CONSEQUENCES DE L'UTILISATION DES TIC SUR LA CRIMINALITE ECONOMIQUE ET FINANCIERE EN ALGERIE

Pr HADID Noufyele - Université d'Alger3
noufeyle.hadid@gmail.com
Mr MERBOUHI Samir- Université d'Alger3
samirmerbouhi254100@gmail.com

Résumé :

Cet article vise à démontrer les conséquences de l'utilisation des TIC sur la criminalité économique et financière en Algérie, car celle-ci, dans son aspect traditionnel, est déjà considérée comme un phénomène complexe et polymorphe. Avec les TIC, plusieurs changements de taille vont apparaitre touchant principalement les typologies des auteurs, leurs profils, ainsi que les modes opératoires.

C'est dans ce contexte bien précis, que le présent article s'inscrit. Il aborde le sujet en estimant utile de faire le point sur cette grande question d'actualité vue dans son aspect technologique étant qu'en Algérie la criminalité économique et financière commence déjà à prendre une connotation « Cyber ».

Mots clés : criminalité économique et financière, TIC, cybercriminalité, cybercriminalité économique et financière, nouvelles formes, nouveaux modes opératoires.

Abstract:

The purposes of this paper are to demonstrate the consequences of the information and communication technologies use, on the economic and financial criminality in Algeria, since this one is already considered as a complex and a polymorphic phenomenon, in its traditional aspect. With the contribution of the information and communication technologies, several large changes will appear and will influence, mainly, the authors' typologies and their profiles, as well as their modus operandi.

It is within this precise context that the present paper focuses. It seems already useful to take into account this major topical issues, precisely, in its technological aspects, as the economic and financial criminality areal ready getting a «Cyber» connotation in Algeria.

Key words: economic and financial criminality, information and communication technologies, cybercrime, economic and financial cybercrime, new forms, new operating modes.

ملخص:

من خلال هذا المقال سوف نحاول توضيح تبعات استعمال تكنولوجيات المعلومات والاتصال على الجريمة الاقتصادية والمالية في الجزائر، فبالنظر إلى جانبها التقليدي تعد هذه الأخيرة أصلا ظاهرة معقدة ومتعددة الأشكال. ضف إلى ذلك تكنولوجيات المعلومات والاتصال ، سيترتب عنها لا محالة عدة تغييرات نوعية، تمس على وجه الخصوص أصناف الفاعلين، صفاتهم وكذا الأنماط الإجرامية.

ضمن هذا الإطار يندرج موضوع هذا المقال، حيث ارتأينا إبراز أهمية هذه الإشكالية من المنظور التكنولوجي، وهذا لأن الجريمة الاقتصادية والمالية بدأت تأخذ دلالات "سيبرانية" في الجزائر.

الكلمات المفتاحية: الجريمة الاقتصادية والمالية، تكنولوجيات المعلومات والاتصال، الجرائم الإلكترونية، الجريمة الاقتصادية والمالية الإلكترونية، أشكال جديدة، أنماط جديدة.

Introduction

Les avancées considérables des TIC ont fait changer les flux mondiaux d'informations ainsi que le monde des affaires. L'Internet et sa portée mondiale, l'automatisation du secteur bancaire, l'économie numérique et d'autres évolutions technologiques ont incidemment offert aux criminels de nouvelles méthodes de nuire. Nous assistons à une ère numérique de croissance rapide, accompagnée de nouvelles menaces automatisées.

Les défis attendus impliquent résolument la collaboration entre spécialistes et experts. Comme le soulignait Edwin Sutherland, le sociologue américain dans son livre «White Collar criminality », dès 1940 des avantages réciproques que pourraient tirer les économistes et les criminologues d'une meilleure intégration de leurs connaissances. Bien que cette démarche à l'interdisciplinaire porte particulièrement sur la criminalité en col blanc, soit la criminalité économique et financière, d'autres formes de criminalité se prêtent également bien à une telle vision, parmi lesquelles figure la criminalité liée aux TIC[i].

L'Algérie, à l'instar des pays de la communauté internationale, recourt depuis plusieurs années à l'utilisation des TIC, notamment avec le lancement de plusieurs projets structurants, tels le : e-paiement, e-gouvernement, e-banking, signature électronique et prochainement le e-commerce. Dés lors, elle n'est donc pas à l'abri de nouvelles formes de criminalité économique et financière ayant comme soubassement les TIC.

Ainsi, eu égard de l'utilisation grandissante des TIC, nous pouvons s'attendre aujourd'hui à une évolution des procédés, des modes opératoires et des méthodes d'exercice de la criminalité économique et financière et subséquemment, l'émergence de nouvelles formes. Avec, particulièrement la phase de transition multisectorielle que l'Algérie traverse, cela va faire d'elle sans doute un pays convoité par les réseaux criminels, afin d'y exercer leurs activités délictueuses.

Cependant, il est constaté que la prise en charge de cette forme de criminalité dans sa nouvelle dimension technologique, voire même dans sa forme traditionnelle, est encore embryonnaire du fait qu'aucune étude empirique n'a été réalisée en Algérie, visant à situer son impact, mis à part quelques travaux plutôt académiques.

Dans cette étude nous avons essayé de démontrer comment cette transition vers l'utilisation des TIC va transformer la criminalité économique et financière en Algérie. Chose qui nous amène à

poser la question suivante : Eu égard à la prolifération accélérée de l'utilisation des TIC, Est-ce que la criminalité économique et financière changera notablement en Algérie et prendra réellement une connotation « Cyber » ?

En matière de lutte contre la criminalité économique et financière, nous pensons que la compréhension des nouveaux risques criminels encourus par l'utilisation des TIC est un élément fondamental dans l'élaboration d'une stratégie visant à contrecarrer le phénomène, qui ne cesse de prendre de l'ampleur en Algérie[ii]. Il s'agit en effet, de comprendre ce qu'est la criminalité économique et financière commise à l'ère des TIC, d'en maitriser les contours ainsi que les rouages et les procédés utilisés.

1.Corrélation entre les TIC et la criminalité économique et financière

Selon l'ONU, la criminalité économique et financière désigne de manière générale, toute forme de criminalité astucieuse et non violente qui a pour conséquence l'appât du gain soit une perte financière. Cette criminalité couvre une large gamme d'infractions, dont le concept reste à ce jour délicat à cerner. En revanche, ce phénomène est devenu de plus en plus compliqué par le recours grandissant à l'utilisation des TIC, qui ont offert aux criminelles de nouvelles opportunités, brèches et perspectives de nuire[iii].

L'évolution rapide et ample des TIC ces dernières années est une des spécificités caractérisant la société moderne et qui peuvent susciter un certain nombre d'interrogations quant à leur utilisation pour perpétrer des infractions relevant du phénomène de la criminalité économique et financière[iv].

Ces technologies ont favorisé l'expansion de nouvelles activités criminelles, souvent difficiles à déceler et utilisant de nouvelles formes et de nouveaux procédés[v]. Elles sont également à l'origine de la complexité de certaines formes de criminalité, qui ne cessent de recourir aux moyens sophistiqués, permettant aux criminels de se procurer des gains faciles en tout anonymat et avec un minimum de risque d'identification.

Les TIC ont amené des changements de taille et de dimension de la criminalité économique et financière en la rendant transnationale. Cependant l'appât du gain, qui constitue la nature fondamentale de cette forme de criminalité, il ne s'est pas métamorphosé ce sont plutôt les moyens utilisés, les types et profils de criminels, les cibles et victimes, les montants des préjudices causés qui ont plutôt changé de forme.

Il est bien évident que les criminels se sont rapidement adaptés et ont compris les avantages susceptibles d'être tirés des TIC, du fait de la rapidité d'exécution des instructions réalisées, le degré de confidentialité assurée grâce aux techniques de cryptage et de chiffrement des données numériques et l'immatérialité des transactions qui protègent l'anonymat, ce qui ne peut que favoriser incontestablement la criminalité économique et financière[vi]

De ce qui précède, il est utile de préciser que la criminalité économique et financière ne saurait échapper à cette évolution. Les TIC facilitent davantage la commission de cette forme de criminalité astucieuse et complexe.

2. Lien de causalité entre les TIC et la cybercriminalité

Les TIC ont fait apparaitre un nouveau concept de criminalité qui est « la cybercriminalité » qui pourrait laisser entendre que nous assistons à un phénomène nouveau, à la fois dans ses moyens et ses objectifs, mais en réalité, ce sont surtout les modes opératoires et les procédés d'attaque qui ont évolués et se sont complexifiés. Les motivations, quant à elles, demeurent

largement inchangées. Cedi dit, l'ultime objectif de la cybercriminalité dans ses aspects économiques et financiers reste bel et bien l'appât du gain[vii].

D'après les spécialistes, il n'existe pas de définition internationale de la cybercriminalité, mais généralement elle décrit la criminalité dans laquelle les TIC sont une partie essentielle. Elle est employée aussi pour les formes de criminalité traditionnelle commises via l'utilisation des TIC. Selon cette définition, dans le premier cas de figure les TIC sont la cible de l'attaque, alors que dans le second cas, elles en sont le vecteur.

De ce fait, nous pouvons admettre, que la cybercriminalité correspond à l'utilisation des TIC dans l'objectif primordial est d'exploiter les failles des individus, des entreprises et des Etats à des fins purement lucratives.

Nous pensons à cet égard que la cybercriminalité est désormais l'une des formes d'exploitation économique les plus rentables avec un faible risque pour ses auteurs et dont les domaines les plus ciblés sont les services financiers et commerciaux en ligne, et les réseaux sociaux, sources primaires pour le vol d'argent et d'informations financières[viii].

3. Croisement de la criminalité économique et financière et la cybercriminalité

La cybercriminalité est en quelque sorte un moteur accélérant de la criminalité économique et financière préexistante, du fait que plusieurs formes de criminalité économique et financière relèvent aujourd'hui de la cybercriminalité. Ceci dit, les TIC font désormais partie intégrante du champ de la criminalité économique et financière.

Il est évident aujourd'hui que la criminalité économique et financière recourt désormais à l'utilisation de plus en plus grandissante des TIC. Par ailleurs, elle rejoigne parfaitement la cybercriminalité avec des agissements économiques et financiers. D'après ce constat nous pouvons dire dés lors, que la cybercriminalité économique et financière constitue le prolongement naturel de la criminalité économique et financière traditionnelle, profitant simplement de nouveaux moyens fournis par les TIC que ceux habituellement mis en œuvre.

Il est constaté également à travers les scandales économiques et financiers perpétrés à travers le monde, que les formes de criminalité économique et financière évoluent en corrélation croissante avec la cybercriminalité, faisant naitre de nouvelles opportunités et occasions pour les criminels[ix]. Il s'ensuit, non seulement l'émergence de nouvelles formes de criminalité économique et financière, mais également l'accroissement du montant du préjudice engendré, l'augmentation du nombre d'affaires enregistrées, et aussi l'internationalisation croissante de cette forme de criminalité[x].

Sur la base de ce croisement, entre deux formes de criminalité que nous croyons à un moment donnée qu'elles étaient complètement distinctes, nous pouvons dire aujourd'hui, que la cybercriminalité est effectivement de plus en plus utilisée comme arme par la criminalité économique et financière qui se focalise sur des cibles financières et économiques.

4. Les caractéristiques de la cybercriminalité économique et financière

A travers la comparaison entre la criminalité économique et financière traditionnelle et la cybercriminalité économique et financière nous allons essayer de démontrer que le cyberespace

est le lieu le plus propice des criminels en col blanc, car il offre des opportunités extraordinaires permettant la réalisation des activités illicites. En effet, les TIC de par leurs caractéristiques sont porteuses de potentialités criminelles adéquates à l'expression de la criminalité économique et financière[xi]. Comme le présente le tableau ci-dessous :

	Criminalité économique et financière traditionnelle	Cybercriminalité économique et financière
Historique	Phénomène plus ancien.	Nouveau phénomène.
Territorialité	Généralement ne sort pas en dehors du territoire national, du fait de l'obligation d'avoir un contact physique, dans le cas échant la proximité pour l'action.	Généralement elle est transnationale, réalisable depuis tout lieu dans le monde sans forcement avoir un contact physique.
Auteur	Le savoir faire criminel est axé essentiellement sur l'humain, à travers son niveau intellectuel, ses compétences, poste occupé, etc.	Le savoir faire criminel est embarqué dans un logiciel réutilisable sur un grand nombre de cibles, un grand nombre de fois.
Quantification	Difficile de quantifier la criminalité économique et financière.	Difficile de quantifier les préjudices financiers engendrés par la cybercriminalité économique et financière.
Statistique	Chiffre noir élevé.	Chiffre noir trop élevé, dû spécialement à la complexité des attaques.
Type de criminalité	Criminalité non violente et astucieuse.	Criminalité non violente et astucieuse, recourant de plus en plus aux TIC.
Nature de la preuve	Preuves matérielles consignées généralement sur le papier.	Preuves immatérielles consignées sous forme numérique et peuvent être détruites ou chiffrées à distance.
Modes opératoires	Non automatisés.	De plus en plus automatisés.
Types d'attaque	Attaque physique.	Attaque numérique.
Gain	Modéré, car généralement l'acte criminel est limité à une cible seulement à la fois.	Plus important, car l'acte criminel est réalisable sur des milliers de cibles à la fois.
Témoins	Témoin classiques.	Experts, programmeurs, fournisseurs d'accès, etc.
Risque encouru	Plus de risque car ce genre t'attaque nécessite une présence physique.	Moins de risque puisque l'attaque est commise à distance.
Techniques d'investigation	Techniques classiques.	En plus des techniques classiques il existe aussi de nouvelles techniques.
Compétences des enquêteurs	L'enquêteur doit avoir des connaissances dans les domaines de : l'économie, la finance, les techniques	En plus des connaissances en finance, techniques bancaires, impôts et autres il doit posséder des connaissances en

	bancaires, les impôts, etc.	matière de TIC.

L'analyse de la présente comparaison, démontre clairement qu'une attaque numérique est facilitée par l'usage des TIC, notamment celle se rapportant à la cybercriminalité économique et financière, à titre d'exemple une attaque commise contre une banque, en la rendant difficile à retracer, du fait de rebonds et du nombre important des machines compromises en chaine, ainsi que la découverte généralement tardive de ce genre d'attaque. Ce qui rend le recours aux TIC avantageux, par dissymétrie.

Ajouté à cela, d'autres paramètres d'ordre purement opérationnel, rendant la lutte contre la cybercriminalité économique et financière de plus en plus complexe. En effet, cette lutte sans fin entre les acteurs de lutte et les cybercriminels repose sur plusieurs principes non équivalents, à savoir :

- Les acteurs de lutte doivent défendre toutes les brèches, qui sont nombreuses et évolutives surtout dans le domaine des TIC, par contre les cybercriminels peuvent choisir le point le plus vulnérable ;
- Les acteurs de lutte ne peuvent défendre ce qu'ils connaissent, tandis que les cybercriminels peuvent chercher d'autres points faibles ;
- Les acteurs de lutte doivent être vigilant en permanence, alors que les cybercriminels peuvent attaquer quant ils veulent ;
- Les acteurs de lutte doivent réagir tout en respectant les lois et les règlements alors que les cybercriminels enfreignent complètement les lois. Les criminels considèrent ce nouvel écosystème comme étant une zone de non droit.

De ce qui précède, il semble que la théorie criminologique, dite du passage à l'acte, corrobore parfaitement les résultats obtenus de cette comparaison. Celle-ci prétend que nous sommes tous des délinquants potentiels pour autant que l'on réunisse trois (03) conditions : une opportunité, une motivation et un minimum de risque[xii]. En effet, les TIC ont offert énormément d'opportunités aux criminels, telles que : la rapidité des transferts, l'anonymat, la dématérialisation, etc. chose qui explique cette transition vers la cybercriminalité économique et financière au détriment de la criminalité économique et financière traditionnelle.

5. Etude de cas: Analyse des rapports techniques dressés par les unités spécialisées de la Gendarmerie Nationale (2013-2016)

Les procédures établies par les services en charge de la police judiciaire sont des outils de recherches qualitatives par excellence, alors qu'en pratique il s'agit des procès-verbaux et des rapports techniques. A ce sujet, une règle d'or de la criminologie indique qu'un indicateur de la criminalité est plus valide lorsqu'il est basé des phases initiales des procédures telles que celles de la police judiciaire[xiii]

En effet, se baser sur les statistiques policières pour expliquer cette métamorphose de la criminalité économique et financière est aberrant. De plus, les statistiques policières ne dépeignent qu'assez superficiellement les phénomènes criminels, car elles sont pauvres en informations sur les modes opératoires. Cependant, les rapports techniques se rapportant aux crimes identifiés, offrent de très utiles informations, notamment sur les différents modes

opératoires utilisés, les typologies de la criminalité qui ont prévalus, les moyens et les outils du crime, les liens entre les criminels, la typologie des auteurs, et les profits générés par le crime, etc.

Justement, pour tenter de répondre sur la problématique de notre étude, nous avons eu recours à l'analyse des rapports techniques dressés par les unités spécialisées de la Gendarmerie Nationale pour la période allant de 2013 à 2016. En effet, un échantillon de six cent quarante trois (643) rapports techniques élaborés par des experts en matière de lutte contre la cybercriminalité ont été exploités, relatifs principalement aux enquêtes judiciaires. La classification des comportements criminels enregistrés lors de l'analyse, comprend principalement trois (03) catégories d'infraction portant atteinte aux personnes, aux biens et à l'ordre public. Toutefois, uniquement les rapports techniques relatifs à l'atteinte aux biens ont été pris en considération, qui sont en nombre de cent quatre vingt sept (187) affaires, et ce, dans l'objectif de se limiter au cadre dans notre recherche.

Le nombre des rapports techniques analysés durant la période de référence, démontre clairement que la cybercriminalité ne cesse de croitre, surtout avec le recours à l'utilisation des TIC. Par ailleurs, les TIC ont rendu le phénomène de la criminalité économique et financière de plus en plus complexe**,** chose qui s'explique par le nombre de faits non élucidés, principalement pour les affaires économiques et financières ayant une tendance internationale.

Il est évident, que les TIC ont rendu difficile la détection de ces nouvelles formes de criminalité en recourant le plus souvent à la dématérialisation et l'anonymat. Chose qui contredit complètement la règle criminologique qui édicte que « le crime ne paie pas » et pourtant un bon nombre de criminels agissent dans l'ombre de cet écosystème.

Les statistiques policières enregistrées permettent de se renseigner sur le nombre d'affaires traitées par les acteurs de lutte en matière de criminalité économique et financière et la cybercriminalité et aussi sur les différentes formes et sur la manière dont elles sont prises en compte. Le paradoxe réside justement dans ce point bien précis, car il ressort de la manière d'enregistrement de ces statistiques qu'on dissocie complètement la criminalité économique et financière vue dans sa dimension classique de la cybercriminalité avec comme effet des incidences économiques et financières, autrement dit la cybercriminalité économique et financière.

En effet, la cybercriminalité économique et financière n'est pas prise en compte du fait qu'il s'agit d'une nouvelle forme de criminalité à part entière. Cependant, selon une étude récente menée en 2014 par le réseau d'entreprises américaines spécialisées dans des missions d'audit, d'expertise comptable et de conseil à destination des entreprises, exerçant sous la raison sociale de PWC (PricewaterhouseCoopers)[xiv], la cybercriminalité est considérée désormais comme la deuxième forme de criminalité économique et financière après les détournements de fonds, ceci dit, qu'elle est comptabilisée en matière de statistique avec la criminalité économique et financière.

Cependant en Algérie la criminalité liée aux TIC, statistiquement parlant elle est classée sous le rangement de la cybercriminalité, mais concrètement, on voit tout d'abord une attaque de cybercriminalité, secondée généralement par une criminalité économique et financière.

Cette démarche entreprise dans l'enregistrement des statistiques liées à la cybercriminalité économique et financière va sans doute fausser le nombre exact de la criminalité économique et financière commise, car les deux formes de criminalité convergent vers l'appât du gain. De ce fait, toutes les démarches entreprises dans l'élaboration de la politique pénale seront vouées à l'échec, à cause de manque de statistiques fiables. Comme le soulignait également un document de travail élaboré par l'ONODC[xv] qui a évoqué le problème d'absence d'informations fiables sur l'étendue du phénomène.

En effet, si nous comptabilisons la cybercriminalité économique et financière avec la criminalité économique et financière traditionnelle, il est évident que le nombre des affaires liées à la criminalité économique et financière augmentera d'une manière significative. Ceci confirme qu'une grande partie de la criminalité économique et financière est mal prise en charge.

Dans le même sillage, il ressort de l'analyse des statistiques policières, que ces dernières ne donnent pas une image claire des tendances de la criminalité économique et financière, principalement celles liées aux TIC du fait des catégories statistiques et de qualifications juridiques qui empêchent une compréhension commune et mesurèrent de ce genre de criminalité.

Effectivement, en matière de reportabilité des statistiques policières, il n'est pas aisé actuellement, d'avoir une bonne visibilité, permettant une meilleure prise en charge de ce phénomène, car la majorité des infractions enregistrées sont comptabilisées dans la nomenclature globale des infractions du droit commun sans distinction avec celles commises par le biais des TIC, exception faite pour les atteintes aux systèmes automatisés des données.

Ce constat est la résultante de l'absence d'un corpus juridique régissant ces nouvelles formes de criminalité, ce qui empêche d'avoir une meilleure politique criminelle, visant à qualifier et quantifier les nouvelles formes de criminalité économique et financière émergentes indépendamment de la criminalité économique et financière traditionnelle.

Cette nouvelle vision de prise en compte des statistiques va aider sans doute à mieux cerner les contours de la criminalité économique et financière et de la définir. Effectivement, la dimension technologique de ce phénomène n'est pas prise compte par les acteurs de lutte en Algérie.

Il faut faire remarquer également, qu'il ressort de l'analyse de quelques affaires traitées en Algérie, que les TIC servent également à réaliser des crimes conventionnels qui étaient jusque là contrôlables. A titre d'exemple, il est facile aujourd'hui d'escroquer une personne sans avoir de contact physique avec elle à l'instar de l'escroquerie de type nigérian connexion « scams 419 » ou « fraudes 419 », qui consiste en l'abus de la crédulité des victimes en utilisant principalement les messageries électroniques de la première génération d'internet ou le Web 1.0 pour leur soutirer de l'argent.

Les sites d'annonces, à l'exemple du site ouedkniss (www.ouedkniss.com), offrent aussi un espace favorable aux escrocs. Cette technique s'avère d'ailleurs relativement fréquente en Algérie. Il s'agit d'arnaques aux personnes mais qui touchent directement à leurs biens du fait que les citoyens algériens ont commencé à étaler leurs biens en ligne sur le net.

Force est de constater aussi, que les menaces émergentes ont une tendance internationale rendant la tâche plus fastidieuse dans la résolution de ce genre d'affaires et demande un travail de grande haleine. Ajouté à cela la conceptualisation des textes juridiques ayant trait à la cybercriminalité en Algérie qui pose un énorme problème quant à leur déploiement en dehors des circonscriptions judiciaires et même du territoire du pays, alors que la structure même des TIC, particulièrement de l'internet, ne connait pas de frontières physiques.

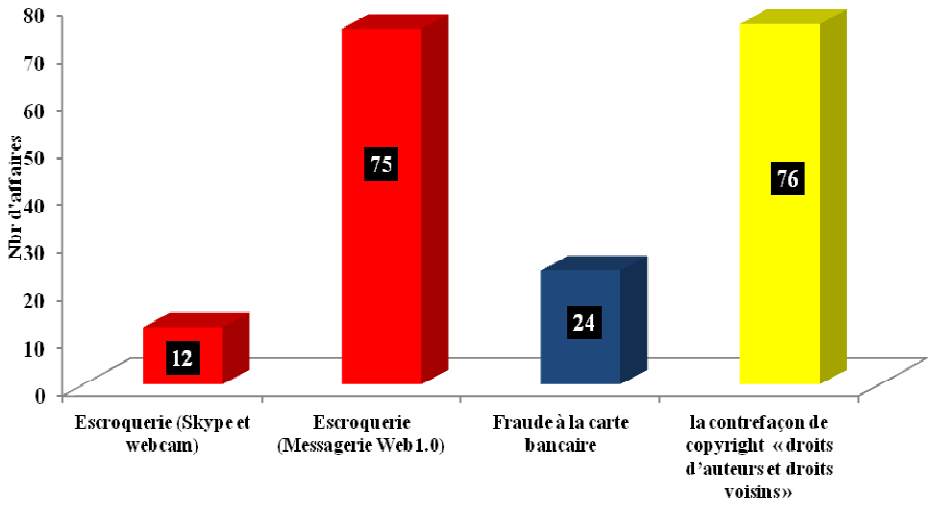
Il apparait en outre qu'avec le recours grandissant à l'utilisation des TIC ces dernières années, la criminalité économique et financière est de plus en plus transnationale que nationale, ce qui a pour incidence de remettre en question tant la protection de l'économie nationale que celle des individus et des entreprises. Comme elle implique aussi la revue des techniques d'enquête ainsi que la catégorisation de la criminalité économique et financière classique, la souveraineté des acteurs de lutte et les instances judiciaires, voire même la prise en charge globale de cette nouvelle dimension de la criminalité économique et financière[xvi].

Certes, l'Algérie a commencé récemment, le 04 octobre 2016, l'utilisation du paiement électronique et ce dans le cadre de la modernisation des systèmes financiers, alors que le recours au commerce électronique est en train de se préparer. Néanmoins le revers de la médaille, fait que ces deux domaines sont complémentaires et constituent la menace majeure des cyberattaques criminelles.

L'analyse des rapports techniques confirme que la criminalité économique et financière en Algérie commence déjà à prendre une autre dimension avec l'apport des TIC. Théoriquement parlant c'est paradoxal, mais nous réalisons qu'effectivement les criminels en Algérie profitent déjà des petites occasions offertes à l'heure actuelle. En effet, plusieurs infractions recourant aux TIC ont été enregistrées, et dont les escroqueries représentent la forme de la criminalité la plus récurrente en Algérie, principalement celle de type « scams 419 », ainsi que d'autres commises à travers l'envoie des SMS ou des messageries électroniques.

Par ailleurs, nous avons enregistré d'autres infractions liées à la contrefaçon de copyright « droits d'auteurs et droits voisins », la fraude à la carte bancaire principalement avec la technique du Social Engineering ou l'ingénierie sociale, l'abus de confiance et l'usurpation d'identité. Le graphe ci-dessous illustre clairement les types de criminalité touchant les biens des individus et des entreprises et qui ont prévalus jusqu'ici en Algérie.

Graphe représentant la distribution par typologie de la cybercriminalité économique et financière en Algérie



Il existe donc, plusieurs infractions économiques et financières ayant recours aux TIC, et ce nonobstant encore la non utilisation du commerce électronique en Algérie. Quoique, cette dernière n'est pas aussi à l'abri de toute tentative sophistiquée de cyberattaque et ce, à l'instar de la tentative de détournement de 951 millions de dollars du compte de la banque centrale du Bengladesh à la Federal Reserve de New York et l'affaire de 81 millions de Dollars de la banque du Vietnam, qui ont été perpétrées à travers l'envoi des ordres frauduleux de virement SWIFT. Notons que toutes les banques algériennes sont adhérées actuellement à ce système qui utilise depuis l'année 2008 le protocole internet (IP).

L'analyse des rapports techniques, principalement les indicateurs de sexe et d'âge des auteurs, démontrent clairement qu'il s'agit d'une criminalité jusqu'ici exclusivement masculine dont l'âge médian des auteurs est de 25 ans.

En ce qui concerne le niveau intellectuel des auteurs, il a été constaté qu'il s'agit de personnes ordinaires ayant un niveau moyen, ce qui démontre clairement les avantages et les bienfaits des TIC, qui sont en train de changer graduellement le paradigme de la criminalité économique et financière en Algérie, qui était auparavant commise par une frange d'âge plus vieille allant à plus de 40 ans, constituée essentiellement de personnes bien placées, occupants des postes de responsabilités tels que les commissaires aux comptes, les experts comptables, les banquiers, etc. En effet, le recours à l'utilisation des TIC a poussé certains jeunes à s'investir davantage dans la criminalité astucieuse plutôt que la criminalité violente.

Les résultats obtenus, confirment parfaitement l'étude de la criminalité économique et financière qui a été réalisée au sein des entreprises suisses en 2005, et dont l'un de ses résultats précise que : **« …** le nombre des gens ordinaires qui commettent des délits économiques et financiers est toujours plus important, notamment grâce à l'accès grandissant aux ordinateurs et autres nouvelles technologies **»**[xvii]**.** En effet, le haut degré de compétence économique et financière, ainsi que le professionnalisme nécessaire à la réalisation de la criminalité économique et financière, font que celle-ci peut être facilitée par les TIC, ces dernières rendent cette forme de

criminalité complexe, de plus en plus à la portée des criminels ordinaires, comme c'est le cas de la typologie relevée actuellement en Algérie.

Effectivement, il revient de dire que les TIC contribuent davantage à la facilitation et l'acquisition de savoir faire criminel, dans tous les domaines de l'économie et de la finance allant même jusque dans les techniques les plus pointues nécessaires à la réalisation de la criminalité économique et financière complexe. Disons que les TIC prêtes aussi main forte aux criminels dans leur identification des opportunités criminelles[xviii].

Il est utile de préciser, que ces statistiques à l'instar de celles délivrées par les instances internationales ne constituent que la partie apparente de l'iceberg, car le chiffre noir, autrement dit, la criminalité qui échappe à la constatation des pouvoirs publics en matière de ce type de criminalité est trop élevé[xix], et ce pour plusieurs raisons, à savoir : criminalité astucieuse, complexe, volatilité de la preuve numérique, ignorance, peur, problème de territorialité, manque de confiance, crédibilité, etc.

A travers cette analyse, il est évident, que la criminalité économique et financière en Algérie est en train d'évoluer en nombre, en forme et en sophistication car les attaques deviennent de plus en plus automatisées. Cela dit, les TIC sont un facteur de proximité criminelle, dès lors la prise en charge de cette forme de criminalité, nécessite une approche globale qui tient compte simultanément des dimensions sociale, juridique, économique et technologique.

Pour conclure, nous retiendrons qu'il ya eu un changement quantitatif en matière du nombre d'infractions enregistrées ayant trait à la criminalité économique et financière, dû singulièrement à l'émergence de nouvelles formes liées spécialement à l'utilisation des TIC, mais également qualitatif manifeste touchant les typologies des auteurs, leur profil (âge, sexe, niveau intellectuel, etc.) ainsi que la manière de commission de ce genre de criminalité. Ce nouveau champ de recherche concerne en particulier la dimension technologique qu'a prise la criminalité économique et financière en Algérie et dont l'ampleur sera de plus en plus importante pour les années à venir, comme c'était le cas de pays qui nous ont précédés en la matière.

Conclusion

En guise de conclusion, nous pouvons noter que notre contribution a été surtout de caractère anticipatif voire préventif étant qu'elle a visé à situer et à définir le changement de paradigme intervenu en matière de compréhension et de perception du phénomène de la criminalité économique et financière principalement dans son nouveau champ d'action technologique que représentent aujourd'hui les TIC.

En ce qui concerne l'Algérie, nous pouvons admettre qu'elle n'est pas du tout à l'abri du nouveau phénomène de la criminalité économique et financière qu'à induit aujourd'hui l'utilisation généralisée des TIC. Bien au contraire, le pays se trouve au cœur de ces mutations vulnérables et il est bien évident que les individus, les entreprises subissent de nouvelles formes de criminalité économique et financière qu'on ne connaissait pas auparavant.

Sur ce, nous pouvons affirmer qu'incontestablement la criminalité économique et financière en Algérie commence déjà à prendre une connotation « cyber ». Cependant elle touche exclusivement les formes conventionnelles qui se sont développées par l'utilisation des TIC principalement l'Internet, donc encore loin des nouvelles formes émergentes observées en d'autres pays où le recours aux TIC est déjà massif.

Ce pourquoi nous sommes donc arrivés à relever qu'il est nécessaire de maintenir la recherche sur le sériage et l'identification des nouvelles formes de criminalité en rapport avec l'utilisation des TIC, ceci en parallèle voire en anticipation des avancées attendues dans le pays, inévitables

par ailleurs, en matière de recours dense aux TIC dans notamment les transactions financières et commerciales.

Dans le même ordre, il ressort pertinent d'être à l'écoute des défis que rencontrent actuellement les pays développés. Cela ne peut que conforter notre vision prospective en Algérie et ce afin de prévoir de nouvelles incriminations, de nouvelles techniques d'investigation, de nouveau champ de recherche, pour une meilleure élaboration d'une politique pénale qui soit cohérente avec les aspects délictueux de la criminalité économique et financière.

Références Bibliographiques

[i] Benoit Dupont, « la coévolution du vol d'identité et des systèmes de paiement, criminologie, les presses de l'Université de Montréal, vol.43, n°2, 2010, p.247-268, Québec. URL : http://id.erudit.org/iderudit/1001777ar.

[ii] Bertrand Perrin, « la lutte contre le blanchiment d'argent : pistes d'actions entre prévention et répression », l'Harmattan, 2009, Paris.

[iii] Onzième Congrès des Nations Unies pour la prévention du crime et la justice pénale, « délinquance économique et financière : défis pour lé développement durable, 18-25 avril 2005, Bangkok (Thaïlande). URL : www.11uncongress.org.

[iv] Ricca Marco, article, « Internet au service de la criminalité économique ? », Revue économique et sociale, 2003: bulletin de la société d'Etudes économiques et sociales.

[v] 13éme congrès des Nations Unies, pour la prévention du crime et la justice pénale, organisé à Doha, 12-19 avril 2015.

[vi] Centre universitaire juridique de recherche sur les menaces criminelles contemporaines, conférence débat sur « crime informatique et cyber-guerre », intervention de Daniel Martin le 18 février 1999.

[vii] Edouard Fernandez-Bollo, « Institutions financières et cybercriminalité » Association d'économie financière « revue d'économie financière », 120, pages 181 à 198, 2015 /4 numéro.

[viii] U. Rasmussen, « La cybercriminalité, un moyen de fraude sophistiqué », Cahiers de droit de l'entreprise n°1, janvier 2013. Dossier 4.

[ix] Maurice Cusson , Benoît Dupont et Frédéric Lemieux , « traité de sécurité intérieur », Presses polytechniques et universitaires romandes, 2008.

[x] Myriam Quéméner, « criminalité économique et financière à l'ère numérique », prix Henri Donnedieu de Vabres, facultés des Droit et de Science politique de Montpellier, Ed. Economica, Paris, 2015.

[xi] Daniel Guinier, Expert en cybercriminalité et crimes financiers prés la Cour Pénale Internationale de La Haye et ancien colonel de la Gendarmerie Française, « Hackers » en devenir et en repenti, quand les talents s'orientent différemment, expertises, n°385, 2013.

[xii] Cusson Maurice, « la criminologie », Hachette supérieur, 6éme édition, 2014, Québec.

[xiv] Economic Crime : A Swiss Perspective, 2014, Suisse, URL: http://www/pwc.ch/user_content/editor/files/pub_adv/pwc_global_economic_crime_survey_14_ch_e.pdf .

[xv] Document de travail élaboré lors du 12éme congrès des Nations Unies pour la prévention du crime et justice pénal : https://www.unodc.org/documents/crime-congress/12th-Crime-congress/Documents/A_CONF.213_9/V1050383f.pdf.

[xvi] Etienne Blais et Bertand Perrin, « la lutte contre la criminalité économique : réponses interdisciplinaires à un défi global » l'Harmattan, 2010, Paris.

[xvii] G. L. Isenring et M.Kilias, l'étude de la délinquance économique dans les entreprises suisses par l'approche situationnelle en vue d'une meilleure prévention. Revue Internationale de Criminologie et de Police Technique et Scientifique .N°, 2005.

[xviii] Solange Ghernaouiti Hélie, « la cybercriminalité, le visible et l'invisible », Presses universitaires polytechniques, 2009, Suisse.