LA CYBERCRIMINALITE A ABAIDJAN, UN PHENOMENE DE MODE OU UNE NOUVELLE GUERRE CONTRE LES FINANCES EN COTE D'IVOIRE?

Docteur Gueu Denis

U.F.R Criminologie de l'Université de Cocody-Abidjan Côte d'Ivoire

Abstract

The evolution of technology gave to the whole humanity a glimmer of hope because it makes easy the realization of works. Thus, transforming the world into one planetary village, the data processing tool becomes today essential in training and information. But it is not all the time success nor profits with the computers especially as one knows the nuisances that they create in finance and economic field. In Côte d'Ivoire, at present, the concept of cybercafé and that of the Internet are mixed up with robbery, swindling and criminality. The phenomenon so much became extensive and we wonder if it is not another way of war against Ivorian finances and economy.

The authors of that practice are not inevitably foreigners because Ivorian youth are strongly involved in nowadays. It is necessary to act quickly in order to stop the misfortune of several people swindled all the time. That must pass by a sensitizing and common sub-regional fight against that phenomenon.

Keywords: Criminality, lifestyle, finances

Résumé

L'évolution de la technologie, a donné à l'humanité entière une lueur d'espoir parce qu'elle facilite la réalisation des travaux. Transformant ainsi le monde en un seul village planétaire, l'outil informatique devient aujourd'hui indispensable à la formation et à l'information. Mais tout n'est pas que succès ni avantage avec les ordinateurs, surtout, quant on sait les désagréments qu'ils engendrent actuellement dans le domaine financier et économique. En Côte d'Ivoire présentement, la notion de cybercafé et celle de l'Internet se confondent avec le vol, l'escroquerie et la criminalité. Le phénomène a tellement pris de l'ampleur qu'on se demande si ce n'est pas une autre forme de guerre contre les finances et l'économie ivoirienne. Les auteurs de cette pratique ne sont pas forcément les non nationaux mais les

jeunes ivoiriens eux-mêmes y sont impliqués fortement ces derniers temps. Il faut vite agir pour freiner le malheur de plusieurs personnes, qui sont grugées à longueur de journée. Cela doit passer par une sensibilisation accompagnée d'une lutte collective sous-régionale.

Motsclés : Cybercriminalité, mode, finances

Introduction et annonce du problème

De plus en plus, les voix se font entendre dans les grandes agglomérations africaines et particulièrement à Abidjan pour décrier l'ampleur du vol d'argent sur le net. Depuis près d'une décennie, l'internet semble devenir un autre danger contre l'économie ivoirienne. Au départ, il était question de faciliter la servitude de l'homme dans les progrès de l'humanité. En effet, depuis les périodes préhistoriques jusqu'à nos jours, beaucoup d'effort et d'investissement ont été faits ; le tout aboutissant à la mondialisation et à la globalisation de l'économie. A l'instar du monde entier, la Côte d'Ivoire va s'inscrire sur l'échiquier des NTIC dans le but de mériter la confiance de nombreux investisseurs, et par là faire fructifier son vaste terrain économique.

Mais avec un revenu fortement contrarié par le coût de la vie qui ne cesse de croître, des comportements délictueux surgissent dans notre société. Entre l'objectif visé et les moyens d'y parvenir, se développe la criminalité silencieuse, astucieuse difficile à contrôler ou à appréhender parce qu'intangible et liée à l'utilisation des NTIC et de l'internet. Cette nouvelle forme de criminalité astucieuse semble à notre avis plus dangereuse que la criminalité violente car elle porte atteinte au patrimoine financier de la société.

Au fond, le terme « cybercriminalité » a été inventé à la fin des années 1990, alors qu'Internet se répandait en Amérique du Nord. Ce terme était utilisé comme une sorte de fourre-tout pour désigner les nouveaux problèmes auxquels se trouvaient confrontées la police et les agences de renseignements découlant des performances toujours meilleures des ordinateurs. Aussi, on l'employait pour décrire de manière relativement vague, tous les types de délits perpétrés sur Internet ou les nouveaux réseaux de télécommunication dont le coût chutait rapidement.

Véritablement, plusieurs recherches ont été menées au sujet de la cybercriminalité. Toutes ces études ont essayé, tant bien que mal de faire la lumière sur la représentation et l'ampleur du phénomène. Mais le fond du problème n'est pas touché, car l'image que présente la cybercriminalité à Abidjan de nos jours laisse entrevoir deux pôles de situation : d'un côté, nous avons un comportement s'inscrivant dans un effet de mode se justifiant par le

plaisir d'être connecté au monde. De l'autre, il y a l'amour du gain facile ancré dans la mentalité d'une grande majorité qui extériorise cette mentalité sur l'internet.

D'une façon ou d'une autre, nous estimons qu'au delà des théories généralistes, il faut aller plus loin dans les recherches en vue de déceler les germes d'une criminalité astucieuse qui s'apparente à une guerre contre les finances.

La cybercriminalité gagne du terrain et par la même occasion continue de faire des victimes : des comptes bancaires vidés, les salaires coupés en deux, les prélèvements illicites, les arnaques à obtention des biens d'autrui, bref la liste est très longue. Ne dit-on pas que le malheur des uns fait le bonheur des autres ? Au moment où des honnêtes citoyens pleurent parce qu'étant victimes de la cybercriminalité, une majorité de criminels sans cœur se réjouissent. Il faut vite mettre fin à cette aventure.

Notre objectif dans cet article est de dégager les vraies sources de ce comportement, analyser les limites des décisions et des lois concernant ce sujet et enfin faire des propositions concrètes en vue d'atténuer un temps soit peu cette pratique.

Cet article comporte trois parties qui sont : la méthodologie (1ère partie), l'état des lieux (2ème partie), l'analyse des décisions et des textes relatifs à ce sujet et propositions de mesures (3ème partie).

Méthodologie

L'hypothèse principale qui a orienté notre recherche est la suivante: *la cybercriminalité développée à Abidjan de nos jours s'inscrit non seulement dans un contexte de mutation médiatique mais aussi dans une logique de gain facile accentuée par une anomie généralisée en côte d'ivoire.*

Pour la justification d'une telle hypothèse, nous avons mené pendant trois mois durant, une enquête auprès d'une population diversifiée à Abidjan. Cette population se compose de certains tenanciers de cybercafé dans les dix communes d'Abidjan, les internautes eux-mêmes, ainsi que quelques victimes de cette pratique.

Pour recueillir les informations, nous sommes passés par plusieurs techniques dont la documentation, l'administration directe des questionnaires, l'observation, le témoignage des gérants de cybercafé ainsi que ceux des victimes, etc.

Quant à l'analyse des données, elle a pris en compte principalement l'analyse qualitative sans oublier un recours par moment à l'analyse quantitative. Nous avons accordé une importance à l'analyse dite qualitative pour le simple fait que nous ne disposions pas de bases de données exhaustives en ce qui concerne le nombre d'internautes à Abidjan.

Echantillon

Nous avons mis l'accent sur un échantillonnage arbitraire mais ciblé. Comme nous le disons auparavant, il est difficile d'obtenir à Abidjan à l'heure actuelle un nombre exact d'internautes, dans la mesure où la maîtrise de l'outil informatique devient un jeu d'enfant, et par conséquent un flux considérable d'Abidjanais a accès à l'internet.

64 personnes au total (sexes et âges confondus) ont été interrogées à travers les dix communes d'Abidjan.

L'état des lieux de la cybercriminalité à Abidjan

L'Identification des auteurs

Pendant notre recherche, nous avons répertorié deux catégories d'auteurs principales : les non nationaux et les nationaux.

Les criminels non nationaux

Impliqués souvent dans des affaires d'escroquerie, certains cybers escrocs nigérians ont la réputation d'être dangereux pour quiconque voudrait les démasquer, pouvant aller jusqu'à tuer. Des cas de meurtres ont ainsi été signalés au Nigeria où un ressortissant américain qui s'était fait arnaqué fut tué à son arrivée au Nigeria. Cette réputation rend ainsi difficile l'approche de ces individus. Ils passent des heures entières dans ces lieux devant des ordinateurs à la recherche d'éventuelles victimes. Agés d'un peu plus de la trentaine en général et de présentation très soignée, ils passent pour d'honnêtes personnes, et bien plus pour ceux dont les "affaires" marchent et qui réussissent à satisfaire leur goût du luxe (voiture, bijoux, vêtements de marque etc.). Il faut noter que très souvent, ces cybers escrocs n'exercent aucune autre activité ; ils consacrent donc tout leur temps à l'escroquerie. Cela se justifie par l'importance des capitaux en jeu qui se chiffrent en millions.

Les nationaux

Appartenant généralement à des familles économiquement nanties, ils ont ainsi les moyens de s'offrir de longues heures de connexion à l'internet dans les cybercafés. Un gérant de cybercafé nous a d'ailleurs signifié lors de nos enquêtes que ces jeunes pouvaient investir en moyenne entre l0000 FCFA et 25000 FCFA par mois en temps de connexion sans compter les frais de téléphone, de photocopie et autres. Selon leur quartier et les cybercafés qu'ils fréquentent, ces cybers délinquants ivoiriens se connaissent entre eux, ils sont amis. Quelque peu naïfs par rapport aux escrocs nigérians, ces jeunes parlent à haute voix au cybercafé de leurs affaires et répondent à des appels téléphoniques de leurs victimes. Avec une voix transformée (accent français de France) et un niveau de langue ajusté à celui de la victime (Européenne) pour la circonstance.

Concernant les biens recherchés par ces escrocs ivoiriens, il est à noter que leurs objectifs sont bien moins élevés que ceux provenant du Nigéria. La plupart du temps, ce sont les gadgets électroniques qui sont convoités (téléphones portables, les ordinateurs portables). Quant aux biens en espèce, les sommes visées s'élèvent souvent en des millions de francs. Malgré leur insouciance, approcher ces jeunes et s'imprégner de leurs activités ne s'avèrent pas toujours facile. Ainsi, conscients de l'illégalité de leurs actions, ceux-ci se méfient de toute personne inconnue.

En outre, bien que les techniques standards soient connues de tous les escrocs, certains d'entre eux ont cependant des techniques d'approche individuelle qu'ils refusent de partager avec leurs collègues. Aussi, vouloir intégrer leur réseau pour faire comme eux ne peut être possible que par cooptation d'un des leurs. Comme les escrocs nigérians, ces jeunes ivoiriens sont des adeptes de la grande vie mondaine. C'est pourquoi, la quasi-totalité des gains qu'ils retirent de leurs forfaits, ne servent qu'à faire la fête dans les maquis, boîtes de nuit, bars climatisés et à s'offrir des vêtements de luxe.

Les victimes

La plupart des victimes vivent en Afrique et en Europe. Les francophones et particulièrement les Français sont les cibles privilégiées des cybers escrocs ivoiriens. Cela peut s'expliquer par la proximité des cultures et surtout par le fait qu'ils aient la langue française en commun. On peut aussi croire que ces facteurs linguistiques amènent les escrocs nigérians à ne pas trop viser les pays francophones. En effet, leur anglais très approximatif les discrédite la plupart du temps auprès de leurs potentielles victimes francophones. Les procédures utilisées sont parfois des manœuvres frauduleuses connexes à l'infraction elle-même. Ainsi, les victimes voient leur identité être associée frauduleusement à des actes de cyber escroquerie. Il s'agit notamment, de renseignements personnels relatifs à leur nom, adresse, numéros de téléphone, date de naissance et logo. On parle alors d'usurpation d'identité. On retrouve ce type de victimisation dans les cas d'arnaques à la loterie (les noms de banques où de grandes entreprises sont associées à l'escroquerie). Dans les arnaques à la carte de crédit et aussi dans les cas d'arnaque à la bourse d'étude où c'est l'image d'institutions universitaires (généralement étrangères) qui est utilisée. A côté du secteur privé, nous avons l'administration publique qui est fortement touchée par ces usurpations d'image, notamment au niveau des institutions judiciaires, policières, financières, etc. Les particuliers sont aussi victimes de ces actes d'usurpation d'identité dans les situations d'arnaque à l'annonce, les scams 419 où le cyber escroc se cache derrière ces identités usurpées pour brouiller ses traces.

Voici quelques exemples de personnes qui ont été victimes :

- Un internaute d'origine française s'est fait escroqué la somme de 140 euros par un jeune ivoirien.
- Monsieur Kouassi konan N. Directeur Général d'une société à Abidjan s'est fait escroqué la somme de 200$ US par une ONG fictive dénommée « la compassion ». Cette somme devrait servir à la préparation d'un sommet concernant certains cadres africains aux Etats-Unis.
- Une française a expédié des vêtements de marque qu'elle vendait en ligne vers Abidjan sans jamais recevoir son argent.
- Mme Keita, femme d'affaire vivant à Abidjan a perdu 21.700.000 FCFA dans une escroquerie 419. Elle voulait aider des orphelins en Côte d'Ivoire.

Les méthodes criminelles utilisées

Le « mougou » ou « le Wess »

Cette forme de cybercriminalité est la plus pratiquée en Côte d'lvoire. Le «mougou» ou « le wess » est un procédé qui consiste à aller sur des sites de rencontre, s'inscrire en se faisant passer pour une femme et chercher par cette voie, des amis à travers l'occident en général et la France en particulier, pour un projet de mariage. Les pourparlers au sujet du mariage se déroulent normalement et les échanges de photo sont faits souvent avec la complicité d'une fille. A ce niveau, le futur mari ne trouve pas d'inconvénient pour faire venir à son «âme sœur » les moyens nécessaires pour les préparatifs du mariage, bien attendu ce mariage qui n'aura jamais lieu.

Le format

C'est le niveau le plus élevé du « broutage ». Il embrasse divers domaines à savoir, la religion, les banques et les finances ainsi que les entreprises privées. Par exemple, dans le domaine de la religion, les escrocs créent sur un site Internet sur lequel ils se font passer pour une association religieuse qui recherche des financements pour la construction d'édifices religieux tels que les mosquées ou les églises. Ils prennent le soin d'expédier aux associations ayant les moyens, des photos de vieilles églises ou mosquées d'un quartier précaire en demandant une aide financière en vue de sa réhabilitation. Une fois l'argent expédié, ils attendent une période bien donnée avant d'expédier cette fois une photo qui présente un autre édifice religieux flambant neuf pour prouver leur bonne foi. Cela fait naître la confiance entre les escrocs et ces associations qui n'hésitent plus à mettre la main à la poche pensant qu'elles ont affaire à une association qui œuvre pour le bien-être de leur religion.

L'escroquerie 419 ou fraude 419

La fraude 419 est la toute première forme cybercriminelle pratiquée en Afrique. Elle fut pratiquée par les Nigérians qui ont trouvé refuge dans notre pays pour mener à bien leurs activités car cette infraction était sévèrement réprimée dans leur pays. La dénomination 419 vient du numéro de l'article du code Nigérian sanctionnant ce type de fraude. Les premières escroqueries de ce type sont apparues comme des escroqueries de livraison postale. Mais avec l'émergence des nouvelles technologies, cette escroquerie devient fertile et possède plusieurs facettes.

Un courrier électronique se présente généralement sous la forme d'un courrier non désiré dans lequel une personne affirme posséder une importante somme d'argent et fait de son désir d'utiliser un compte existant pour transférer rapidement cet argent. La personne à l'origine de ce type de courrier demande de l'aide pour effectuer ce transfert, en échange de quoi il offre un pourcentage sur la somme qui sera transférée. Si la victime accepte, on lui demandera petit a petit d'avancer des sommes d'argent destinées a couvrir des frais imaginaires (notaires, entreprises de sécurité etc.) avant que le transfert ne soit effectif ; bien entendu, ce transfert n'aura jamais lieu.

A ces actes de délinquance énumérés s'ajoutent les braquages, l'utilisation de faux documents d'identités, de faux chèque, de fausse monnaie et blanchissement d'argent, le proxénétisme etc.

Quelques mesures préventives

Au niveau des fournisseurs d'accès à l'internet

Au-delà de la coopération entre le public et le privé, il faut mettre en place des dispositions juridiques contraignantes. Il serait intéressant d'exiger une conservation pour un certain délai, des traces numériques auprès des ces entreprises fournisseuses de l'internet. Aujourd'hui, la plupart des sociétés de téléphones mobiles sont devenues des fournisseuses de l'internet. Ces affaires ne sont pas en soi mauvaises, mais les autorités de l'Etat consacrées à ce secteur doivent veiller au contrôle rigoureux de la gestion de l'internet, tant au niveau de ces sociétés qu'au niveau des clients.

Au niveau des cybercafés

Envisager la possibilité de soumettre les cybercafés à une procédure de déclaration auprès du régulateur. Aussi, les amener à signer une charte qui les oblige à enregistrer tout client (nom, prénoms, etc.) et à fournir certaines statistiques sur leurs activités. Créer des dispositions judiciaires permettant d'effectuer des perquisitions dans ces lieux. Ces investigations seront placées sous la tutelle d'un centre national de Cybersécurité. Celui-ci réunira en son sein des experts de divers domaines de compétence qui réfléchiront sur la

problématique de la cybercriminalité. Ce centre permettra en outre d'effectuer, une veille technologique. A cela, peut s'ajouter la création d'une cyberpolice (brigade anti-cybercriminalité) qui est une section ou un département de la police chargée de la surveillance, de la constatation et de la répression des infractions commises via le réseau. Ce genre de structure existe en France. On a par exemple la Police centrale de lutte contre la criminalité liée aux technologies de l'information et de la Communication (OCLCTIC). Ce service de police judiciaire, est le point de contact national en matière de lutte contre la cybercriminalité.

Au niveau des entreprises de transfert d'argent et de transport de colis

Point final du processus d'escroquerie, ces entreprises, par l'entremise de certains de leurs employés, se rendent complices des cybers escrocs dans la récupération de leurs gains. Il faille donc mettre en place des dispositions juridiques les contraignant à garder pendant un certain délai, toutes les traces de leurs transactions. En outre, il faut exiger une certaine rigueur dans la procédure de retrait de tout fonds à leurs caisses.

Une politique de prévention et de coopération

Axée donc sur la sensibilisation et l'éducation des internautes, cette politique de prévention permettra de connaitre les conduites sécuritaires. Il s'agira d'amener les victimes à communiquer en portant plainte et en rendant témoignage de leur victimisation afin d'éviter à d'autres personnes de tomber dans les mêmes pièges. En outre, par une forte communication autour de cette infraction, il est clair que les cybers escrocs ne seront plus libres d'exercer leur forfais. Les informations sur les peines qu'ils encourent pourraient dissuader de potentiels cybers délinquants. Notons que la prévention devra être le fruit, fractions communes des acteurs privés des TIC, des ONG, associations de consommateurs et des services de répression.

Par ailleurs, l'adhésion de la Côte d'Ivoire à la convention de Budapest sur la cybercriminalité serait un grand pas dans la lutte contre ce phénomène interplanétaire qui nécessite une réponse harmonisée. Une telle coopération est une nécessité pour la Côte d'Ivoire, quand on sait que la convention de Budapest représente plus de 80% des infrastructures en matière de réseaux et aussi parce qu'aucune législation viable ne pourrait se concevoir si elle n'est pas compatible ave celles des Etats les mieux outillés. Relevons que concernant l'Afrique, seule l'Afrique du Sud a signé cette convention.

Conclusion

Parler de la cybercriminalité, c'est toucher à une évidence qui ronge l'économie ivoirienne de nos jours. Le point de mire de ce déluge financier c'est Abidjan où l'ampleur de l'internet continue de faire des victimes. Hommes d'affaires, fonctionnaires, commerçants,

etc. tout le monde y laisse sa peau. Le phénomène va au-delà d'un simple effet de mode. Il s'agit d'une stratégie astucieuse bien organisée en vue de se faire fortune sans beaucoup d'effort. La Côte d'Ivoire par l'action des cybercriminels est aujourd'hui un pays à risque. Ainsi à l'instar du Nigeria, où toute transaction en rapport avec son cyberespace ou avec le pays lui-même est systématiquement évitée à cause de sa réputation de pays expert en escroquerie sur l'internet, la Côte d'Ivoire est inscrite sur la liste rouge des pays à ne pas fréquenter "électroniquement". En conséquence, dès lors que vous décidez de faire des achats en Euro via Internet à partir de la Côte d'Ivoire, le vendeur vous ferme automatiquement la porte. Par de nombreux cas de cyber escroquerie menés à partir de notre pays, ce dernier inspire désormais un sentiment de méfiance. Cela est confirmé par le témoignage d'un cybermarchand Européen victime d'une escroquerie à la carte bancaire venant de la Côte d'Ivoire. Il y révèle : *« Depuis ma mésaventure, j'ai supprimé la Côte d'Ivoire sur la liste et de là toute l'Afrique noire ».* Il va donc sans dire que cela aura un impact négatif sur le développement économique du pays. En exploitant les mêmes voies d'accès au marché que les entreprises licites, ces escrocs portent atteinte non seulement aux biens des consommateurs, mais aussi aux intérêts des entreprises. Les investisseurs sont par conséquent réticents à entrer en relation d'affaire avec des entreprises ivoiriennes.

Vu donc la place importante qu'occupe l'internet dans les relations commerciales actuellement, une balkanisation du cyberespace ivoirien serait à coup sûr, d'un préjudice économique incommensurable pour le pays. La cyber escroquerie se présente comme une menace directe au développement de la cyber économie en Côte d'Ivoire.

Références bibliographiques:

Abou E. (1992), « Approche criminologique de la criminalité économique et financière », mémoire de maîtrise, UFR criminologie université d'Abidjan Cocody.

Adia D. M. (2006), « La criminalité astucieuse en Côte d Ivoire: le cas de l'escroquerie 419 à Abidjan ». Mémoire de Maîtrise, UFR criminologie, Université de Cocody- Abidjan.

Akoue Y. C. (1995), « Le piratage informatique à Abidjan », mémoire de maîtrise, UFR criminologie, Université d'Abidjan-Cocody.

Alline J.P. (2003), « Gouverner le crime: les politiques criminelles Françaises de la révolution au XXIe siècle », Paris, Edition l'harmattan.

Centre Ivoirien de Recherche Economique et Sociale (2008), « Analyse économique de la cybercriminalité, forum national sur 1a cybercriminalité ».

Colantonio F. (2001), « criminalité informatique et cybercrime», Dossier, école de criminologie Jean Constant, faculté de Droit, Université de Liège.

Koudou K. R. (1998), « Education et développement moral de l'enfant et de l'adolescent africain (pour ne pas en faire des délinquants) », Edition l'harmattan.

N'guessan K. J. (1998), « la piraterie des œuvres musicales à Abidjan », mémoire de maîtrise, UFR criminologie, Université d'Abidjan-Cocody.

Quere S. (2001), « Les clans criminels Nigérians », mémoire du centre d'étude sur les menaces criminelles contemporaines, Département de recherche sur les menaces criminelles (D.R.M.C.C), Université de Paris II (panthéon- Assas).

Rose P. (1995), « criminalité informatique », éditions Puf, Paris.

Szabo D. (1978), « Criminologie et politique criminelle », libraire Philosophique, Montréal les presses de l'Université de Montréal.