Global Scientific JOURNALS

GSJ: Volume 12, Issue 2, February 2024, Online: ISSN 2320-9186

www.globalscientificjournal.com

# L'EVOLUTION TECHNOLOGIQUE ET SES MULTIPLES FACETTES : COUP D'ŒIL CRIMINOLOGIQUE DANS LES SERVICES FINANCIERS MOBILES « MOBILE MONEY »

Par

**KAZADI KADI MOYO Nicot**

*Informaticien et Criminologue*

Assistant-chercheur / République Démocratique du Congo (RDC)
Tél : +243 84 84 40 494
E-mail : kadykadim.4k@gmail.com



**Résumé**

Dans les pays de l'Organisation pour l'harmonisation du droit des affaires en Afrique (OHADA), la vie des affaires est maintenant marquée par une avancée visible des technologies en matière de circulation des biens et des personnes, ainsi qu'en matière de moyens de paiements. S'agissant en particulier de ces derniers, ils permettent aujourd'hui de payer des biens et services tels que les factures, la scolarité, les commandes de marchés ou tout simplement d'effectuer un transfert ou encore recevoir l'argent à partir de son téléphone portable. Cet ensemble d'opérations économiques effectuées par la voie de la digitalisation téléphonique s'appelle Mobile Money, Mobile Banking ou Argent Mobile, en français.

Malheureusement, en dépit de toutes ces opportunités, les services financiers mobiles sont aussi devenus très vite des relais d'une panoplie inestimable des situations problématiques (criminalité) transformant les acteurs impliqués dans ces services financiers en victimes (Mercy W. Buku et Rafe Mazer, 2017). La criminalité technologique est désormais

une réalité. Elle est d'autant plus dangereuse qu'elle pénètre au sein des familles, là où la délinquance ordinaire ou classique n'avait pas accès jusqu'à présent (Boos, R., 2016).

Ce travail vise à déceler les différentes formes des situations-problématiques qui se vivent dans les services financiers mobiles (Mobile Money). Etant une étude criminologique qui se veut empirique, le travail se dote l'objectif de faire une analyse sur les comportements gênants qui se vivent dans ces services financiers. En d'autres termes, il est question ici de donner un sens ou des sens aux situations-problématiques (criminalité) que vivent les acteurs impliqués dans les services financiers mobiles. Ceci dans le but de comprendre comment ces situations-problématiques se construisent et se réalisent.

Pour cela, nous référant aux données de terrain, plusieurs formes de criminalité se dégagent entre acteurs impliqués dans les services financiers via le téléphone portable, dont les dénominations relèvent de la catégorie institutionnelle ayant reçu chacune d'elles une signification lors des entretiens avec les acteurs de terrain. Parmi ces formes de criminalité non exhaustives, les plus marquantes sont : « le piquage », « le dribbling », « le marimisage», « l'accidentage », « l'évasion » et « la dotation d'identité ».

**Mots clés** : Criminalité, Mobile Money, Technologies de l'information et des communications (TIC), Situation-problème.



## Abstract

In the countries of the Organization for the Harmonization of Business Law in Africa (OHADA), business life is now marked by a visible advance in technologies in terms of the movement of goods and people, as well as in terms of means of payment. Regarding the latter in particular, they now make it possible to pay for goods and services such as bills, schooling, market orders or quite simply to make a transfer or even receive money from one's account. cellphone. This set of economic operations carried out through telephone digitalization is called Mobile Money, Mobile Banking or Argent Mobile, in French.

Unfortunately, despite all these opportunities, mobile financial services have also very quickly become relays for an invaluable range of problematic situations (crime) transforming the actors involved in these financial services into victims (Mercy W. Buku and Rafe Mazer, 2017). Technological crime is now a reality. It is all the more dangerous because it penetrates into families, where ordinary or classic delinquency had no access until now (Boos, R., 2016).

This work aims to identify the forms of problem situations experienced in mobile financial services (Mobile Money). Being a criminological study which aims to be empirical, the work has the objective of carrying out an analysis of the embarrassing behaviors that occur in these financial services. In other words, it is a question here of giving meaning or meanings to the problematic situations (crime) experienced by the actors involved in mobile financial services. This with the aim of understanding how these problematic situations are constructed and realized.

For this, referring to field data, several forms of crime emerge between actors involved in financial services via mobile phones, the names of which fall under the institutional category having received each of them a meaning during the interviews with the actors. ground. Among these non-exhaustive forms of crime, the most notable are: “stealing”, “dribbling”, “marimisage”, “accident”, “escape” and “identity granting”.

**Keywords :** Crime, Mobile Money, Information and communications technologies (ICT), Problem situation.



## Introduction

« Le millénaire actuel a vu la consécration des technologies numériques (sous le vocable des [nouvelles] technologies de l’information et de la communication [NTIC])[1] comme la fin du Moyen Âge a vu celle de l’imprimerie » (Chawki, M., 2006). Cette évolution technologique considérable se manifeste dans tous les secteurs d’activités : les transports, la communication, la santé, ou encore la vie des affaires.

Dans les pays de l’Organisation pour l’harmonisation du droit des affaires en Afrique (OHADA) par exemple, la vie des affaires est maintenant marquée par une avancée visible des technologies en matière de circulation des biens et des personnes, ainsi qu’en matière de moyens de paiements. S’agissant en particulier de ces derniers, ils permettent aujourd’hui de payer des biens et services tels que les factures, la scolarité, les commandes de marchés ou tout simplement d’effectuer un transfert d’argent à partir de son téléphone portable. Cet ensemble

[1] Les expressions « technologies de l’information et de la communication (TIC), « nouvelles technologies de l’information et de la communication » (NTIC) ou encore « information technologies » (IT) désignent tout ce qui relève des techniques utilisées dans le traitement et la transmission des informations, principalement l’informatique, l’internet et les télécommunications.
[Source : http://www.techno-sciences.net/?onglet=glossaire&definition=10714 (consulté le 17 Octobre 2022)]

d'opérations économiques effectuées par la voie de la digitalisation téléphonique s'appelle communément le Mobile Money, Mobile Banking ou Argent Mobile, en français.

Cette mise en place de systèmes de paiement par téléphone mobile a eu notamment pour conséquence ; des centaines de millions de citoyens auparavant coupés de tous services financiers sont à présent capables de réaliser des paiements électroniques instantanés à bas coût (Aucante, M., 2020). C'est à ce titre qu'African banking forum précise que près de 70% de la population africaine utilise aujourd'hui le téléphone mobile. Selon toujours la même source, les technologies de l'information et de la communication contribuent à hauteur de 18 milliards de dollars américains comme inclusion financière sur le continent africain.

De même, à travers cette digitalisation, nous assistons à une véritable indépendance du consommateur. Celui-ci n'est plus obligé de parcourir des kilomètres afin d'effectuer une opération auprès des banques ou des établissements financiers. Cela fait dire à Estelle Brack que « le client devient davantage un acteur de sa propre relation avec l'argent » (Brack, E., 2016).

Le mobile money, encore appelé mobile banking, ou encore « monnaie mobile » n'a pas de définition précise. Elle peut néanmoins être appréhendée comme l'ensemble des services financiers par téléphone portable, offerts par les banques. Il s'agit, principalement dans ce cas, des services de consultation de solde, de paiement de factures et de transfert d'argent (Chaix, L. et Torre, D., 2015). Pour ce même auteur (Chaix, L., 2013), les services monétaires par téléphone mobile, constituent une réelle opportunité pour accélérer la croissance et le développement socio-économique car, estime-t-il, ces services offrent de nouvelles possibilités de mieux assurer l'accès aux services financiers, contrairement aux prestataires de services bancaires et financiers traditionnels.

Malheureusement, en dépit de toutes ces avancées significatives et opportunités offertes, les services financiers mobiles sont aussi devenus très vite des relais d'une panoplie inestimable des situations-problèmes ou problématiques[2] (Pires, A., 1995) transformant les acteurs impliqués dans ces services financiers en victimes (Mercy W. Buku et Rafe Mazer, 2017). Tous les progrès génèrent aussi de nouvelles fragilités et vulnérabilités propices aux

[2] Ce sont des situations contraires aux règles ou normes sociales préétablies : la déviance, le crime, la délinquance, etc. les situations qui gênent au moins un seul acteur qu'il y ait les normes ou pas. Cette notion a été proposée dans le cadre de la perspective abolitionniste de Louk Hulsman et de la nouvelle criminologie clinique de l'École de Louvain (Debuyst, 1983). Son but premier est de permettre de décrire certains événements, certains conflits, etc. sans utiliser immédiatement une notion morale ou, pire encore, juridico-pénale qui introduit souvent une tendance à vouloir expliquer la situation d'une certaine manière et à présupposer que l'intervention pénale (répressive) est la manière « adéquate » de résoudre le problème. La notion de situation-problème désigne simplement le fait que pour au moins un acteur quelconque une situation donnée est vécue ou perçue comme « créant un problème » ou comme étant négative, inacceptable, indésirable.

menaces ou aux risques, car ils aiguisent l'imagination des criminels (Leman-Langlois, S., 2006). La criminalité technologique est désormais une réalité. Elle est d'autant plus dangereuse qu'elle pénètre au sein des familles, là où la délinquance ordinaire ou classique n'avait pas accès jusqu'à présent (Boos, R., 2016).

Ce travail vise à déceler les situations-problématiques qui se vivent dans les services financiers via mobile money. Etant une étude criminologique qui se veut empirique, le travail se dote l'objectif de faire une analyse sur les formes de criminalité qui se vivent dans ces services financiers. En d'autres termes, il est question ici de donner un sens ou des sens aux formes des situations-problématiques (criminalité) que vivent les acteurs impliqués dans les services financiers mobiles. Ceci dans le but de comprendre comment ces situations-problématiques se construisent et se réalisent.

**Méthodologie**

En sciences sociales, faire du terrain ou mieux se soumettre à l'épreuve du terrain suppose pour le chercheur de casser les cloisons de son bureau, aller rencontrer des personnes dans leurs milieux de vie, de travail ou encore milieux naturels, les voir faire ou faire avec elles, le faire parler et parler avec elles sur ce qu'elles font, vivre de relation, des situations, des évènements (Tshinyama Kadima, I. 2009).

Cet article dont l'objet est l' :« Analyse des formes de criminalité dans les services financiers via le téléphone portable : Mobile Money », s'applique sur les données de terrain récoltées auprès des usagers des services financiers mobiles de la ville de Lubumbashi, en République Démocratique du Congo.

Pour mieux appréhender l'objet sous étude, nous avons procédé par une immersion tout à fait méthodique dans l'univers du terrain de recherche à travers les acteurs impliqués dans le phénomène à étudier, c'est-à-dire la criminalité[3] dans les services financiers via mobile money. Parmi ces acteurs, quatre catégories ont été identifiées dont, d'une part les acteurs internes qui sont les banquiers et les opérateurs de téléphonie mobile (y compris leurs agents) et, d'autre part, les acteurs externes qui sont les vendeurs du service ainsi que les clients ou consommateurs des services financiers mobiles. Toutes ces personnes ont été rencontrées différemment selon le rôle que chacune d'elles joue dans les services financiers mobiles. De ce

[3] Par criminalité il faut s'entendre un : « Ensemble des actes criminels commis dans un groupe social donné au cours d'une certaine période » (AEBI M. F.,1999).

fait, durant nos descentes de terrain, nous nous sommes conformés à la réalité de chaque participant.

L'étude étant du type qualitatif, nous avions le choix entre l'échantillonnage par cas unique et l'échantillonnage par cas multiples. Nous avons à cet effet porté notre choix sur le mode d'échantillonnage par cas unique choisi par « effet boule de neige ou chaîne » qui consiste à identifier « de bons cas grâce à des personnes qui connaissent d'autres personnes ayant des cas riches en informations » (Miles et Huberman, 2003).

Nous avons pour cela établi les premiers contacts avec les personnes ressources de chaque catégorie d'acteurs ciblée par notre recherche en fonction de leur acceptation et leur disponibilité. A l'issue de différents entretiens avec les premiers acteurs disponibles, nous avons eu l'opportunité d'entrer en contact et de rencontrer d'autres personnes ressources en fonction de leur apport informationnel utile pour le décryptage de notre objet de recherche.

C'est de cette manière que nous sommes arrivés à avoir des entretiens avec les différents acteurs de ces services (mobile money) qui ont déjà été victimes. Par conséquent, l'angle pouvait varier selon le lieu où l'enquêté (acteur) pouvait se trouver et surtout où apparaissait la disponibilité de nous fournir les données nécessaires à l'objet de recherche.

Pour garantir l'anonymat des acteurs de terrain, nous avons décidé d'user des pseudonymes en lieu et place de leur identité nominale. Précisons qu'au moment de la récolte des données, les enquêtés ne se sont pas prononcés en rapport avec l'anonymat. Par conséquent, cette tâche est revenue à nous-mêmes. À ce titre, les clients dans les services financiers mobiles (mobile money) sont ici présélectionnés parmi les chefs-lieux de provinces de la République Démocratique du Congo (RDC), les vendeurs de ces services par contre, sont les provinces du même pays tandis que les agents sont présélectionnés parmi les communes de la ville de Lubumbashi et les fonctionnaires judiciaires (officiers et inspecteurs de police judiciaire) sont présélectionnés par l'anonymat RDC suivi de l'indice (1- 6) tandis que les opérateurs de téléphonie mobiles et leurs services financiers sont désignés par leurs noms respectifs : Vodacom (M-Pesa), Orange (Orange money), Airtel (Airtel money) et Africell (Afri money).

**Regard criminologique sur les services financiers mobiles : Mobile Money**

Plusieurs formes de criminalité se dégagent entre acteurs impliqués dans les services financiers via le téléphone portable à Lubumbashi, dont les plus marquantes sont : le piquage, le dribbling, le marimisage, l'accidentage, l'évasion et la dotation d'identité.

Bref, notre corpus empirique présente huit formes de criminalité dont les dénominations relèvent de la catégorie institutionnelle ayant reçu chacune d'elles une signification lors des entretiens avec différents acteurs de terrain. La liste n'étant pas exhaustive.

## 1. « Le piquage »

Le concept « piquage » désigne respectivement l'action de piquer qui veut dire : percer ou entamer légèrement avec un objet pointu, ce qui signifie autrement dérober (Dictionnaire universel, 2010). Parlant à cet effet de l'aspect criminogène dans les services financiers par téléphonie mobile, piquer devient l'action par laquelle une personne non autrement identifiée se permet de soustraire dans le compte mobile de sa cible (future victime) une somme d'argent à son insu et par conséquent, celui-ci ne se rendra compte qu'après l'opération.

Par ailleurs, cette forme de criminalité est possible ou est réalisée par une personne censée connaître bien sa cible, c'est-à-dire une personne proche de la victime, qui connaît non seulement sa situation économique mais également détient des informations sur les coordonnées relatives à son compte mobile, en l'occurrence son PIN[4] ou code confidentiel.

Après avoir été piqué, monsieur Kamina, utilisateur et client dans les services financiers mobiles déclare ceci :

> *« Avant je ne comprenais absolument rien. Il m'arrivait que quand j'ai quelque chose dans le compte, je trouve des messages soit de retrait soit des transferts. Cela me dépassait énormément. Un jour, j'avais dit cela à un vendeur mais qui ne m'avait pas dit les choses clairement. Arrivé un moment, ma grande sœur m'appelle pour me demander si j'avais reçu l'argent qu'elle m'a envoyé. A mon grand étonnement, je luis dis que je n'avais pas reçu l'argent de sa part. Alors elle insiste pour dire vérifie tes messages, je t'ai envoyé 20 USD, d'ailleurs avec mon propre numéro.*
>
> *Directement, je prends le téléphone et curieusement je constate qu'elle avait raison. Je vois un message de réception de 20 USD mais le solde avait un montant insignifiant c'est-à-dire moins de 20 USD. J'étais bouleversé. Ce n'est qu'après un moment que je m'étais rappelé qu'un de mes fils avait mon téléphone avec lui. Je l'appelle pour lui demander s'il avait pris mon argent, celui-ci refuse. C'est quand j'avais haussé le ton qu'il avait fini par avouer que c'est lui qui avait transféré l'argent de mon téléphone vers un autre numéro. Donc, toutes les fois que je trouvais les messages de transfert, c'était lui ».*

[4] De l'anglais, Personal Identification Number ou NIP en français : Numéro d'Identification Personnelle

Notons également que le passage à l'acte du piquage peut être réalisé de deux manières :

- **A distance** : avec l'évolution exponentielle actuelle de la technologie, il est tout à fait possible que quelqu'un qui est à distance de sa victime puisse parvenir à réaliser son projet via des manipulations complexes. C'est ce qui évoque la problématique de la territorialité dans le domaine de la cybercriminalité. C'est le cas aussi avec les agents officiels qui ont la possibilité d'accéder à partir de leurs machines dans le compte d'une personne une fois le mot de passe fourni. Ceci s'approuve par le fait que, lorsqu'un client décède par exemple, les proches ont droit d'aller chez l'opérateur de téléphonie mobile où il était abonné afin de récupérer l'argent moyennant les pièces justificatives notamment l'acte de décès, la carte d'électeur, le PIN…

Pour démontrer que les agents officiels ont la possibilité de recourir au piquage, monsieur Haut-Katanga, vendeur des services financiers par la téléphonie mobile relate ce qu'il a vécu en ces termes :

> *« C'est possible on a déjà eu à le faire. Un ami était décédé brusquement comme tu l'as dit là et on l'avait fait. Nous étions partis à la Shop avec tous les documents justifiants le décès et l'argent nous était remis en le transférant dans le numéro de l'un des nôtres ».*

- **Sur place** : dans ce cas, il s'agit d'une personne qui vit avec la cible et qui connaît très bien son PIN. Alors, en l'absence ou pendant que sa cible s'occupe d'autres affaires, le déviant peut prendre son téléphone et faire le transfert comme cela a été le cas de monsieur Kamina cité ci-haut.

Comme nous l'avons dit précédemment, le « piquage » peut être exécuté soit par une personne proche de la victime, soit par une personne se trouvant à distance. Alors, qu'il s'agisse d'un acte commis à distance ou sur place la responsabilité pour ce crime d'être commis ou pas incombe beaucoup plus à la victime qu'au déviant. Et donc, le facteur le plus important pour déterminer si un crime sera commis, n'est pas la présence d'un criminel expérimenté ou une personne socialement déviante, mais s'il y a une opportunité pour un crime d'être commis (Cohen, E.L. et Felson, M., 1979).

Voilà pourquoi nous demandons à tous les utilisateurs du mobile money de rester toujours confidentiels en ce qui concerne les informations relatives à leurs comptes mobiles. Ceci constituera un mode control aussi efficace c'est-à-dire un gardien de prévenir les violations criminelles propices à la commission d'un crime (Cohen, E.L. et Felson, M., 1979).

**2. « Le dribbling »**

Du verbe « dribbler » qui veut dire : berner ou tromper (Dictionnaire universel, 2010), le dribbling est l'action par laquelle une personne dans la plupart des cas, inconnue, contacte l'autre (cible) par appel direct ou par SMS[5] en racontant des flatteries (récompenses, bonus) ou des histoires à compassion en usant des méthodes un peu plus expérimentées. D'habitude, les appelants se présentent comme des agents des opérateurs mobiles money du client (abonné) ou encore comme des employés des sociétés qui font les tombolas gagnantes. Et quand ils appellent c'est pour dire au client que soit son compte mobile a des problèmes techniques qu'il faut décanter ou encore que le client venait de gagner à une tombola.

Par la suite ils vont demander au client (future victime) de faire une série des manipulations en appuyant sur les touches du téléphone. Or, ce qu'il faut savoir est que chaque touche du téléphone émet un son différent de l'autre. Le souci de l'appelant est non que sa cible lui fournisse les informations nécessaires telles que le mot de passe verbalement mais qu'il arrive plutôt à capter ou détecter le PIN du client afin de vider son compte. C'est en quelque sorte une pratique qui exploite les faiblesses psychologiques et sociales pour permettre d'obtenir quelque chose de la personne ciblée. C'est exactement de l'ingénierie sociale dans le monde de cybercriminalité.



La question que l'on peut se demander ici est celle de savoir comment les criminels obtiennent les numéros mobiles money des abonnés ?

Deux méthodes s'imposent :

a. La première et la plus simple est que lorsqu'un client va soit pour faire un dépôt ou un retrait mobile money, les vendeurs du service (mobile money) auprès de qui il fait les transactions restent avec les numéros des clients et d'autres écrivent cela dans leurs cahiers ou carnets mais, il arrive que certains d'entre eux revendent ces cahiers-là auprès des individus mal intentionnés leur permettant ainsi d'accéder aux numéros des abonnés ;
b. La deuxième méthode concerne certains employés (agents officiels en fonction ou anciens) de l'opérateur mobile money qui dérobent les fiches contenant les numéros des abonnés et les revendent auprès des individus leur permettant ainsi d'accéder aux numéros des abonnés.

[5] Short Message Service (Court Message Textuel) : est un texte écrit envoyé à partir d'un téléphone mobile vers un autre téléphone mobile

Pour avoir été dribbler, monsieur Tanganyika, vendeur du mobile money relate ce qui suit :

> *« Au fait, j'avais de l'argent dans mon compte Airtel Money, un montant de 1.300.000 FC. Alors je reçois un coup de téléphone d'un inconnu qui se présente comme un agent. Il me dit que je venais de gagner un bonus sur mon compte. D'où, ajoute-t-il, pour utiliser cet argent ou pour que cet argent soit opérationnel, il fallait que je valide cela avec un code que lui, allait me donner. D'abord il m'a posé la question de savoir si j'ai un autre téléphone par lequel il peut me rappeler afin que le téléphone dans lequel il y a la carte sim du compte puisse être libre pour permettre de faire les manipulations et ma réponse était non. Pour cela, il me demandera de mettre mon téléphone en mains libres (hauts parleurs).*
>
> *Il m'a dicté, j'ai tapé. Après avoir terminé à manipuler ce code, il m'a dit que l'opération était terminée et donc je pouvais maintenant utiliser le bonus et m'a remercié pour ma fidélité au réseau Airtel puis a raccroché. Après avoir raccroché, le temps pour moi de vérifier dans mon compte pour voir le bonus que je venais de gagner, curieusement je vois un message du Service qui me dit que je venais de faire un transfert de 1.250.000 FC vers un numéro que je ne connais pas. C'est au moins ça ».*



Il faut noter que l'on distingue deux types de dribbling :

- *Le dribbling avec rationalité* : c'est quand la future victime se fait dribbler en espérant gagner en retour quelque chose auprès de son bourreau. Le gain attendu par la future victime peut être promise ou non.
- *Le dribbling sans rationalité* : c'est quand la future victime se fait dribbler sans avoir à l'esprit qu'il gagnera quelque chose dans la transaction. Et donc, elle le fait par empathie, curiosité ou ignorance.

Statistiquement parlant, le dribbling avec rationalité présente plusieurs cas que celui sans rationalité. Cet état des choses se justifie par le simple fait que l'homme étant naturellement rationnel (Debuyst C.,1990), l'individu ravisseur profite plus de cet état d'esprit pour convaincre sa cible attrayante. Par ailleurs, la rationalité de la part de la cible devient une brèche par laquelle le déviant exploite pour arriver au bout c'est-à-dire à la réalisation de son projet macabre.

Ici, dans les manipulations kilométriques qui lui sont dictées, la victime transfère elle-même sa réserve financière de son compte vers un autre sans le savoir.

**3. « Le marimisage »**

Du swahili de Lubumbashi « marimi » qui veut dire « non avisé », « imprudent », « ignorant », « non méfiant », le marimisage est une action par laquelle le déviant profite de l'imprudence, de manque de souplesse ou de manque de méfiance ou carrément de manque de connaissance de sa cible pour passer à l'acte. Le marimisage est beaucoup pratiqué pendant que la personne (future victime) donne son téléphone au convoiteur tout en lui communiquant même son PIN.

Cette forme de criminalité est fréquente surtout lors des retraits de fonds auprès des agents par les clients qui n'ont pas assez d'expériences dans les manipulations téléphoniques (technologiques). Voici les représentations sociales (Jodelet, D.,2003) que maman Kolwezi, cliente dans le mobile money, se fait de son vendeur des services, monsieur Tshopo.

> *« Mon fils, tu vois ces gens auprès de qui nous avons l'habitude de récupérer l'argent à travers le téléphone, sont des grands voleurs. Comme tu le sais, nous vos mamans, n'avons pas une connaissance approfondie dans la manipulation des téléphones. Un jour, j'étais allée auprès d'un cabinier pour retirer de l'argent. Je lui donne le téléphone puis me demande le mot de passe.*
>
> *Un autre jour, je suis encore partie, il me donne et un autre jour encore. Maintenant, arrivé un autre jour, je suis allée pour retirer. Avant, ton grand frère qui m'avait envoyé l'argent m'avait déjà dit qu'il avait envoyé 50.000 FC. J'y arrive, comme il était déjà habitué à mon téléphone, me donne 30.000 FC. Je lui dis que dans le téléphone, il y a 50.000 FC et que j'avais besoin de retirer toute la somme. Avec insistance, il me dit qu'il n'y avait que 35.000 FC et qu'il y avait possibilité de retirer au moins 30.000 FC sans oublier les frais de retrait. Puis j'appelle ton grand frère qui avait envoyé l'argent pour lui dire ce qui était passé, il me demanda de le lui passer au téléphone, il lui gronda sérieusement par la suite me dit de ne plus y aller car le monsieur m'avait volé. C'est un voleur ».*

Monsieur Kamalondo, à son tour, relate le phénomène de cette manière :

> *« Vous savez avec ces histoires-là de monnaie numérique, la meilleure sécurité c'est le mot de passe du compte mobile ; eeh ! Ce code-là qui vous permet d'accéder au compte. Alors un jour j'avais fait cette imprudence là j'étais en déplacement à Kinshasa. Comme je ne me sentais pas du tout bien et que j'étais dans le besoin*

*d'argent ; j'appelle un neveu là je lui donne le téléphone ainsi que le mot de passe pour qu'il récupère un peu d'argent et pour lui c'était une opportunité de me voler.*

*Pour moi, le neveu ne pouvait rien faire ce qui fait que je n'avais même pas vérifié le solde quand il était rentré. Mais à ma grande surprise ; deux jours après quand je voulais maintenant acheter la marchandise, je me rends compte que le solde n'était pas exact. Au total, dans le compte avant le retrait, il y avait 1.800.000 FC. Pour moi, après avoir retiré 200.000 FC ; normalement il fallait qu'il reste dans le compte au moins 1.600.000 FC. Ce n'est qu'après deux jours que je m'étais rendu qu'il y avait un manquant de 200.000 FC et plus. Cette situation-là m'avait tellement affecté. Voilà au moins le mauvais souvenir que je retiens du mobile money parce qu'à un certain moment, je m'étais dit, si par exemple j'avais avec moi l'argent en espèces peut être que cela ne pouvait pas m'arriver ».*

Le marimisage est aussi possible dans le cas des vendeurs imprudents qui se contentent seulement du message entrant (dépôt, retrait ou paiement de services) sans prendre le temps de vérifier le solde. Tel est le cas de monsieur Lualaba qui relate ce qu'il vit au quotidien en cette matière :

*« C'est pourquoi tu vas constater que j'insiste sur la confiance et la souplesse de soi. Supposons que le vendeur aussi ne soit pas souple, le client peut avant de retirer vous parler par exemple d'un montant donné (20.000 FC par exemple) mais lors du retrait, il ne retire plus la somme dictée mais plutôt une autre inférieure à celle dictée (15.000 FC). Ce genre des cas sont fréquents.*

*La plupart des clients quand ils se retrouvent dans ce genre des cas, ont l'habitude de dire que le montant dicté est celui qui était dans le compte et qu'oubliant il fallait aussi les frais de retrait, c'est pourquoi il y a eu cela. Au fait, tout ça ne sont que des raisons on ne refuse pas mais ce qui est inquiétant est que si le vendeur n'est pas prudent, c'est-à-dire sans vérifier le message et qu'il donne seulement la somme dictée au lieu de la somme retirée véritablement là il perd non ? Ce sont des cas vrais, il y a des clients qui viennent aussi nous voler comme ça».*

A la question de savoir comment certains clients arrivent à communiquer leur PIN à d'autres personnes, monsieur Tshwapa, vendeur du service mobile money rejette la responsabilité aux victimes :

*« Même toi-là comment tu peux arriver à donner ton mot de passe à quelqu'un. C'est quand même grave. Tel que tu me vois là, j'ai beaucoup de mots de passe des*

*gens. Surtout les mamans, tu vas voir elle arrive puis te donne et le téléphone et le mot de passe, tu retires pour elle. Si j'étais voleur par exemple, tu ne vois pas que j'ai la possibilité de gagner de l'argent comme ça. Pour te prouver que ce que je dis là est vrai, je te communique aussi le mot de passe d'une de mes clientes : « 1070 » et comme tu ne le connais pas, tu ne feras rien mais moi il suffit que j'ai son téléphone dans mes mains et directement j'ai l'argent s'il y en a bien sûr ».*

Comme nous le démontrent les propos de nos enquêtés et tel que nous l'avons défini, le marimisage est la résultante d'une confiance inconsciente que la personne manifeste à l'endroit des tiers. Cela par mauvaise compréhension des choses ou quasiment par manque des connaissances du système financier moderne qu'elle utilise.

**4. « L'accidentage »**

Issu du mot « accident » qui est un événement imprévu, survenant brusquement et qui entraîne des dommages, l'accidentage devient une situation problématique qui arrive chez une personne indépendamment de sa volonté. Cette forme de criminalité survient très souvent dans le cas où le téléphone portable qui est l'instrument duquel l'argent est dépendant à partir de la carte SIM, c'est-à-dire contenant la liquidité, est soit volé, soit perdu.

Monsieur Lodja, utilisateur du mobile money, relate ce qui lui est arrivé à cause de l'accidentage :

*« Tu sais quoi ? La société actuelle et ses réalités, nous demande de fournir les efforts d'être à la page comme aiment bien le dire les intellectuels (rigolade et frottement des mains). Et parfois même les business que nous faisons aussi nous exigent d'avoir les comptes mobiles qui font que quand tu n'en as pas, tu seras considéré comme quelqu'un qui ne vit pas dans ce siècle. Pour cela, je m'étais décidé à ce qu'on ouvre pour moi un compte mobile monnaie pour permettre de réserver le peu que je trouve journellement.*

*Pour ce qui est de mon cas, j'avais quelque chose de considérable dans mon compte (675.000 FC). Un jour, nous avions deuil, notre ami avait perdu son épouse. Le jour de l'enterrement, à la morgue, j'avais le téléphone avec moi. Alors, quand le moment de sortir le corps de la défunte était venu, c'est nous qui allions soulever le cercueil, j'avais pris le téléphone pour le mettre dans la poche de la jaquette que je portais ce jour-là. Je suppose que c'est pendant les encombrements que quelqu'un avait profité pour me voler le téléphone. Quand nous étions arrivés au cimetière et à un moment donné il fallait qu'on appelle le chauffeur qui nous avait*

*transporté pour rentrer maintenant, je vérifie dans la poche de la jaquette je ne trouve pas mon téléphone. Mon frère, la tête m'avait bougée ce jour-là, j'avais même regretté pourquoi j'étais parti à ce deuil-là ».*

Comme son nom l'indique, l'accidentage est un événement imprévisible, incertain, qui arrive brusquement chez la personne. En outre, ce qu'il faut noter est que depuis l'avènement du mobile money, le vol des téléphones portables est devenu très récurrent simplement parce que le délinquant connaît aujourd'hui que cet outil procure actuellement un double avantage : le téléphone lui-même en tant que matériel et en plus l'argent qui s'y trouve étant donné que plusieurs personnes aujourd'hui disposent au moins d'un compte mobile money.

**5. « L'évasion »**

Du verbe « évader », l'évasion est le fait que quelqu'un ou quelque chose échappe au contrôle de son gardien. Dans le cas d'espèce, par évasion, nous entendons le fait que quelqu'un arrive à perdre soit le tout ou partie de sa réserve mobile (mobile banking) dans une situation de crise (accidentage) par exemple.

L'évasion est donc la conséquence de l'accidentage. Après avoir été victime de l'accidentage, monsieur Lodja donne l'explication de ce qui s'en était suivi :

*« C'est ainsi que j'étais parti à la shop de Vodacom, j'arrive là j'explique comment le problème s'était déroulé. Ils m'avaient demandé toutes les coordonnées (carte d'électeur, mot de passe du compte) après ils me demandent de repasser après 24 heures. Après ces 24 heures, j'arrive là, ils me diront qu'ils avaient réussi de récupérer l'argent mais malheureusement ce n'était plus toute la somme mais seulement 450.000 FC qu'ils m'avaient remis. Selon leurs explications, le monsieur qui avait volé le téléphone, avait déjà retiré les 225.000 FC. Ainsi, j'étais obligé de récupérer ne fusse que ce qu'ils m'avaient remis ».*

Illustrant tous les deux cas (Accidentage et Evasion), madame Kananga relate l'histoire que son coreligionnaire Mbuji-Mayi, utilisateur du mobile money, avait vécue :

*« L'autre problème, c'est celui d'un frère avec qui, nous partageons la même foi. Ce frère-là avait perdu son téléphone dans lequel il y avait d'argent. Il était parti au niveau du service où on avait retiré l'argent qui y était mais ce n'était plus la totalité ; il n'avait eu que la moitié de la somme qui y était ».*

Il ressort des propos des enquêtés que l'évasion est une forme de criminalité perpétrée par les agents officiels des opérateurs mobiles. Cela s'explique par le simple fait qu'un

déviant, rationnel qu'il est, après avoir chiper ou ramasser le téléphone puisse d'abord ne récupérer qu'une partie de la somme globale et laisser une autre comme si le mobile banking (réserve mobile) lui appartenait. Ceci est non seulement inconcevable mais aussi incompréhensible.

Pour cela, nous essayons de comprendre que ces agents profitent de la situation vécue par la personne pour en tirer aussi gain. Et donc, certaines formes de criminalité dans le Mobile Money ne sont possibles que lorsqu'il y a une opportunité qui se présente. Dans leur théorie, Cohen, E.L. et Felson, M., (1979), explique ce fait de cette manière : « Le facteur le plus important pour déterminer si un crime sera commis n'est pas la présence d'un criminel expérimenté ou une personne socialement déviante, mais s'il y a une opportunité pour un crime d'être commis ».

Ce même cas d'opportunité est parfois vécu de la manière suivante :

> *« Oui, quand je suis allé là-bas à leur shop sur chaussée ; je trouve les agents qui vendent dehors. A mon arrivée, je vois déjà un monsieur qui arrive et me dit : « maman, qu'est-ce qu'on peut faire pour vous ? » je lui pose le problème ; je lui dis que mon compte Airtel money était bloqué et je voulais qu'il soit débloqué. Il dit que c'était un petit problème. Et qu'il pouvait le faire. Il m'amène quelque part, on s'assoit ; il me demande le numéro de téléphone ainsi que le mot de passe que j'utilisais ; le vrai. Je lui donne et il prend aussi mon téléphone et commence à manipuler.*
>
> *Après avoir manipulé mon téléphone, je le vois prendre son téléphone et appelle et je l'entendais dicter mon numéro et le mot de passe à celui que lui, avait appelé. Quelques minutes après, vraiment il n'avait pas duré et puis me remet mon téléphone et me dit que je rentre à la maison et que dans 24 heures le compte sera débloqué. J'avais accepté et puis me demande sa main d'œuvre ; je lui paie et je suis partie. Et 24 heures après comme il l'avait dit, je vois un message entrer dans mon téléphone pour me dire que mon compte venait d'être débloqué. Mais curieusement, quand j'entre dans le compte, il n'y avait rien comme argent. Tout était pris. Voilà ce qui m'était arrivé ».*

Madame Kinshasa renchérit :

> *« Les gens que j'avais expliqué m'avaient dit que c'est lui qui m'avait volé. Il avait donc profité de la panne pour me voler ».*

L'« évasion » est aussi possible même quand le téléphone n'est pas perdu ou volé. Certains clients arrivent à perdre leur réserve mobile pendant que le téléphone est là. C'est une situation qui est parfois liée à la qualité du service mobile money. Néanmoins, cette forme de criminalité présente un nombre réduit des cas.

**6. « La dotation d'identité »**

Le concept « dotation » vient du verbe « doter » qui veut dire assigner, fournir ou attribuer quelque chose à quelqu'un (Dictionnaire universel, 2010). Contrairement à l'usurpation d'identité qui est une technique consistant à s'approprier ou à utiliser l'identité d'une tierce personne pour des fins mafieuses (Olivier I., 2008), la dotation d'identité devient son opposé.

La dotation d'identité est une forme de criminalité récurrente dans les services financiers mobiles qui consiste pour les agents officiels ou débrouillards et même vendeurs du service mobile money d'enregistrer sous leurs identités les cartes SIM qu'ils vendent et parfois même les comptes mobiles des clients. Ceci se fait lors de l'ouverture du compte où ces acteurs habiletés à ouvrir les comptes mobiles, mettent leurs identités en lieu et place de celle du propriétaire et ce, pour des raisons parfois inavouées.

Cette forme de criminalité pose des sérieux problèmes lors du déblocage par exemple du compte mobile ou de l'activation d'une SIM blanche en une SIM active où l'identité du propriétaire par pièce d'identité officielle est toujours exigée. A ce moment-là, l'identité du compte mobile ou de la SIM active sera différente de la vraie identité de la personne. Par conséquent, l'opération ne sera pas possible parce que pour les agents officiels habiletés à faire ce travail, cela sera compris comme une tentative de fraude ou de vol.

La plupart des clients ne savent même pas sous quelle identité leurs comptes ont été créés. Voici ce qu'a vécu monsieur Inongo, consommateur du service mobile money comme situation-problème liée à la dotation d'identité :

> *« Quand il m'avait posé la question, alors je lui dis que j'ai une carte SIM où il y a une somme considérable d'argent. Maintenant, la carte SIM en question n'affiche plus dans mon téléphone. Voilà pourquoi je viens auprès de vous pour que vous m'aidiez à faire la SIM blanche. Il prend le téléphone ainsi que la carte d'électeur puis me demande cinq numéros des correspondants avec qui je cause.*
> *Il fait des manipulations au cours d'un moment donné puis me dit que l'opération n'était pas possible parce que la carte SIM active avait une identité différente de la mienne. Il me dit que la carte SIM était enregistrée sous le nom de Gbadolite*

*pendant que moi, je m'appelle Inongo. Quand il avait dit cela, directement je m'étais rappelé parce que cette SIM-là, je l'avais payé en cours de route quand je venais ici en 2021 ».*

Pour résoudre le problème de la dotation d'identité afin d'être rétabli dans ses droits, monsieur Inongo a fait recours aux pratiques frauduleuses :

*« Après cela, il me dit que comme il y a de l'argent dans la carte SIM, si j'allais au niveau de la shop, on va me suspecter comme quelqu'un qui a volé une carte SIM d'autrui et qui veut voler l'argent et ça va compliquer. Pour cela, je veux vous aider. Je lui demande comment ?*
*Il me dit qu'il a quelqu'un (son ami) à partir de Kinshasa qui est agent et travaille dans une shop. Est donc, celui-là pourra nous aider à changer l'identité de la carte SIM en votre nom à partir de là et comme il y a de l'argent, cela nous permettra de faire facilement la SIM blanche. Après lui avoir donné ses droits et effectivement il appelle son ami là et ils causent puis font ce que lui-même appelait la mise à jour de la carte SIM. Après cette mise à jour, j'étais allé à la shop pour faire la carte SIM blanche puis récupérer l'argent. C'est de cette manière que les choses s'étaient passées ».*

Reconnaissant le phénomène de « dotation d'identité », monsieur Maïndombe, vendeur du service mobile money donne les raisons pour lesquelles ils enregistrent les cartes SIM et les comptes mobiles sous leurs identités et même autre que leurs propres identités :

*« C'est vrai, ce que tu dis là est tout à fait correct. Mais nous quand on fait cela, moi personnellement, ce n'est pas dans une mauvaise intention mais je ne sais pas pour les autres peut être. Pour moi, quand je fais cela c'est juste pour gagner du temps. Tu sais, si on doit chaque fois commencer à demander à chaque client son identité, il y en a d'autres qui ne maîtrisent même pas leur propre identité. Voilà pourquoi nous le faisons. C'est seulement pour gagner du temps et faciliter les clients ».*

Contrairement à ce que dit monsieur Maïndombe, mademoiselle Mbandaka estime que ces agents et même vendeurs du service le font sciemment. Elle relate ce que l'a vécu où le vendeur voulait intentionnellement mettre son identité au lieu de lui demander la sienne.

*« J'arrive devant une cabine, je trouve le monsieur qui était là et je lui dis que j'avais besoin d'ouvrir un compte Orange Money. Le monsieur accepte, me*

*demande le téléphone. Curieusement, le monsieur commence à manipuler le téléphone jusqu'au point de me demander que je lui dicte le mot de passe. Fâchée, je luis dis mais monsieur tu as mis quelle identité ? Parce que tu ne m'as pas demandé mon identité et grave encore tu veux que te dicte mon mot de passe ? En quoi est-ce qu'il sera secret si toi tu restes avec ? Il avait échoué quoi dire et je lui avais obligé de refaire les choses afin qu'il mette mon identité et que le mot de passe c'est moi-même qui dois taper et non lui et il était obligé de le faire ».*

Voilà d'une manière très détaillée les différentes formes de criminalité qui se vivent dans les services financiers mobiles dits Mobile Money. A noter aussi que cette liste est loin d'être exhaustive.

**Conclusion**

L'évolution technologique et ses multiples facettes : coup d'œil criminologique dans les services financiers mobiles « Mobile Money », tel est le titre de cette exercice scientifique. Telle que formulée, la thématique est un carrefour où l'interdisciplinarité exigée dans les recherches scientifiques modernes est de rigueur car celui-ci ne pourra intéresser non seulement le criminologue mais aussi l'économiste ainsi que les experts en télécommunication et en droit.

Cette dissertation présente l'état de lieux de la criminalité dans ces services financiers modernes. Nous y avons fait mention d'une liste non exhaustive des comportements problématiques qui expliquent la présence de la criminalité dans ces services.

Pour mieux appréhender l'objet sous étude, nous avons procédé par une immersion tout à fait méthodique dans l'univers du terrain de recherche à travers les acteurs impliqués dans le phénomène étudié, c'est-à-dire la criminalité dans les services financiers via mobile money. Ces acteurs ont été rencontrés différemment selon le rôle que chacun d'eux joue dans les services financiers mobiles.

L'étude étant du type qualitatif, nous avions le choix entre l'échantillonnage par cas unique et l'échantillonnage par cas multiples. Nous avons à cet effet porté notre choix sur le mode d'échantillonnage par cas unique choisi par « effet boule de neige ou chaîne » qui consiste à identifier « de bons cas grâce à des personnes qui connaissent d'autres personnes ayant des cas riches en informations ».

Dans l'analyse des données collectées sur terrain, nous sommes arrivés aux résultats selon lesquels, six formes de criminalité ont été évoquées, à savoir : « le piquage », « le dribbling », « le marimisage », « l'accidentage », « l'évasion » et « la dotation d'identité ».

Soulignons que notre réflexion n'a pas la prétention d'avoir épuisé toute la problématique autour de la criminalité dans les services financiers mobiles dits Mobile Money. Elle a néanmoins abordé les questions en rapport avec les formes de criminalité dans ces services financiers modernes, la manière dont celles-ci se construisent et se réalisent.

**Référence**

AEBI M. F., (1999), La validité des indicateurs de la criminalité: Les sondages de délinquance autoreportée face aux données de police et du casier judiciaire, Thèse de doctorat, Lausanne: Université de Lausanne, I.P.S.C.

ANNIE, B., (2016), l'utilisation des TIC à des fins de harcèlement criminel en situation de violence conjugale, mémoire, Université de Montréal, Montréal.

AUCANTE, M., (2020), La bancarisation de l'Afrique par les téléphones mobiles : de nouveaux acteurs sur la scène financière mondiale ?, Thèse de doctorat, Université Paris II Panthéon-Assas, Paris.

BOOS, R., (2016) « La lutte contre la cybercriminalité au regard de l'action des États ». Droit. Université de Lorraine.

BRACK, E., (2016), Les nouveaux usages financiers mobiles en Afrique, rapport issu du african forum banking.

CHAIX, L. et TORRE, D. (2015), « Le double rôle du paiement mobile dans les pays en développement », in Revue économique, 2015/4 Vol. 66, pages 703 à 727.

CHAIX, L., (2013), « Le paiement mobile : modèles économiques et régulation financière », in Revue d'économie financière, 112, p. 277-298.

CHAWKI, M., (2006), Essai sur la notion de cybercriminalité, IEHEI. Accessible en ligne à http://www.ie-ei.eu/bibliotheque/cybercrime.

Cohen, E.L. et Felson, M. (1979). Social Change and Crime Rate Trends: a Routine Activity Approach. American Sociological Review, 44(4), 588-608.

DEBUYST C. (1990), Grille de lecture d'acteur social, éd, Bruxelles pierre Mardaga ;

Dictionnaire universel (2010), édition spéciale de la République Démocratique du Congo, Hachette, Paris.

FATTAH, E. (1980), Victimologie : tendances récentes. Criminologie, volume 13, numéro 1, pp 6–36. Presses de l'Université de Montréal.

JODELET, D., (2003), « les représentations sociales : un domaine en expansion », in D. Jodelet (dir), Les représentations sociales, Paris, Presses Universitaires se France.

Kevin B. (2018), Le Hacking pour les nuls, First Interactive, Paris ;

LAETITIA Chaix. (2013). Le paiement mobile : perspectives économiques, modèles d'affaires et enjeux concurrentiels. Economies et finances. Université Nice Sophia Antipolis.

LEMAN-LANGLOIS, S. (2006). Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial. Criminologie, 39 (1), 63–81. https://doi.org/10.7202/013126ar

MERCY W. BUKU et RAFE MAZER, (2017) « Services financiers mobiles : protéger les clients, les prestataires et le système de la fraude », Note de politique de gestion des transferts mobile money, CGAP, Washington.

MILES, M.B., & HUBERMAN, A.M, (2003), Analyse des données qualitatives (2e éd.). Paris : De Boeck.

NICOLAS K. (2014), Guide de prévention contre les arnaques, vols et agressions : 500 conseils d'un policier de terrain, Albin Michel, Paris ;

OLIVIER I. (2008), L'identité numérique en question : 10 scénarios pour la maitrise juridique de son identité sur Internet, Eyrolles, Paris ;

PIRES A. (1995), « La criminologie d'hier et d'aujourd'hui » in DEBUYST C., DIGNEFFE F., LABADIE J.-M. et PIRES A., Histoire des savoirs sur le crime et la peine. Tome I. Des savoirs diffus à la notion de criminel-né, Presses de l'Université de Montréal, Presses Universitaires d'Ottawa et De Boeck Université.

TSHINYAMA KADIMA, I. (2009), L'observation ethnographique d'un commissariat à Lubumbashi. Une compréhension des pratiques policières en contexte congolais, thèse de doctorat, Lubumbashi, Unilu-Ecocrim.