, pour pousser les 41 pays membres non seulement à adapter leurs

[452]Groupe des huit pays les plus industrialisés
[453]N. El CHAER, , op.cit, p.39

législations et signer des conventions et accords entre eux, mais également pour les encourager à intensifier leurs enquêtes transnationales pour une meilleure coopération contre les cybers crimes.

Nous passerons donc en revue les conventions traitant des problèmes d'extradition et d'entraide (Paragraphe 1) pour évoquer par la suite celles traitant de la compétence des Etats (Paragraphe 2).

Paragraphe 1: Extradition et entraide judiciaire

L'extradition est considérée comme le plus ancien instrument de coopération internationale[454].

Pour ce qui est du problème d'extradition[455], une convention européenne d'extradition a vu le jour le 13 décembre 1957 à Washington. Cette convention donne, à son article 1, une définition de l'extradition qui est la suivante: que les parties signataires de la convention se fassent *«livrer réciproquement les individus qui sont poursuivis pour une infraction ou recherchés aux fins d'exécution d'une peine ou d'une mesure de sureté par les autorités judicaires de la partie requérante».*

Cette convention impose, à son article 2, pour son application d'une part l'existence de la condition préalable de double incrimination c.à.d. que l'infraction soit punissable tant dans le pays de la partie requérante que dans celui de celle

[454]Il semble relever « *à la fois du devoir de la solidarité dans la lutte contre le crime, de l'intérêt bien compris de notre pays qui n'a pas à recueillir les criminels impunis et du moindre mal pour éviter que les Etats requérants n'en viennent à des procédés unilatéraux*» V. M. HABHAB, op.cit.p.334

[455]«*Mécanisme juridique par lequel un Etat (l'Etat requis) sur le territoire duquel se trouve un individu, remet ce dernier à un autre Etat (l'Etat requérant) afin qu'il le juge ou lui fasse exécuter sa peine*» (V.M.HABHAB,op.cit.p.334)

requise; et d'autre part que la peine de l'infraction dans chacun des deux pays soit de minimum un an d'emprisonnement.

Dès lors que l'infraction informatique commise est prévue dans ladite convention européenne l'extradition peut être invoquée par un Etat auprès d'un autre Etat sans qu'il y ait entre eux un accord bilatéral de coopération judicaire d'extradition à condition de remplir l'exigence de la double incrimination de l'infraction au niveau des deux états requis et requérant et que la peine maximale de l'infraction qu'une personne a commis, dans les deux pays, n'excède pas un an d'emprisonnement.

Une autre convention a été adoptée au niveau européen à ce même sujet en 1997 dans le cadre de l'Union Européenne[456].

Par la suite le 15 décembre 2001[457], une troisième convention fut prise, éliminant la condition de la double incrimination pour certaines infractions. Cet objectif a été réalisé par l'adoption d'une décision-cadre qui a pour but de substituer le système de l'extradition et de rendre la procédure plus simple[458].

Les pays arabes, dont le Liban, ne sont pas familiers avec le mécanisme d'extradition et ne sont pas encore prêts à l'appliquer. En effet, la condition de la double incrimination empêche l'application de ce mécanisme. La plupart des pays arabes ne disposent en effet même pas de législations spécifiques pour régir ces délits informatiques, d'où l'incrimination sur la base des textes traditionnels non spécifiques aux délits informatiques que pratique ces pays, ne remplis pas la condition de double incrimination préconisée dans la convention européenne de 2001. Ainsi que les articles 32 et 33 du code pénal libanais, forment un obstacle à l'extradition[459].

---

[456]N. EL CHAER, op.cit., p. 282.

[457]Suite aux attentats de 11 septembre 2001, les membres de l'U.E. ont décidé le 14-15 décembre 2001 de créer un mandat d'arrêt européen qui se «*substituera au système d'actuel extradition entre Etats membres et permettra la remise directe des personnes recherchées d'autorité judiciaire, sans que la règle de la double incrimination soit requise pour quelques infractions*» (V. N. ELCHAER, op.cit.,p.282)

[458]N.EL CHAER, op.cit.p.283

[459]Art.22 du code pénal énonce que « *l'extradition n'est pas permise pour les infractions qui relèvent des compétences territoriales, personnelle et réelle de la loi libanaise fixées…* » Et l'art.23 du même code énonce que l'extradition est refusée lorsque l'infraction n'est pas punie par la loi libanaise d'une peine criminelle ou délictuelle (puisque la double incrimination est

Notons Enfin, que la convention européenne d'extradition de 2001 prévoit que même en cas d'absence de traité d'extradition entre deux Etats, ces derniers auront quand même l'obligation de communiquer au Secrétaire General du Conseil de l'Europe, le nom et l'adresse des autorités en charge d'envoi des demandes d'extradition.

Pour ce qui est de l'entraide judiciaire, qui consiste pratiquement en l'audition des témoins, l'accomplissement d'actes d'instruction, la communication des pièces ou dossiers, les demandes d'obtention des données stockées sur un système informatique qui existe sur le territoire d'un autre pays…, une convention européenne a été adoptée à Strasbourg le 20 avril 1959, pour régler le problème d'entraide judiciaire en matière pénale entre les pays signataires de cette convention[460].

L'importance de cette convention émerge du fait que les pays signataires, en application de l'article 1 de la convention, *«s'engagent à s'accorder mutuellement (...) l'aide judicaire la plus large possible dans toute procédure visant des infractions dont la répression est, au moment où l'entraide est demandée, de la compétence des autorités judicaires de la partie requérante»*.

L'entraide judiciaire en matière pénale se fera, conformément à l'article 3 de la convention, au moyen de commissions rogatoires internationales[461] adressées à la partie requise par les autorités judicaires de la partie requérante et qui ont généralement pour objet d'accomplir des actes d'instruction ou de communiquer des pièces à conviction, des dossiers ou documents. Ces commissions régies par des traités internationaux et des lois internes servent pour une meilleure coopération internationale[462],

La convention traite d'une façon détaillée, à son titre III, de la procédure à suivre d'une part en cas de remise d'actes de procédures et décisions judicaires: remise par simple transmission ou selon les procédures prévues par le pays de la partie

---

requise, donc ces articles empêchent l'application du système d'extradition) V. M. HABHAB, op.cit., p.334.

[460]N.EL CHAER, op.cit.p.283

[461]*«Demande adressée par l'autorité judicaire d'un état à l'autorité d'un état étranger d'accomplir en son nom et pour son compte une mesure d'instruction »*

[462]M, HABHAB, op.cit., p.329

requérante avec preuve de la remise; et d'autre part en cas de comparution de témoins, experts et personnes poursuivis: par citation à comparaitre, indemnités frais de voyages d'un témoin, d'un expert…

Tout en sachant qu'un pays peut refuser, en application de l'article 2 de cette convention, de conférer à un autre une aide judicaire lorsqu'il estime que l'exécution de la demande d'extradition «*est de nature à porter atteinte à la souveraineté, à la sécurité, à l'ordre public ou à d'autres intérêts essentiels de son pays*»[463].

C'est précisément le 23 novembre 2001, qu'une convention sur la cybercriminalité a vu le jour à Budapest[464]. Cette convention avait pour objet la lutte contre les délits informatiques[465] en harmonisant les lois nationales en matière d'attaques contre les systèmes d'information et traiter entre autre des questions d'extradition, d'entraide et des problèmes de compétence[466] .Elle exige l'entraide la plus large possible et encourage les Etats à designer une autorité centrale unique pour mieux gérer la coopération entre eux ou même designer une autorité émanant de chacun d'entre ces pays et dans ce cas la coopération sera faite entre ces différentes autorités.

Cette même convention s'attarde également sur la notion de rapidité [467]dans la collecte des preuves électroniques et impose aux Etats l'obligation d'une

[463]N.EL CHAER, op.cit.p.284
[464]La Convention du Conseil de l'Europe sur la cybercriminalité
[465]En particulier elle traite de quatre genre d'infractions : 1-Les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes, 2-les infractions informatiques et fraudes informatiques (manipulation des données informatique pour effectuer un transfert illicite de propriété ou pour se procurer un avantage patrimonial frauduleux au préjudice d'autrui), 3- altération ou sabotage informatique (altérer le fonctionnement d'un système informatique par l'introduction, transmission, effacement, détérioration ou altération des données informatiques, exemple : virus qui ralentissent le fonctionnement du système), 4- les infractions portant atteinte à la propriété intellectuelle. Elle mentionne explicitement que tous ces comportements ne peuvent être incriminées que si elles ont été commises d'une façon intentionnelle et sans droit c.à.d. sans autorisation.
[466]La convention avait pour but: 1- l'harmonisation des législations nationales pour faciliter la lutte contre la délinquance liée à l'informatique, 2- l'adaptation des moyens d'enquête et de poursuites au terrain du cyberspace, 3- la mise en place d'un système de coopération international rapide et efficace (V.N. EL CHAER, op. cit.p. 334)
[467]M. HABHAB, op.cit.p. 345

conservation rapide de données stockées au moyen d'un système informatique tout en imposant une durée de temps maximale et une confidentialité absolue.

En fin de compte cette convention invite les pays à collaborer, à tous les niveaux, et s'entraider aux fins d'investigation ou de procédures. Elle propose l'idée d'une coopération à travers un réseau de points de contacts disponibles 24h/24, 7j/7[468].

Outre les deux problèmes d'extradition et d'entraide judicaire, les conventions traitent également des problèmes liés à la compétence des Etats (Paragraphe 2).

Paragraphe 2: Compétences des Etats

Les délits de cybercriminalité transfrontaliers posent, vu la multitude des éléments de rattachement territoriaux, également deux problèmes celui de la «revendication simultanée de compétences» par plusieurs Etats et celui de la détermination de la loi applicable.

La solution à ce genre de problèmes de compétence serait l'existence de mécanismes de transmission des procédures. Or cette transmission ne peut être résolue que par des accords, par lesquels un état renonce à ses droits juridictionnels en faveur d'un autre[469]. Or ce genre de convention est très rare, ce qui oblige les différents Etats à revenir à l'application de leurs lois nationales en matière de compétence[470].

Pour revenir au principe en matière de compétence territoriale, la compétence revient à la juridiction de l'Etat où a été commise en tout ou partie l'infraction. Cet Etat commencera les enquêtes et déclenchera les poursuites en appliquant ses lois nationales. Or, en ce qui concerne les délits informatiques, il est parfois difficile de localiser le lieu de commission de l'infraction ce qui rend la détermination du for

[468] N.EL CHAER, op.cit.p.350
[469] N. EL CHAER, op.cit.p.297
[470] ف. م. جبور، مرجع سابق ، ص ٢٠٥

compétent beaucoup plus compliquée qu'elle n'apparait[471]. Afin d'éviter la question de conflits, les Etats doivent conclure des accords pour traiter les questions des critères de compétence.

En France[472], comme au Liban[473] le principe est celui de la territorialité. Les tribunaux français et libanais se considèrent compétents pour les délits informatiques dès lors que l'un des faits constitutifs de l'infraction a eu lieu sur leur territoire. On cite à cet égard l'arrêt Yahoo[474], dans lequel le tribunal correctionnel de Paris s'est déclaré compétent, puisque Yahoo avait publié sur son site internet faute de système de filtrage des pages concernant des ventes aux enchères d'objets Nazis[475].

Le juge libanais peut en outre se déclarer compétent lorsque le délinquant avait prévu la réalisation du résultat de l'infraction sur le territoire libanais.

Le droit français et le droit libanais[476] consacrent non seulement le principe de territorialité mais également deux autres principes[477]: celui de «l'extension par l'indivisibilité»[478] et celui de «l'extension par assimilation»[479]. Il faut noter que le droit français s'applique aussi aux crimes qui ont eu lieu au bord des navires, aéronefs militaires français ou même non immatriculés en France, et même s'applique aux questions de complicité : tout individu qui en France s'est rendu coupable comme complice d'un crime même si commis à l'étranger sera jugé par les tribunaux français[480].

---

[471]M. HABHAB, op.cit.p. 118

[472]En application de l'article 113-2 CPF

[473]Art. 15 CPL, selon lequel la compétence revient aux tribunaux libanais lorsqu'un des éléments constitutifs du délit ou un des actes de participation criminelle ou accessoire de l'infraction a été commis au Liban, ou si le résultat criminel se produit sur le territoire libanais ou même s'il était prévisible qu'il s'y produise.

[474]TGI Paris le 22 mai 2000 (arrêt cité par N. EL CHAER, op.cit.,p. 292)

[475]Comme sanction Le TGI a condamné la société Yahoo à retirer les dites publicités et lui a imposé de mettre en place un système de filtrage des contenus pour les internautes français.

[476]M. HABHAB, op.cit., p.120

[477]N. El CHAER, op.cit, p.298

[478]Selon lequel le juge français ou le juge libanais est compétent lorsque les faits commis à l'étranger forment un tout indivisible avec les infractions imputées en France/ au Liban.

[479]En application duquel le juge français est compétent lorsqu'on assimile certains actes commis en France à un élément constitutif de cette infraction

[480]N.EL CHAER, op.cit. ,p. 301

D'autre part, les tribunaux français et libanais[481] se déclarent compétents en application des règles de compétence personnelle, déterminée par la nationalité de l'auteur ou de la victime. Ainsi Ces tribunaux se considèrent compétents dès lors que soit l'auteur soit sa victime est de nationalité française/ Libanaise.

La loi française, et même la loi libanaise depuis 1996, vont même jusqu'à consacrer le principe de compétence universelle selon lequel la loi française/libanaise s'applique lorsque la personne est arrêtée sur le territoire français/libanais, peu importe sa nationalité lorsque les délits informatiques portent atteinte aux intérêts fondamentaux de l'Etat[482] .

De tout ce qui précède et vu les larges compétences nationales sur la base desquelles chaque pays se déclarera compétent lorsqu'un éventuel délit informatique viendrait à endommager les intérêts de plusieurs pays nous déduisons l'existence d'une insécurité juridique régnant en matière de compétence internationale.

La convention européenne de Budapest de 2001 a réaffirmé les trois principes que nous retrouvons en droit français et libanais selon lesquels tout Etat est considéré compétent lorsqu'un de ses éléments de l'infraction a été commis sous son territoire ou que le résultat de cette infraction a eu lieu dans ce pays, ou même si un de ses ressortissants a commis l'infraction[483].

Or le même problème que nous avons déjà soulevé plus haut se pose : les infractions commises au moyen de systèmes informatiques n'ont pas de territoire fixe ce qui fait que plusieurs Etats peuvent se considérer compétents pour résoudre le litige, et le délinquant peut être sanctionné, pour un même fait, plusieurs fois dans plusieurs pays. Pour échapper à ces problèmes, la convention a imposé l'obligation de consultation entre les pays concernés et de coopération[484] entre eux au niveau de collecte de preuves sous forme électronique par exemple, ainsi qu'au niveau des infractions pénales liées à des systèmes et données informatiques. De plus, pour traiter du problème de compétence, plusieurs auteurs ont proposé différents critères à unifier entre Etats pour designer la compétence tels : le lieu où

[481] Art. 19 et 20 du CPL
[482] Art. 113-10 CPF
[483] م، عبد الرؤوف ألحن ، مرجع سابق، ص ٢٠٠ - ٢٠١
[484] N. EL CHAER, op.cit.p.327

l'infraction a été commise, ou le critère de prévisibilité du dommage, ou le critère du droit le plus approprié[485].

Afin de résoudre le problème de conflits positif de compétences, plusieurs solutions ont été proposées : placer une hiérarchie de compétences selon les valeurs atteintes par l'infraction[486], ou bien créer un critère de rattachement basé sur un élément objectif dans le but de coordonner l'enquête, la poursuite et la répression de ces délits informatiques transnationaux. L'exemple des tribunaux américains, qui utilisent un test de contact pour déterminer leur compétence et délimiter les hypothèses dans lesquelles leurs tribunaux sont compétents, est un exemple à suivre par tous les autres pays[487]. Nous pensons que la meilleure solution à ces problèmes reste tout de même l'élaboration d'accords internationaux sur le problème de compétence entre les pays concernés.

Les accords et conventions ont le mérite de résoudre un autre problème qui se pose celui de l'efficacité internationale des jugements répressifs rendus à l'étranger. En France et au Liban, les jugements répressifs rendus à l'étranger sont dépourvus d'effets sur le territoire français/libanais, de même pour les jugements de condamnations rendues à l'étranger qui ne sont pas exécutoires en France/ au Liban. Ce principe de territorialité des jugements répressifs ne pourra être atténué et la règle « non bis in idem »[488] ne prendra plein effet ni en droit français ni en droit Libanais que par l'intervention de conventions internationales en la matière[489].

L'intérêt des conventions internationales réside essentiellement dans les résolutions et recommandations qu'elles offrent et qui devrait être suivis à la lettre (Section 2).

[485] ف. جبور، مرجع سابق ، ص ٢٠٧
[486] N. El CHAER, op.cit, p. 307
[487] M. HABHAB,op.cit.p.128
[488] Selon lequel une personne ne peut être condamnée plusieurs fois pour un même délit, par plusieurs tribunaux appartenant de plusieurs Etats.
[489] Ce stricte principe de territorialité des jugements répressifs est atténué par quelques conventions internationales (V. N. EL CHAER, op.cit., p, 308)

Section 2: Les Résolutions mises au point par les congrès et organisations internationales :

Maintes associations internationales de droit pénal, groupes de travail et organismes internationaux ont formulé plusieurs résolutions pertinentes au sujet des cyberescroqueries. Nous allons exposer tout de suite brièvement celles de l'AIDP (paragraphe 1), pour présenter par la suite celles d'autres groupes de travail et organismes internationaux (paragraphe 2).

Paragraphe 1: Résolutions de l'AIDP

Il est intéressant de souligner l'importance accrue des résolutions des congrès et organisations internationales.

Les résolutions intéressantes à soulever sont premièrement celles de l'AIDP[490] qui traitent longuement des infractions informatiques et autres crimes contre la technologie informatique. Les résolutions de cette association visent notamment la protection de la vie privée des nouveaux dangers causés par la technologie informatique ainsi que les droits internationaux de l'homme et leurs droits d'accès aux informations.

L'association propose des mesures de prévention non pénales, mais qui nécessitent pour leurs efficacités un encouragement au niveau national et supranational, tels: «*l'utilisation de mesures de sécurité volontaires par les usagers d'ordinateurs, l'imposition de mesures de sécurité obligatoires dans certains secteurs sensibles, ainsi que la création et mise en œuvre de législations pour protéger la sécurité des ordinateurs (...) le développement de normes professionnelles dans l'industrie informatique, ainsi que la formation du personnel des systèmes de l'investigation, de la poursuite et même du système juridique*»[491].

[490]L'Association Internationale de Droit Pénal créée en 1924. Cette association est une plateforme d'échange au niveau mondial réunissant des spécialistes de sciences pénales dont les domaines principaux sont les suivants: la politique criminelle et la codification du droit pénal, le droit pénal comparé, les droits de l'homme dans l'administration judiciaire pénale, la justice pénale internationale en droit pénal international.

[491]Résolutions des congrès de l'Association Internationale de Droit Pénal (1926-2004), nouvelles études pénales, association international de droit pénal (AIDP/IAPL), numéro 20, 2009

De plus, l'association pousse les Etats à modifier leurs lois nationales pour les délits déjà incriminés et de créer de nouveaux délits traitant des nouvelles infractions informatiques. Les nouveaux délits proposés sont les suivants: 1-les fraudes relatives à l'ordinateur[492] 2-les falsifications économiques[493],3-les dommages causés aux données ou programmes informatiques[494], 4- le sabotage d'ordinateur[495], 5- l'accès illégal à un système informatique ou à un ensemble de systèmes par violation des mesures de sécurité, 6- l'interception non autorisée[496], 7- la reproduction non autorisée d'un programme informatique protégé par la loi, 8- la reproduction non autorisée d'une topographie[497].

Le Conseil de l'Europe a aussi proposé une liste dite «optionnelle» pour des actes supplémentaires incriminables, énumérant les actes suivants: 1- l'altération de données ou de programmes informatiques, 2- l'espionnage informatique[498] 3- l'utilisation non autorisée d'un ordinateur[499].

De plus, les résolutions des Congrès de l'AIDP ont le mérite de faire également référence à d'autres abus à ne pas négliger dont : les trafics de mots de passe obtenus d'une façon illégale, ainsi que les distributions de virus…

[492]Toute insertion ou altération, un effacement ou suppression des données ou programmes informatiques, au déroulement du traitement des données informatiques causant une perte économique ou de possession mais aussi avec une intention de s'approprier un gain économique illégal à soi-même ou à autrui.

[493]Toute insertion, altération, effacement ou suppression de données ou programmes informatiques au déroulement de traitement de données informatiques, commis dans le cadre d'un délit de falsification.

[494]Tout effacement, endommagement, détérioration ou même suppression illégale de données ou de programmes informatiques.

[495]Toute insertion ou altération, effacement ou suppression de données ou de programmes informatiques avec une intention d'arrêter ou de bloquer le fonctionnement d'un ordinateur ou d'un système de télécommunication.

[496]Tout empêchement ou arrêt sans droit, d'un système informatique ou ensemble de systèmes, qui se trouve à l'intérieur d'un système informatique ou d'un ensemble de systèmes.

[497]Résolutions des congres de l'Association Internationale de Droit Pénal (1926-2004), nouvelles études pénales, association international de droit pénal (AIDP/IAPL), numéro 20, 2009.

[498]Toute acquisition par des moyens impropres , ou révélation ou utilisation d'un secret économique ou commercial sans droit avec une intention de causer une perte économique notamment à celui qui détient ce secret, et avec le but d'obtenir un avantage économique.

[499]Avec l'intention de causer une perte ou un dommage au système ou à son fonctionnement ou à la personne habilitée à utiliser le système ou à son fonctionnement

Tous ces délits préconisés par les résolutions de L'AIDP, ainsi que ceux faisant l'objet de la liste dite supplémentaire du Conseil de l'Europe, deviennent de plus en plus essentiels à intégrer dans les lois nationales à cause du progrès technologique et l'augmentation du chiffre des infractions informatiques[500].

L'AIDP rappelle que les sanctions pénales doivent être adéquates, définies clairement et limitées seulement aux actes intentionnels graves comme les actes comprenant les données informatiques sensibles ou des informations confidentielles protégées par les lois nationales.

L'AIDP s'est-elle même attardée sur l'utilité d'édicter des normes internationales renforçant la sécurité des systèmes informatiques. Elle a même mis à la disposition des autorités nationales, des mesures d'instruction et de poursuites adéquates : perquisition d'un ensemble de systèmes et la saisie de biens non corporels, tout en exigeant que le recours à ces mesures soit fait dans le respect des droits de l'homme.

En dernier lieu, l'AIDP invite les Etats à multiplier leurs recherches en ce qui concerne les délits de «technologie de l'information», à adopter de nouvelles techniques d'enquête et à mettre à la disposition de la police des outils de lutte efficaces pour faire face aux cyber-crimes.

A cet égard l'association propose d'assurer des programmes de formation mises à jour pour les enquêteurs, policiers, juges et avocats qui devraient tous devenir familiers aux détails techniques des cyber-crimes[501]. De même l'association recommande d'avoir recours à des experts bien formés, tel que les fournisseurs de service Internet ou compagnies de télécommunications, pour apporter assistance aux policiers.

[500]Résolutions des congres de l'Association Internationale de Droit Pénal (1926-2004), nouvelles études pénales, association international de droit pénal (AIDP/IAPL), numéro 20, 2009

[501]Les agents de police français, sont formés depuis 1983, par des stages de formation de plusieurs niveaux. Par contre les agents libanais manquent totalement de formation et d'expérience dans ce domaine. Le meilleur exemple à suivre serait celui des Etats-Unis, où les agents du FBI, sont formés à l'académie de Quantico en Virginie, pour faire face aux dangers des cyber-crimes (V.N. EL CHAER, op.cit.p.227).

D'autres groupes de travail et organismes internationaux se sont de leur côté intéresser à la cybercriminalité et ont émis des recommandations pertinentes à ce sujet (Paragraphe 2).

Paragraphe 2: Recommandations des groupes de travail et autres organismes

Un premier groupe de travail international «l'Anti-Phishing Work Group» a réussi à réunir de nombreuses entreprises, banques et organismes de sécurité dans l'intention de trouver des solutions contre l'hameçonnage[502]. Ce groupe a formulé des recommandations aidant les entreprises à mettre en œuvre en premier lieu des moyens pour informer leur clientèle des nouveaux dangers de l'informatique et de l'internet. Par la suite, il a prévu des mesures de sécurité internes[503] contre la cybercriminalité telle le système d'authentification par deux étapes ou le recours au protocole HTTPS[504].

Un second groupe de travail est celui de «l'Anti-phising Working group »[505] (l'Apwg)[506]. Ce groupe très actif s'est également intéressé aux escroqueries commises par hameçonnage. Il offre des forums de discussions et essaye de trouver des solutions potentielles pour faire face à la cybercriminalité, il établit même des rapports annuels pour mettre le point sur la situation mondiale de diffusion du «phising».

Dans le même but, l'organisation «Digital PhishNet», pousse à une coopération entre les entreprises mondialement renommées comme Microsoft, America online, Verisign et les agences gouvernementales comme le FBI, Secret Service et US Postal Inspection Service, tout ceci dans le but de combattre le «net phising»[507].

L'Interpol, en tant qu'organisation internationale intergouvernementales de police criminelle regroupant 179 pays et dont les bureaux se situent dans 186 pays

[502]D.SERRES et A.CLUZEAU, op.cit.
[503]C'est grâce au recours des banques brésiliennes à des mesures de sécurité interne tel que celles préconisées par l'anti phising work group que le Brésil possède désormais un des systèmes bancaires les plus sûrs mondialement (V. D.SERRES et A.CLUZEAU,op.cit.).
[504]Protocole de transfert hypertexte sécurisé
[505]Groupe crée au composé de représentants de cabinets d'avocats et d'entreprises, d'opérateurs d'internet, de banques et de fournisseurs de technologie.
[506]J. VAUGHAN, op.cit.p.7
[507]J.A.HITCHCOCK, op.cit. p. 380

membres, vise de son côté l'amélioration de la coopération policière au niveau mondial et travaille depuis plus de 15 ans dans le domaine de la criminalité informatique[508]. Pour arriver à ces finalités, l'Interpol tient fermement, depuis 2006, à l'instauration d'un système mondial d'alerte rapide[509]. En application de ce système, les organes policiers de l'Interpol collectent, rassemblent et analysent les informations concernant les délinquants et leurs victimes afin de mieux combattre toute variété de cybercriminalité possible et imaginable[510]. Le seul inconvénient à l'efficacité de l'Interpol réside dans le fait que cette organisation n'intervient malheureusement que suite à une demande présentée par les BCN[511][512].

Au niveau européen on trouve l'Europol basée à La Haye qui facilite à son tour les échanges entre les polices nationales de ses pays membres en matière de la criminalité et propose des échanges d'informations et d'expérience[513].

Il s'avère aussi nécessaire de recourir à l'idée des magistrats de liaison, permettant la création d'un cadre pour un échange de magistrats ou de fonctionnaires experts pour une meilleure coopération judiciaire entre plusieurs états[514]. Ce système de liaison s'avère intéressant pourra aider les états souffrant d'un manque de formation au niveau de leurs magistrats et de leurs enquêteurs, tel que le Liban. En application de ce système de liaison si un juge donné a besoin de recueillir des éléments de preuve il pourra s'adresser à un magistrat de liaison situé dans le pays concerné par la demande d'assistance, pour l'assister au niveau des procédures à suivre.

En ce qui concerne la coopération policière internationale des poursuites qui est elle aussi d'une nécessité absolue[515], c'est le G8[516], qui a invité les pays membres, depuis 1997, à l'adopter. Cette coordination devra englober une coordination des

[508] N. EL CHAER, op.cit. p. 219
[509] L'Interpol a mis en œuvre, en juin 2006, un système mondial d'alerte rapide fonctionnant 24 heures sur 24 et 7 jours sur 7 (V. M. HABHAB,op.cit.p.339)
[510] م، عبد الرؤوف ألحن ، مرجع سابق، ص ٢٣٩
[511]Bureau central national-Interpol
[512]Qui sont les intermédiaires entre les pays et le secrétariat général de l'Interpol.
[513] م. عبد الرؤوف ألحن ، مرجع سابق، ص ٢٤٠
[514]M. HABHAB, op.cit. p. 341.
[515]N. El CHAER, op.cit.,p. 314.
[516]Groupe G8 est le groupe des huit pays les plus industrialisés, ce groupe fait appel à une « *coordination internationale des poursuites* » (V.N. EL CHAER, op.cit.p.317).

activités, la formation des policiers, l'échange des informations opérationnelles et l'harmonisation des méthodes d'investigation, d'enquêtes et de poursuite[517]. Elle sera plus efficace, au cas où une convention internationale prévoirait un point de contact entre les pays pour l'échange d'informations et un organe de liaison pour faciliter les poursuites et enquêtes.

Un autre séminaire européen a eu lieu le 17 novembre 2001, pour lutter contre la cybercriminalité[518], il regroupait des cyber-policiers de 26 pays européens réunis dans le but de trouver des solutions pour améliorer les méthodes d'investigations et d'enquêtes, et permettre une grande coopération entre eux. Les Etats-Unis organisent de leur côté des programmes de formation pour cyber-policiers, pour mieux les former contre la délinquance informatique[519]. Il serait tant souhaitable que la France et d'autant plus le Liban songe à ce genre de solution.

Les recommandations et solutions proposées par le conseil européen de Lisbonne[520] réuni en mars 2000 afin d'harmoniser les législations de ses 15 pays membres n'est pas moins important à signaler. En effet, ce conseil vise à renforcer la sécurité des réseaux et doter les pays membres d'un cadre juridique identique. Il a mis en place des hotlines pour une meilleure lutte contre la cybercriminalité.

Les travaux du Conseil de l'Europe amènent de nouvelles solutions aux problèmes des cyber-crimes avec l'adoption le premier novembre 1985 d'une convention sur la protection des données personnelles à l'égard du traitement automatisé de données qui apporte des solutions précises et efficaces à ce propos[521].

Pour revenir à la convention européenne de Budapest sur la cybercriminalité de 2001[522]que nous avons étudier plus haut, elle invite les Etats à désigner un point de

[517]N.EL CHAER, op.cit.p.225.
[518] Séminaire intitulé «*Enquêtes de police judiciaire et nouvelles technologies de l'information et de la communication*» (V.N. EL CHAER, op.cit.p.318).
[519]Les Etats-Unis, coopèrent avec d'autres pays pour établir des Académies internationales de formation des forces de police (V.N.EL CHAER, op.cit.p.319).
[520]Le plan d'action est élaboré par la commission et le conseil et approuvé par le Conseil européen de Feira en juin 2000, prévoit le développement d'une approche coordonnée et cohérente de la délinquance informatique pour la fin 2002 (V.N. EL CHAER, op.cit.p. 324).
[521]La convention sur la cybercriminalité et le droit pénal congolais, Christophe KaweKasongo, université de Kinshasa RDC- licence en droit, 2003.
[522]Convention ouverte non pas seulement aux pays membres de l'union européenne, mais à tous les Etats qui ont participé à son élaboration: Afrique du sud, le Canada, les Etats Unis

contact valable et opérant 24 heures sur 24 sept jours sur sept, dans le but de prêter l'aide et l'assistance immédiate et rapide aux internautes[523]. Ce point de contact a vocation à succès à condition que ses membres soient bien formés en matière de criminalité informatique mais aussi qu'ils soient bien équipés[524]. Cette même convention a également consacré, à son deuxième chapitre, les mesures à prendre au niveau national, elle a fixé une norme commune déterminante les infractions pénales tenant en compte les nouvelles infractions et actes illicites qui ont vu le jour avec le progrès des moyens de télécommunications.

La convention a aussi pour but d'améliorer les procédures pénales elle exige, comme nous l'avons déjà mentionné plus haut, l'entraide la plus large possible et impose une rapidité dans la collecte des preuves électroniques et de la conservation des données de trafic qui ont trait à une communication passant par un système informatique avec indication d'informations telles l'origine, la destination, l'heure, la date ou la durée de communication des données électroniques[525].

En définitive les priorités sont les suivantes: 1-saisir ou obtenir d'une façon similaire un système informatique ou un support de stockage informatique, 2-conserver une copie des données informatiques, 3- préserver l'intégrité de ces données.

Nous déduisons de tout ce qui précède qu'il parait indispensable de recourir à une coopération internationale et effective en adoptant des instruments juridiques internationaux adéquats et en suivant les résolutions et recommandations émises par ces instruments.

---

d'Amérique et le Japon. L'adhésion des Etats non membres et même ceux n'ayant pas participé à son élaboration est possible à condition qu'ils consacrent des principes démocratiques au niveau institutionnel. Le Liban peut à ce titre adhérer à cette convention sur la protection des données personnelles, elle pourra lui servir de loi de base pour lutter contre la cybercriminalité, vu que la cour de cassation libanaise a consacré le respect des obligations internationales, et selon commandant El-Hajj, la procédure d'adhésion du Liban à cette convention est en cours.

[523]N.EL CHAER, op.cit.p.349

[524]La convention sur la cybercriminalité et le droit pénal congolais, Christophe KaweKasongo, université de Kinshasa RDC- licence en droit, 2003.

[525]N. EL CHAER, op.cit.p.343-344

CONCLUSION

Partant de la définition classique de l'escroquerie qui figure aux articles 313-1 à 3 CPF et aux articles 655-656 CPL nous avons pu constater, en nous attardant sur les moyens frauduleux classiques, que les deux droits français et libanais se ressemblent au niveau de l'escroquerie classique. En effet, les deux droits énumèrent presque les mêmes moyens frauduleux tout en insistant sur la notion d'intention frauduleuse et sur l'importance du moment de la remise. Nous avons relevé un seul point de divergence entre les deux droits: la notion d'abus de qualité vraie qui existe en droit français mais qu'on ne retrouve pas en droit libanais.

Par la suite nous nous sommes arrêtés dans le second chapitre de notre première partie sur les sanctions de l'escroquerie dite classique et ses moyens de répression dans les deux droits français et libanais. Et c'est partant de la constatation que ces deux droits incriminent tout deux l'escroquerie ayant pour but la remise d'une information lorsque cette information se trouve sur un support matériel, que nous nous sommes posé la question de savoir si l'information électronique, et de façon plus générale, tous les délits entrant dans la cybercriminalité peuvent-ils faire l'objet d'une escroquerie? Sur la base de quelles lois doivent-ils être incriminés? Sur la base des lois incriminant les délits d'escroquerie dite classique ou sur la base de lois spéciales qui leur sont adaptées? D'où l'idée derrière notre seconde partie dans laquelle nous avons longuement traité du sujet des nouvelles méthodes d'escroquerie, qui s'effectuent le plus par le recours à l'Internet vu que le monde matériel «cohabite» désormais de plus en plus avec le monde virtuel.

C'est ainsi qu'au fil du premier chapitre de la seconde partie nous avons présenté les formes de cyber-escroqueries les plus pratiquées à savoir l'hameçonnage (phishing), l'escroquerie à la nigériane, les loteries frauduleuses, les escroqueries liées aux dépôts/titres bancaires mais également celles relatives aux cartes bancaires et à la «fraude au président».

Nous avons relevé par la suite, sous le second chapitre de la seconde partie, que la France a eu recours depuis plus de dix ans à plusieurs lois spéciales plus ou moins

adaptées aux nouvelles formes d'escroquerie. La grande force de la France s'est révélé être la spécialisation et l'expérience de ses enquêteurs et policiers qui assistent de façon permanente à des forums afin d'élargir leurs connaissances et de fortifier leur formation. Une autre constatation que nous avons faite est l'existence de plusieurs organismes français de lutte contre la cybercriminalité.

Malgré ces efforts considérables, la France doit continuer à adapter ces textes et légiférer de nouvelles lois spéciales pour pouvoir réprimer toutes les nouvelles sortes d'infractions informatiques existantes et à venir.

Nous nous sommes rendu compte qu'une multitude de pays européens, versent eux même annuellement des milliards d'euros pour moderniser les lois spéciales concernant le commerce électronique et les fraudes informatiques se multipliant chaque année sur leurs territoires.

Comme nous l'avons signalé les Etats-Unis ont complètement mis à jour leurs lois pénales. Leur législation est l'une des plus achevée et des plus adaptée aux nouvelles cyberattaques[526]. Il en est de même pour l'Australie, l'Inde, le Japon et la Turquie…qui luttent de façon effective contre la criminalité informatique.

Nous avons pu constater enfin qu'au niveau des pays arabes la position adoptée face à la lutte contre la cybercriminalité varient selon les pays. Certains pays arabes, tel que l'Egypte en 1992, la Tunisie en 2000, la Jordanie en 2001, la Syrie en 2012, Dubaï, ont déjà adopté une loi protégeant la vie privée de la délinquance informatique. Tandis que d'autres pays comme le Liban, sont encore très loin de cette évolution législative.

Le Liban n'a légiféré aucune nouvelle loi spécifique concernant les maintes variétés d'escroqueries informatiques ce qui est fort regrettable. Il n'a même pas songé à adapter ses lois existantes pour faire face à la montée en pic du phénomène de cybercriminalité, tout ceci malgré le fait que chaque jour, des libanais sont victimes de ces cyber-crimes. Face à ce constat les juges libanais se trouvent

[526]Les Etats unis étaient le second pays après la Suède à légiférer dès 1997 une disposition contre la fraude informatique en adoptant des lois la réprimant : «Conterfeit Access Device» et «Computer Fraud and Abuse Act» sanctionnant l'accès non autorisé à un système informatique et l'utilisation et manipulation des données. Cela fût complété par une multitude de lois spéciales dont le «Computer Fraud and Abuse Act» de 1986.

devant une impasse et ne peuvent qu'appliquer les textes traditionnels inadaptés sous peine de déni de justice.

En outre, nous avons bien mis en relief les autres points de faiblesse du droit libanais. Ces faiblesses se révèlent notamment au niveau de la procédure pénale et au niveau de la formation des magistrats libanais. Le manque d'organismes de lutte contre les crimes informatiques est lui aussi flagrant, on ne trouve actuellement qu'un seul organisme libanais spécialisé qui est *«le bureau de lutte contre les délits informatiques*». Ce bureau, est conscient de la difficulté de localisation et de poursuite des escrocs sur le territoire libanais et affirme clairement que cela est dû au manque de policiers/enquêteurs bien formés, d'équipements et de matériels adéquats.

Le Liban ne doit pas rester muet face à la montée en puissance des nouvelles infractions liées à l'informatique, une réforme doit impérativement intervenir le plus tôt possible pour que ce pays ne devienne pas l'un des «paradis de la cybercriminalité». Le législateur Libanais devra redoubler d'efforts afin d'adopter de nouvelles lois spécifiques et adapter ces textes traditionnels concernant la procédure pénale. Pour y arriver, il pourra tout simplement s'inspirer des lois françaises spéciales et en suivre le modèle comme il l'a toujours fait. Sinon il serait grand temps pour le législateur libanais d'adopter l'un des projets de loi proposé par des spécialistes libanais de droit et dont un est annexé au présent mémoire. Le Liban a même la possibilité de s'inspirer de la convention de 2001 de Budapest à ce sujet, vu qu'il a déjà présenté sa candidature à cette convention et la procédure est en cours.

Une fois que le législateur libanais adoptera des lois spéciales en se référant à l'une des solutions que nous venons de proposer, le Liban devra aussi ratifier des conventions internationales afin de renforcer la lutte contre les infractions informatiques qui ne connaissent ni de limites ni de frontières. Et c'est petit à petit qu'il devra enfin songer à mieux former ses enquêteurs, policiers et magistrats par l'intensification et la multiplication des stages de formation, forums, congrès, colloques… tout ceci en assurant simultanément des équipements et moyens de lutte, de poursuite et de localisation adéquats et efficaces.

Les efforts à poursuivre dans les pays européens et les nouvelles résolutions que doit prendre le plus tôt le Liban se justifient pleinement avec l'apparition fulgurante de la «*rançongiciel*» ou «*ransomware*», cyberattaque sui generis qui allie les techniques astucieuses d'escroquerie à celles du chantage de grande envergure.

Redoutable, furtive et difficilement tractable l'attaque rançongicielle *«reléguerait presque les holdup et autres braquages»*[527]. Cette cyberattaque est un type de logiciel malveillant qui empêche une personne d'accéder à un ordinateur, un téléphone portable, ou des données personnelles en les verrouillant et en chiffrant le système et les fichiers numériques qu'il contient[528]. La principale motivation des hackers de rançongiciel est l'appât d'un gain considérable.

Ces virus informatiques assez sophistiqués se propagent souvent par des pièces jointes dans des courriels électroniques, des liens venant de réseaux sociaux, des sites piratés ou encore des publicités donc le contenu renvoi a un site malveillant qui teste les vulnérabilités de l'ordinateur[529].

L'utilisateur apprend, en voyant s'afficher sur son ordinateur un message à entête pseudo-officielle de gendarmerie ou de police, que son ordinateur est verrouillé pour avoir soi-disant enfreint la loi. Il y aura lieu de régler immédiatement une amende/rançon afin de déverrouiller l'ordinateur et permettre à l'utilisateur d'accéder de nouveau à ses fichiers[530]. Dans la majorité des cas, l'utilisateur se verra accorder entre 24 à 72 heures pour payer la rançon sous peine que la clé privée ne soit détruite et que les fichiers ne soient perdus à jamais.

Cette cyberattaque d'un *«niveau sans précédent»* et qui *«prend des données en otage»*[531] a frappé une centaine de pays, affectant le même jour 12 mai 2017 le fonctionnement de nombreuses entreprises et organisations internationales aux Etat

[527]Ch. CORVENIEN, *«le «rançongiciel», dernière arme fatale du crime organisé»*, art. publié le 27/1/2013, Le Figaro, www.lefigaro.fr.
[528]L. RONFAUT, *«comment se protéger et réagir face à un rançongiciel?»*, art. publié le 28/6/2017, Le Figaro, www.lefigaro.fr.
[529]E. FREYSSINET, *«investigations & transformations numériques»*, www.ericfreyssi.net.
[530]M. LARDEUX, *«une arnaque en progression dite «rançongiciel»»*, art publié le 11/2/2014, le journal d'information de l'ile de Ré, www.realahune.fr.
[531]J. TOUSSAY, *««Ransomware» ou «rançongiciel», un logiciel malveillant qui prend vos données en otage»*, art. publié le 13/5/2017, le Huffington Post, www.huffingtonpost.fr.

Unis, en France, en Allemagne, en Belgique, en Italie, en Russie, en Ukraine, à Taiwan, au Mexique… dont les entreprises espagnoles Telefonica et Gas Natural, le constructeur français Renault, les hôpitaux britanniques, le géant de livraison de colis Fedex, les systèmes Windows....[532]. Selon une étude de Google[533] les rançongiciels de portée mondiale, spécialement de type «*Wanna Cry*», ont ainsi extorqué aux entreprises mondiales plus de 25 millions de dollars entre 2016 et 2017[534].

Face à la brusque accélération des cyberattaques, phénomène qui n'est pas prêt de s'arrêter conséquence d'un monde de plus en plus connecté, mieux vaut tard que jamais, la Commission Européenne va faire voter en 2018 un *«paquet cyber»*. Ce *«paquet cyber»* est un ensemble de mesures de lutte contre les toutes nouvelles cyberattaques y compris les rançongiciels contre lesquels ,l'Europe, le Liban et plusieurs autres Etats restent *«mal équipés»*[535].

Le paquet en question sera axé sur le renforcement de la *«détection, la traçabilité et la poursuite des cybercriminels devant les tribunaux»* par exemple via *«un renforcement du partage d'informations entre centre de cyber sécurité»*, la création *«d'une plateforme de liens entre agences européennes et internationales (comme L'Interpol)»* et la coordination du *«financement de la recherche technologique»*[536].

Les mesures de ce «paquet cyber» réprimant le rançongiciel et plusieurs autres délits à venir mériteraient, sans conteste, une étude séparée non moins intéressante que celle du présent mémoire.

---

[532]*«Une attaque informatique de portée mondiale crée la panique»*, art. publié le 12/5/2017, Le Monde, www.lemonde.fr; *«Attaque informatique de portée mondiale»*, art. publié le 13/5/2017, Le Figaro, www.lefigaro.fr.

[533]Etude commune entre Google, l'entreprise spécialisée dans le bitcoin Chainalysis et les Universités UC San Diego et NYU Tandon School of Engineering dont les résultats ont été présentés au Black Hat, l'une des plus grandes conférences sur la sécurité informatique aux Etats unis qui s'est tenu du 25 au 27 juillet 2017 à Las Vegas.

[534]*«Les rançongiciels ont extorqué plus de 25 millions de dollars, conclut une étude de Google»,* art publié le 27/7/2017, Le monde, www.mobile.lemonde.fr.

[535]S. ROLLAND, *«Cyberattaques: que contient le "paquet cyber" que l'Europe veut voter en 2018?»*, art publié le 20/9/2017, La Tribune, www.latribune.fr.

[536]Idem.

Sur ce, nous concluons notre mémoire à travers l'observation judicieuse, raisonnable et loin d'être utopique de la commission européenne selon laquelle le souci premier et dernier de tout pays, y compris à notre sens celui de la France et du Liban, doit être celui de faire en sorte que les lois spéciales et moyens de lutte du paquet cyber *«restent à un niveau assez avancé que les armes déployées par les cybercriminels»*[537].

[537]S. ROLLAND, *«Cyberattaques: que contient le "paquet cyber" que l'Europe veut voter en 2018?»*, art publié le 20/9/2017, La Tribune, www.latribune.fr.

ANNEXE:

PROPOSITION DE LOI PAR ECOMLEB[538]

TITRE VI- De diverses infractions liées au commerce électronique

Présentation des textes

Le commerce électronique, l'informatique et les nouvelles technologies de l'information se développent et prennent une place croissante dans la vie économique et la vie quotidienne. Les réseaux et les systèmes d'information sont de plus en plus interconnectés. Cette évolution comporte de nombreux avantages, mais fait apparaître de nouveaux types de délinquance. Les attaques intentionnelles contre les systèmes informatiques font partie de ces nouveaux risques.

Or, la loi pénale libanaise ne prend pas en compte la technologie informatique comme un moyen susceptible de porter atteinte aux biens ni les menaces d'attaques contre les systèmes informatiques. Compte tenu des principes de légalité des crimes et délits et d'interprétation stricte de la loi pénale, les incriminations existantes du droit pénal ne sont pas toujours suffisantes.

Le 23 novembre 2001, le Conseil de l'Europe a adopté à Budapest une convention sur la cybercriminalité. Cette dernière constitue la première convention pénale à vocation universelle destinée à lutter contre le cyber-crime.

La Convention préconise de prendre des mesures législatives en vue d'ériger en infraction pénales les actes suivants : – accès illégal à tout ou partie d'un système informatique ; – interception illégale de transmissions non publiques ; – atteinte à l'intégrité des données ; – atteinte à l'intégrité d'un système ; – abus de dispositif ; – falsification informatique ; – fraude informatique (préjudice patrimonial causé à autrui).

[538]Un avant-projet d'une loi sur la communication, l'Ecriture et les Transactions Electroniques, de Mai 2005, du Ministère de l'Economie et du Commerce , www.economy.gov.lb

Concernant les interceptions illégales, la loi libanaise n° 140 du 27/10/1999 relative à la protection du droit au secret des communications effectuées par tous moyens de communication prévoit que toute interception effectuée contrairement aux dispositions de la loi est incriminée pénalement. Il n'est donc pas nécessaire de créer un nouveau délit d'interception illégale. La falsification informatique fait référence au faux électronique, traitée ci-après au chapitre 5. Le délit d'escroquerie est défini et réprimé à l'article 655 du code pénal. La question se pose de savoir si ce texte peut s'appliquer aussi aux agissements à finalité frauduleuse qui passent par l'emploi de la technique informatique. La manipulation de données par des escrocs adeptes de l'informatique, l'utilisation d'un ordinateur en amont de la remise constituent des manœuvres frauduleuses au sens de ces dispositions. L'article 655 du code pénal ne nécessite pas d'être modifié pour être adapté à l'escroquerie commise via l'emploi de l'informatique.

En revanche, la loi pénale libanaise doit protéger les systèmes informatiques contre les atteintes illégitimes, à l'instar de nombreux autres pays.

Le présent Titre a donc pour objectif d'adapter le droit pénal libanais au développement des nouvelles technologies.

Les dispositions proposées s'articulent en 5 chapitres.

L'informatique peut être le vecteur de fraudes en tout genre. Or, il n'existe pas en droit libanais d'incrimination relative à la fraude informatique, ce qui permet à la délinquance informatique de se développer au Liban en toute impunité. Le chapitre 1 crée les incriminations relatives aux atteintes aux systèmes informatiques en général, qu'ils soient ou non reliés à un réseau.

Le développement de l'utilisation des cartes de paiement en raison de la diversité des services et des facilités de paiement qu'elles offrent, notamment dans le cadre du commerce électronique, s'est accompagné corrélativement de l'apparition de nouveaux types de fraude. De nombreuses fraudes à la carte bancaire peuvent être poursuivies au travers des infractions traditionnelles contre le patrimoine (vol, escroquerie, abus de confiance). Il ne paraît donc pas nécessaire de créer de nouvelles incriminations visant spécifiquement l'escroquerie ou l'abus de confiance commis au moyen d'une carte bancaire. Il n'existe pas en revanche de texte relatif à la contrefaçon de cartes de paiement. Compte tenu de la gravité de tels

agissements, il est proposé de créer une incrimination de contrefaçon de cartes de paiement ou de retrait. C'est l'objet du chapitre 2 du Titre VI.

Le Titre V de l'avant-projet relatif au commerce électronique et aux contrats commerciaux électroniques comporte des interdictions et obligations en matière de démarchage et de promotion non sollicités. Le chapitre 3 crée les sanctions pénales afférentes à ces interdictions et obligations.

Le chapitre 4 a pour objet d'adapter l'article 209 du code pénal sur la publication afin qu'il couvre également la publication via les services de communication en ligne.

Le chapitre 5 a pour objet d'adapter l'incrimination du faux en écritures au faux électronique, corollaire de la création de l'écrit électronique.

Chapitre 1 – Des atteintes aux systèmes informatiques

La liste des modifications à apporter au droit pénal libanais pour y introduire les incriminations relatives aux intrusions et « destructions » commises au préjudice des systèmes informatiques a été établie au regard de la Convention de Budapest du 23 novembre 2001 et en raison des silences du droit positif libanais en la matière. Il est proposé d'ériger en infraction pénale les actes d'accès illégal à tout ou partie d'un système informatique, d'atteinte à l'intégrité des données ou d'un système et l'abus de dispositif.

Le Titre XI du Livre II du code pénal étant relatif aux infractions contre le patrimoine, il proposé d'insérer les dispositions relatives à la fraude informatique dans ce titre, sous la forme d'un chapitre nouveau. L'article 1er du chapitre 1 définit la notion de système informatique.

Le terme de système informatique est proposé pour désigner des dispositifs assurant le traitement de données au sens large, connectés ou non, objets d'une attaque. La définition proposée est inspirée de l'article 1 a) de la Convention sur la cybercriminalité. Elle est complétée par une liste non limitative d'exemples de systèmes informatiques.

L'article 2 du chapitre 1 vise l'accès illégal à tout ou partie d'un système informatique.

La rédaction est inspirée de l'article 323-1 du code pénal français. L'incrimination englobe tous les modes de pénétration irréguliers dans un système informatique. Sont concernés tous les accès non autorisés dans les ordinateurs d'autrui, que ce soit par malveillance, par défi, ou par jeu, que l'accès sans droit s'effectue directement sur la machine visée ou à distance. L'accès tombe sous le coup de la loi pénale dès lors qu'il est le fait d'une personne qui n'a pas le droit d'accéder au système ou n'a pas le droit d'y accéder de la manière qu'elle a employée. Lorsque l'accès a été régulier, le maintien sur un système automatisé de données peut devenir frauduleux, lorsque, par une sorte d'interversion de titre, l'auteur du maintien se trouve privé de toute habilitation (jurisprudence de la Cour d'appel de Paris - CA Paris, 11ème Ch., 5 avril 1994, Jurisdata n° 1994-021093 -). Une personne qui se serait immiscée par erreur dans un système mais s'y serait maintenue de manière consciente rentre ainsi dans le cadre de l'incrimination. L'intrusion sans droit dans un système informatique est incriminable sans considération des conséquences qu'elle peut avoir. L'alinéa 2 créé une circonstance aggravante lorsqu'il en est résulté la suppression ou la modification de données ou programmes, ou l'altération du fonctionnement du système informatique.

L'article 3 du chapitre 1 vise l'atteinte à l'intégrité du système.

Il est inspiré de l'article 323-2 du code pénal français. Il existe différents moyens par lesquels on peut perturber le fonctionnement d'un système informatique, par exemple : – par introduction de données (ex. : par introduction de virus - programmes informatiques capables de se reproduire qui peuvent être conçus pour effacer ou altérer les données des systèmes dans lesquels ils ont été introduits -) ; – par effacement ou modification des données ; – par l'envoi de nombreuses requêtes sur un même serveur en vue d'empêcher son fonctionnement normal (attaque visant à saturer le serveur, dite attaque par déni de service). Les termes « par tout moyen » permettent d'englober les différentes méthodes, actuelles ou futures.

L'article 4 du chapitre 1 vise l'atteinte à l'intégrité des données.

Il est inspiré de l'article 323-3 du code pénal français. Le texte sanctionne les altérations volontaires de données, ainsi que les manipulations d'informations, l'introduction volontaire de données erronées dans un fichier, la modification ou la

suppression malveillantes de données sans qu'il ne soit porté atteinte au système informatique lui- même.

L'article 5 incrimine l'abus de dispositif. Il est inspiré de l'article 323-3-1 du code pénal français. L'incrimination de l'abus de dispositif permet de poursuivre ceux qui fournissent les outils servant à commettre les attaques informatiques. Elle vise à ériger la fourniture de moyens en infraction autonome. En matière de sécurité informatique, les mêmes outils peuvent être utilisés à des fins malveillantes ou à des fins légitimes, en vue de tester la sécurité des systèmes d'information ou pour des activités de recherche. Les outils d'analyse de la sécurité peuvent parfois servir à commettre une attaque. On peut également citer les activités de recherche. Il faut donc pouvoir distinguer les cas où les outils sont utilisés pour des motifs légitimes, des cas où ils ne sont conçus qu'à des fins malveillantes. Par ailleurs, en droit libanais, il existe des dispositions spécifiques sur la complicité, avec lesquelles l'incrimination ne doit pas faire double emploi ou créer des confusions, le complice étant moins puni que l'auteur principal. La rédaction proposée tient compte de ces deux impératifs.

L'incrimination englobe la fourniture frauduleuse de mots de passe pour accéder à des systèmes informatiques. L'utilisation des termes « dispositif, toute donnée » fait référence à cette fraude.

L'article 6 prévoit la répression de la tentative, l'article 202 du code pénal déclarant que la tentative d'un délit n'est punissable que dans les cas déterminés par une disposition spéciale de la loi.

Chapitre 2 – De la contrefaçon des cartes de paiement ou de retrait

Le chapitre 1 ci-dessus couvre les atteintes aux systèmes informatiques de données relatives aux cartes bancaires. En revanche, une incrimination spécifique est nécessaire pour couvrir les actes de falsification et de contrefaçon de cartes bancaires. Le terme de « cartes de paiement ou de retrait » englobe tous les types de cartes émises par les banques ou toute autre institution admise à en délivrer. Cette terminologie est celle employée dans la partie du Titre V de l'avant-projet de loi relative aux transferts de fonds électroniques.

Il est également proposé d'insérer les dispositions relatives à la contrefaçon des cartes de paiement et de retrait dans le Titre XI du Livre II du code pénal relatif aux infractions contre le patrimoine.

L'article 1 du chapitre 2 incrimine la contrefaçon et la falsification d'une carte de paiement ou de retrait, la mise en circulation ou l'utilisation d'une carte contrefaite ou falsifiée, et l'acceptation d'un paiement au moyen d'une carte contrefaite ou falsifiée. Il est inspiré de l'article L 163-4 du code monétaire et financier français.

L'article 2 du chapitre 2 incrimine la fourniture au sens large ou la détention d'outils ou de données destinés à permettre la contrefaçon ou la falsification de cartes de paiement ou de retrait. Il est inspiré de l'article L 163-4-1 du code monétaire et financier français. La rédaction de l'incrimination est plus large que pour les abus de dispositif, car l'exception de « motif légitime » ne s'applique pas pour les outils servant à fabriquer de fausses cartes de paiement ou de retrait.

L'article 3 prévoit la répression de la tentative.

Il n'est pas apparu nécessaire de proposer des dispositions relatives à la confiscation des cartes contrefaites ou des moyens ayant servi ou destinés à commettre les délits visés, dans la mesure où il existe déjà des dispositions sur la confiscation aux articles 42, 69 et 98 du code pénal.

Chapitre 3 – De l'inobservation des règles applicables au commerce électronique

Le chapitre 1 du Titre V de l'avant-projet relatif au commerce électronique et aux contrats commerciaux conclus par voie électronique propose l'insertion dans le Titre IV du code de commerce de deux articles rédigés comme suit :

« Art. 41-1 Sont interdits le démarchage et la promotion non sollicités qui, par quelque moyen que ce soit, utilisent les coordonnées d’une personne physique si celle-ci n’a pas exprimé son consentement préalable à une telle forme de publicité.

Il est fait exception à ce principe lorsque l’auteur du message non sollicité s’adresse à un client dont il a obtenu régulièrement l’adresse à l’occasion d’une transaction antérieure.

Art. 41-2 Tout message de démarchage ou de promotion non sollicité doit clairement indiquer à son destinataire l'adresse à laquelle il pourra transmettre une demande exigeant péremptoirement que ces communications cessent, sans autre frais que ceux liés à l'envoi de son refus. »

Afin d'assurer l'effectivité de ces dispositions, il est prévu de sanctionner leur non-respect par une peine d'amende. Il est proposé d'insérer ces sanctions dans le Titre XII du Livre II du code pénal relatif aux contraventions, en ajoutant un chapitre VII intitulé : « De l'inobservation des règles applicables au commerce électronique.»

Chapitre 4 – De la publication électronique

L'article 209 du code pénal définit ce qui est considéré comme moyen de publication. L'alinéa 1er vise les actes et gestes ayant lieu dans un endroit public, l'alinéa 2 les paroles ou cris, et l'alinéa 3 « Les écrits, dessins, peintures, photographies, films, emblèmes, ou images quelconques s'ils ont été exposés dans un lieu public, ouvert ou exposé au public, ou s'ils ont été vendus ou mis en vente ou distribués à une ou plusieurs personnes. »

Les nouveaux réseaux de communication comme internet sont incontestablement des moyens de publication modernes, mais ne sont pas visés par l'article 209 : internet ne constitue pas à proprement parler un « lieu » et les notions de vente ou de distribution visent des supports traditionnels et non électroniques. Il existe par ailleurs plusieurs articles du code pénal qui font référence à l'article 209 : – 214 : relatif à la participation criminelle de l'auteur, – 319 : relatif aux atteintes au crédit de l'Etat, – 384 : relatif à l'outrage, – 386 : relatif à la diffamation, – 388 : relatif à l'injure, – 474 : relatif à l'atteinte aux sentiments religieux, – 526 : relatif au racolage public en vue de la prostitution, – 531, 532 : relatifs aux outrages à la pudeur publique et aux bonnes mœurs, – 539 : relatif à la propagande de l'usage de pratiques abortives, – 578 : relatif à la menace de commettre un dommage injuste, – 582, 584 : relatifs à la diffamation et à l'injure.

Pour que l'article 209 couvre la publication sur les réseaux sans toucher à l'équilibre du code pénal, il est proposé de modifier l'alinéa 3 pour viser explicitement tous les moyens de publication, y compris le moyen électronique.

Chapitre 5 – Du faux électronique

L'article 453 du code pénal incrimine la falsification de documents écrits. Le projet de loi relative aux écrits électroniques en général et à leur sécurisation introduit en son article 5 le principe d'équivalence entre l'écrit et la signature sous forme électronique et les écrits et signatures figurant sur un autre support. Le faux en écriture électronique doit être punissable au même titre que le faux en écriture sur un support papier. C'est pourquoi il est proposé de modifier l'article 453 du code pénal afin qu'il vise explicitement le faux d'un écrit électronique, compte tenu du principe d'interprétation stricte du droit pénal. La rédaction reprend celle proposée par la commission de réforme du droit pénal, en y ajoutant les mots : « y compris électronique » par cohérence avec la nouvelle rédaction proposée pour l'article 209 du code pénal.

Contenu des textes

Chapitre 1 – Des atteintes aux systèmes informatiques

Article 1 Le Titre XI du Livre deuxième du code pénal comporte un Chapitre (à préciser par le législateur) intitulé: « Des atteintes aux systèmes informatiques ».

Article 2 Le Chapitre (à préciser par le législateur) du Titre XI du Livre deuxième du code pénal comporte les articles 1 à 6 ci-après :

Article 1 Au sens du présent chapitre, un système informatique s'entend d'un dispositif quelconque assurant le traitement électronique de données, fonctionnant de façon isolée ou connecté à d'autres dispositifs. Sont notamment considérés comme un système informatique : un ordinateur, un réseau d'ordinateurs, un serveur, un site internet, un extranet, un intranet, un système de traitement électronique de données relatives aux cartes bancaires, un téléphone mobile.

Article 2 Quiconque, dans une intention frauduleuse, accède ou se maintient dans tout ou partie d'un système informatique, sera puni d'un emprisonnement de deux

mois à un an et/ou d'une amende de 1 000 000 à 20000 000 de livres libanaises. S'il résulte de cet acte soit la suppression de données numériques ou programmes informatiques, soit leur modification, soit une altération du fonctionnement du système informatique, la peine sera de six mois à deux ans d'emprisonnement et/ou d'une amende de 2 000 000 à 40 000 000 de livres libanaises.

Article 3 Quiconque, dans une intention frauduleuse, entrave ou perturbe (fausse), par tout moyen, le fonctionnement d'un système informatique sera puni d'un emprisonnement de six mois à trois ans et/ou d'une amende de 3 000 000 à 60 000 000 de livres libanaises.

Article 4 Quiconque, dans une intention frauduleuse, supprime ou modifie, par tout moyen, les données numériques ou programmes d'un système informatique sera puni d'un emprisonnement de six mois à trois ans et/ou d'une amende de 3 000 000 à 60 000 000 de livres libanaises.

Article 5 Quiconque produit, détient, diffuse ou met à disposition un dispositif, programme informatique ou toute donnée conçus ou adaptés à seule fin de permettre la commission de l'une des infractions prévue dans les articles précédents sera puni d'un emprisonnement de six mois à trois ans et/ou d'une amende de 3 000 000 à 60 000 000 de livres libanaises.

Article 6 La tentative des infractions prévues dans ce chapitre est punissable.

Chapitre 2 – De la contrefaçon des cartes de paiement et de retrait

Article 3 Le Titre XI du Livre deuxième du code pénal comporte un Chapitre (à préciser par le législateur) intitulé : « De la contrefaçon des cartes de paiement et de retrait ».

Article 4 Le Chapitre (à préciser par le législateur) du Titre XI du Livre deuxième du code pénal comprend les articles 1 à 3 à ci-après :

Article 1 Sera puni d'une peine d'emprisonnement de six mois à trois ans et/ou d'une amende de 10 000 000 à 60 000 000 de livres libanaises :

1°- Quiconque contrefait ou falsifie une carte de paiement ou de retrait ; 2°- Quiconque met en circulation ou use, en connaissance de cause, d'une carte de paiement ou de retrait contrefaite ou falsifiée ; 3°- Quiconque accepte, en

connaissance de cause, de recevoir un paiement au moyen d'une carte de paiement ou de retrait falsifiée.

Article 2 Sera puni d'une peine d'emprisonnement de six mois à deux ans et/ou d'une amende de 2 000 000 à 20 000 000 de livres libanaises quiconque produit, détient, diffuse ou met à disposition un dispositif, programme informatique ou toute donnée spécialement conçus ou adaptés pour permettre la commission de l'une des infractions prévue par l'article précédent.

Article 3 La tentative des infractions prévues dans ce chapitre est punissable.

Chapitre 3 - De l'inobservation des règles applicables au commerce électronique

Article 5 Il est créé au Titre XII du Livre deuxième du code pénal un Chapitre VIII intitulé : « De l'inobservation des règles applicables au commerce électronique ».

Article 6 Le Chapitre VIII du Titre XII du Livre deuxième du code pénal comprend les articles 770-1 à 770-2 ci-après :

Article 770-1 Quiconque contrevient aux interdictions édictées par le Titre IV du code de commerce en matière de démarchage et de promotion non sollicités sera puni d'une amende de 30 000 000 à 50 000 000 de livres libanaises.

Article 770-2 Quiconque contrevient aux obligations imposées par le Titre IV du code de commerce à toute personne émettant un message de démarchage ou de promotion non sollicité sera puni d'une amende de 15 000 000 à 30 000 000 de livres libanaises.

Chapitre 4 – De la publication électronique

Article 7 L'alinéa 3° de l'article 209 du code pénal est modifié comme suit : 3°- Les écrits, dessins, peintures, photographies, films, emblèmes, ou images quelconques s'ils ont été exposés dans un lieu public, ouvert ou exposé au public, ou s'ils ont été vendus ou mis en vente ou distribués à une ou plusieurs personnes, quel que soit le moyen de la publication, y compris (le moyen) électronique.

Chapitre 5 – Du faux électronique

Article 8 L'article 453 du code pénal est modifié comme suit :

Le faux en écritures est l'altération frauduleuse de la vérité dans les faits ou énonciations qu'un acte, un écrit ou tout autre support d'expression, y compris électronique, formant titre a pour objet de constater et dont peut résulter un préjudice soit matériel, soit moral ou social.

RÉFÉRENCES BIBLIOGRAPHIQUE

I- OUVRAGES GÉNÉRAUX

1) OUVRAGES GENEAUX DE DROIT FRANÇAIS

1. **CONTE Ph.**, *«Droit pénal spécial»*, Manuels, 2ème éd., Lexis Nexis, 2005.

2. **GATTEGNO P.**, «*Droit pénal spécial, cours de droit privé*», éd. Dalloz 1995.

3. **LARGUIER J. et CONTE Ph.**, «*Droit pénal des affaires*», 10ème éd., Armand Collin, Paris, 2001.

4. **LARGUIER J. et LARGUIER A-M.**, «*Droit pénal spécial*», Mémentos droit privé, 9ème éd. Dalloz, Paris, 1996.

5. **LUCAS DE LEYSSAC M-P. et MIHMAN A.**, «*Droit Pénal des Affaires*», Manuel théorique et pratique, éd. Economica 2009.

6. **PRADEL J. et DANTI-JUAN M.**, «*Droit pénal spécial, droit commun-droit des affaires*», 4ème éd., Cujas 2007/2008.

7. **PRADEL J.**, «*Droit pénal comparé*», Précis Dalloz 3ème édition 2008

8. **RASSAT M-L.**, «*Droit pénal spécial, Les infractions des et contre les particuliers*», précis Dalloz, 5ème éd. Delta, Paris, 2006.

9. **VERON M.**, «*Droit pénal spécial*», 13ème éd. Sirey Université 2010.

10. **VERON M.,** «*Droit pénal des affaires*», Compact, 6ème éd. Amand Collin, 2005.

11. **VERON M.,** «*Droit pénal spécial*», 6ème éd. Arman Collin, Paris, 1998.

12.WILFRID J-D., «*Droit pénal des affaires, Droit privé*», précis Dalloz, 4ème éd. 2000

2) OUVRAGES GENERAUX DE DROIT LIBANAIS :

١٣. **القهوجي ع.** ،«*قانون العقوبات، القسم الخاص، جرائم الاعتداء على المصلحة العامة وعلى الانسان و المال*»،منشورات الحلبي الحقوقية، بيروت، طبعة ٢٠٠٢

١٤. **حسني م.** ،«*جرائم الاعتداء على الأموال*» ١ / ٢ ، طبعة ثالثة ، منشورات الحلبي الحقوقية ، بيروت.

١٥. **شلالا ن.ن،** «*دعاوى الاحتيال وما جرى مجراه* »، دراسة مقارنة من خلال الفقه والاجتهاد والنصوص القانونية، المؤسسة الحديثة للكتاب ،٢٠٠١

١٦. **نصر ش.** « *جريمة الاحتيال*»، الطبعة الأولى ، ٢٠١٢

١٧. **نصر ف.**، «*قانون العقوبات الخاص، جرائم وعقوبات ، دراسة مقارنة وتحاليل* »، منشورات صادر، طبعة ٢٠٠٩

١٨. **عالية س.** ،« *شرح قانون العقوبات ، (القسم العام) معالمه- نطاق تطبيقه- الجريمة- المسؤولية- الجزاء*» ، مجد المؤسسة الجامعية للدراسات والنشر والتوزيع)، بيروت ، ٢٠٠٢

II- OUVRAGES SPECIAUX:

1) OUVRAGES SPECIAUX DE DROIT FRANCAIS:

CASILE J-F., «*Le Code pénal à l'épreuve de la délinquance informatique*», éd. Presses-universitaires d'Aix Marseille, PUAM, 2002.

2) <u>OUVRAGES SPECIAUX ARABES ET LIBANAIS</u> :

1. **EL CHAER N.**, «*La criminalité informatique devant la justice pénales*», éd. juridiques Sader, 2004.

2. **HABHAB M.**, «*Le droit pénal libanais à l'épreuve de la cybercriminalité*», éd. juridiques Sader, 2011.

٣. **الحن م. عبد الرؤوف** «*جريمة الاحتيال عبر الانترنت*» (الأحكام الموضوعية والأحكام الاجرائية)، منشورات الحلبي الحقوقية، ٢٠١١

٤. **السراج ع.** ،«*شرح قانون العقوبات الاقتصادي في التشريع السوري والمقارن* » ، منشورات جامعة دمشق، ٢٠١٠

٥. **الغول ح. م.** ،«*جرائم شبكة الانترنت، والمسؤولية الجزائية الناشئة* عنها »، دراسة مقارنة، منشورات بدران الحقوقية، ٢٠١٧

٦. **جبور ف.** ،«*حماية المستهلك عبر الانترنت، ومكافحة الجرائم الالكترونية ، دراسة مقارنة*»،منشورات الحلبي الحقوقية ، بيروت ، طبعة ٢٠١٢

٧. **شومان ن.** ، «*التكنولوجيا الجرمية الحديثة وأهميتها في الاثبات الجنائي*» ، ٢٠١١

٨. **مغبغب ن**. ،«*مخاطر المعلوماتية والانترنت ، المخاطر على الحياة الخاصة وحمايتها، دراسة في القانون المقارن*»، ١٩٩٨

٩. **ناصيف إ.** ،«*العقود الدولية ، العقد الالكتروني في القانون المقارن* »، منشورات الحلبي الحقوقية ، بيروت ، ٢٠٠٩

3) <u>OUVRAGES SPECIAUX DE DROIT ANGLAIS:</u>

1. **HITCHCOCK J.A.**, «*Net crimes and Misdemeanors, outmaneuvering Web spammers, Stalkers, and Con Artists*», second edition, Information Today Inc., 2006.

2. **KOZYRIS Phaedon (J.)**, «*Regulating internet abuses, invasion of privacy*», published by Kluwer Law International , 2007.

3. **Online fraud and crime**: Are consumers safe? Hearing before the subcommittee on commerce trade and consumer protection, 2001, p. 33.

4. **VAUGHAN J.,** «*Texas's new e-consumer protection acts: A (PH)ARWELL to phishing and spyware*», Texas Wesleyan law review, 2006.

III- ARTICLES ET CHRONIQUES:

1. **BOUZAT P.**, «*Crimes et délits contre les biens*», RSC 1978, p.355à 361.

2. **CONSTANT J.,** «Arnaques au faux président : l'escroc Gilbert Chikili arrêté en Ukraine » www.leparisien.fr.

3. **CORVENIEN CH., «***le rançongiciel, dernière arme fatale du crime organisé*» www.lefigaro.fr

4. **DEVEZE J.**, note sous l'arrêt Cass.Crim.9 mars 1983, recueil Dalloz, 1984, p.209 à 214.

5. **FREYSSINET E.,** «*investigations & transformations numériques*» www.ericfreyssi.net.

6. **GASSIN R.**, note sous les arrêts Cass. Crim 10 décembre 1970 et Trib correct. Saint-Etienne, 17 avril 1970, recueil de jurisprudence 1972.

7. **GRAULLE B.,** «*Fraude au président : les banques menacées*» www.business.lesechos.fr.

8. **GRONDON A., «***Le boom inquiétant de la fraude au président*» www.leseechos.fr.

9. **LARDEUX M.,** «*une arnaque en progression dite rançongiciel*», www.realahune.fr

10. **LECHEVALIER, A-S.,** «*Fraude au président : des milliers d'entreprises escroquées*», www.parismatch.com.

11. **LEDERER E.,** «*Les banques en première ligne face à la fraude au président*», www.business.lesechos.fr.

12. **MATSOPOULOU H.**, note sous l'arrêt Cass. Crim. 24 mars 2010, pourvoi n^{0}08-85, 109, RSC, septembre 2010, chronique de jurisprudence, p.629 à 631.

13. **MATSOPOULOU H.**, note sous l'arrêt Cass. Crim. 1er juin 2011, pourvoi n^{0} 10-83.568, RSC, Octobre/décembre 2010, chroniques de jurisprudence, p.839 et 840.

14. **MATSOPOULOU H.**, note sous l'arrêt Cass.Crim. 25février 2004, pourvoi n^{0}03-81.173, RSC, Juillet/septembre 2005, chroniques de jurisprudence, p.576 et 577.

15. **MATSOPOULOU H.**, note sous l'arrêt Cass.Crim. 28 février 2012, pourvoi n^{0}11-82.953, RSC, Octobre/décembre 2012, chroniques de jurisprudence, p.865 à 867.

16. **RONFAUT L.**, «comment se protéger et réagir face à un rançongiciel ?», www.lefigaro.fr.

17. **ROLLAND S.** «*Cyberattaques : que contient le paquet cyber que l'Europe veut voter en 2018 ?*» www.latribune.fr

18. **TOUSSAY J.**, «*Ransomware ou rançongiciel, un logiciel malveillant qui prend vos données en otage*», www.huffingtonpost

IV- MEMOIRES :

1. **KASONGO C.K.**, *«la convention sur la criminalité et le droit pénal congolais»*, Licence en droit 2003, Université de Kinshasa RDC.

2. **SERRES D. et CLUZEAU A.**, *«la cybercriminalité nouveaux enjeux de la protection des données»*, maitrise en droit de l'entreprise 2008, Université Laval.

V- RESOLUTIONS ET CONGRES :

Résolutions des congrès de l'Association Internationale de Droit Pénal (1924-2004), nouvelles études Pénales, édition èrès2009, n^0 20.

VI- SITOGRAPHIE :

www.business.lesechos.fr
www.huffingtonpost.com
www.lemonde.fr.
www.legifrance.gouv.fr
www.lefigaro.fr
www.russian-detective.com/scams

www.latribune.fr
www.parismatch.fr
www.leparisien.fr

TABLE DES MATIÈRES