RA2LC n°19, Vol.1 – septembre 2026
Soumission | 08-07-2026
Publication | 30-09-2026

Ziglôbitha,
Revue des **A**rts, **L**inguistique,
Littérature & **C**ivilisations
Université Peleforo Gon Coulibaly - Korhogo

DE LA DESCRIPTION DENSE À LA SATURATION THÉORIQUE : UNE ENQUETE QUALITATIVE SUR LA CYBER-FRAUDE ET LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL EN RDC

Christian NGUABONGA LUTETE[1]
Université de Kinshasa, République Démocratique du Congo
christian.nguabonga@fonarev.cd

&

Raoul KIENGE-KIENGE INTUDI[2]
Université de Kinshasa, République Démocratique du Congo
raoul.kienge@unikin.ac.cd

&

Joël NZAMPUNGU IMBOLE[3]
Université de Kinshasa, République Démocratique du Congo
joel.nzampungu@unikin.ac.cd

Résumé : Cet article détaille le dispositif méthodologique qualitatif déployé pour analyser la réaction sociale face à la cyber-fraude bancaire et aux enjeux de protection des données à Kinshasa (République Démocratique du Congo) en 2026. S'appuyant sur un ancrage ethnographique au cœur du centre financier de la commune de la Gombe, l'étude opérationnalise les concepts de « description dense» (Geertz, 1973) et la participation observante au sein d'organisations bancaires caractérisées par une culture du secret. A travers un échantillonnage par choix raisonné et l'utilisation de la technique de la « boule de neige », le corpus a été stabilisé à 12 acteurs de haut niveau (RSSI, directeurs de conformité, analystes AML et inspecteurs de la Banque Centrale du Congo), guidé par le principe de saturation théorique. L'article examine les barrières structurelles d'accès à ce terrain sensible, décrit un protocole strict de double anonymisation pour neutraliser les risques réputationnels, et expose l'usage de l'analyse de contenu thématique appliquée au décryptage des représentations de la menace, des rituels de contrôle et des interférences politiques.

Mots-clés : Ethnographie, saturation théorique, cyber-fraude, protection des données, Kinshasa et criminologie en milieu fermé.

[1] Responsable de la sécurité à Fonarev, **Christian NGUABONGA** est licencié en administration des affaires et sciences économiques de l'UPC. Il est également apprenant finaliste en criminologie économique et environnementale à l'école de criminologie de l'Université de Kinshasa.
[2] Raoul Kienge-Kienge est juriste et criminologue, Directeur de l'école de criminologie de l'Université de Kinshasa.
[3] Docteur en communication et doctorant en criminologie, Joël NZAMPUNGU est enseignantchercheur à l'école de criminologie de l'Université de Kinshasa.

FROM THICK DESCRIPTION TO THEORETICAL SATURATION : A QUALITATIVE RESEARCH PROTOCOL ON CYBER-FRAUD AND DATA PROTECTION IN THE DRC

Abstract : This article outlines the qualitative methodological framework designed to investigate social and institutional responses to banking cyber-fraud and data protection challenges in Kinshasa (Democratic Republic of the Congo) in 2026. Grounded in an ethnographic approach within the financial hub of La Gombe, this study operationalizes "thick description" and "observant participation" within highly secretive banking organizations. Utilizing purposive sampling combined with the "snowball" technique, the corpus was stabilized at 12 elite interviewees—including CISOs, compliance directors, AML analysts, and Central Bank of the Congo inspectors—guided by the principle of theoretical saturation. The paper critically examines the structural barriers to accessing such sensitive settings, delineates a comprehensive double-anonymization protocol to mitigate reputational risks, and details the application of thematic content analysis to decode threat representations, control rituals, and political interferences.

Keywords: Ethnography, theoretical saturation, cyber-fraud, data protection, Kinshasa, deep-field criminology.

Introduction

L'écosystème financier de la République Démocratique du Congo (RDC), et plus spécifiquement sa capitale Kinshasa, connaît une transition numérique fulgurante. L'interconnexion généralisée des réseaux, la multiplication des services de banque mobile (*Mobile Money*) et la dématérialisation des flux monétaires ont profondément modifié les rapports économiques nationaux. Cependant, cette numérisation accélérée s'accompagne d'une mutation corrélationnelle des formes de criminalité en col blanc. A la délinquance financière analogique traditionnelle a succédé une cyberfraude bancaire multiforme et endémique, caractérisée par des techniques d'ingénierie sociale agressives, des attaques par rançongiciels, des interceptions de flux de paiement et, de manière plus pernicieuse, des spoliations orchestrées de comptes d'épargne dits « dormants ». Face à cette asymétrie de la menace, l'appareil législatif national tente de s'adapter, notamment par la promulgation de la Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication, complétée par les directives macroprudentielles de la Banque Centrale du Congo (BCC).

Sur le plan scientifique, l'étude de la criminalité informatique en col blanc au sein des pays du Sud global se heurte à un vide empirique persistant. La majorité des théories criminologiques contemporaines sur le contrôle numérique ont été formalisées à partir de terrains occidentaux occidentalisés. Surtout, la recherche empirique se heurte à une barrière épistémologique majeure : le caractère hermétique des institutions bancaires privées. En tant que sanctuaires

du capitalisme technologique, les banques commerciales opposent un droit de réserve drastique à toute investigation externe, motivées par la peur de voir leurs vulnérabilités techniques dévoilées, ce qui mettrait en péril la confiance du public, condition *sine qua non* de leur survie économique : Comment, dès lors, enquêter scientifiquement sur des objets d'étude frappés du sceau de la « haute sécurité » et du secret réputationnel sans se contenter d'analyses juridiques abstraites, de rapports de cabinets de conseil privés ou de descriptions techniques désincarnées ?

Cet article se donne pour objectif d'expliciter, de formaliser et de justifier le protocole d'enquête qualitative de type compréhensif qui a permis de lever le voile sur la réalité vécue de la cyber-fraude et de la protection des données au sein du système bancaire kinois. L'enjeu est de démontrer l'effectivité d'un agencement méthodologique combinant l'immersion ethnographique, l'échantillonnage par choix raisonné indexé sur le principe de saturation théorique, la participation observante et l'analyse de contenu thématique stricte. Il s'agit de décrire comment les résistances du terrain ont été identifiées, problématisées puis surmontées, afin d'offrir une méthode robuste permettant de documenter scientifiquement les dynamiques de la réaction sociale interne et étatique.

Cette recherche est structurée en cinq sections principales. La première section examine les fondements de l'ancrage ethnographique au sein du centre financier de Kinshasa/Gombe, démontrant l'apport de la « description dense » pour capter la matérialité du contrôle et les rituels informels de la suspicion. La deuxième section formalise les stratégies d'échantillonnage par choix raisonné et par effet « boule de neige », tout en justifiant la clôture du corpus par le principe de saturation théorique et en explicitant le protocole de double anonymisation. La troisième section détaille l'articulation opérationnelle des techniques de collecte, entre participante et clinique de l'entretien semi-directif non-directif. La quatrième section expose le protocole d'analyse de contenu thématique structuré autour d'une tripartition du codage textuel. La cinquième section propose une réflexion approfondie sur l'éthique de la recherche en terrain sensible, analysant les obstacles structurels rencontrés et les stratégies de négociation permanente qui ont transformé l'enquête d'une menace perçue en un outil d'aide à la décision managériale.

1. L'ancrage ethnographique à la Gombe

1.1. La commune de la Gombe comme scène criminologique et spatio-temporelle

Pour mener à bien une étude compréhensive des dispositifs de contrôle face à la cyber-fraude, le choix du terrain d'enquête ne pouvait être abstrait. Il s'est fixé sur la commune de la Gombe à Kinshasa. Ce choix géographique repose sur une rationalité spatio-temporelle précise : la Gombe constitue le centre névralgique du pouvoir politique, diplomatique et financier de la République Démocratique du Congo. C'est le lieu où se concentrent les sièges sociaux des plus grandes institutions financières du pays, à l'instar de la Rawbank, de l'Equity BCDC, de l'Access Bank RDC, ainsi que les infrastructures de la Banque Centrale du Congo.

D'un point de vue criminologique, cet espace clos de quelques kilomètres carrés fonctionne comme une enclave technologique au sein d'une mégapole caractérisée par l'informalité économique. L'immersion prolongée au sein de ces sièges sociaux a permis de mener des observations de terrain durant le mois de juin 2025. Pénétrer quotidiennement ces espaces caractérisés par des architectures de verre, des portails de sécurité biométriques et une surveillance par caméras en circuit fermé constitue la première étape d'une rupture épistémologique avec les représentations théoriques de la délinquance de rue. Le terrain kinois offre un contraste saisissant : la Gombe est le lieu où se gèrent des flux financiers virtuels colossaux, tandis qu'à sa périphérie immédiate s'exprime une précarité matérielle aiguë. C'est précisément au cœur de cette tension structurelle que se déploient les stratégies de cyber-fraude en col blanc, rendant l'immersion sur cette scène spatio-temporelle indispensable pour comprendre la mise en œuvre réelle des politiques de sécurité des systèmes d'information.

1.2. De l'organigramme abstrait à la matérialité du contrôle

L'approche qualitative mise en œuvre s'oppose à la simple lecture positiviste des politiques de sécurité inscrites dans les manuels de procédure des banques. Pour restituer la complexité des rapports de force et des tactiques de contournement, cette recherche a opérationnalisé le concept fondamental de « description dense » théorisé par l'anthropologue Clifford Geertz dans son ouvrage séminal *The interpretation of cultures* (1973, p.12). Selon Geertz, « la description ne doit pas se limiter à enregistrer un comportement ou un événement brut (ce qu'il nomme une description mince), mais doit s'attacher à restituer la hiérarchie stratifiée des structures de signification dans lesquelles les acteurs produisent leurs actions ».

Sur notre terrain, appliquer la description dense impliquait de dépasser les organigrammes abstraits et les déclarations d'intention pour se confronter à la matérialité technique des dispositifs de contrôle. Cela s'est traduit par

l'observation minutieuse de l'agencement physique des espaces de travail : la configuration des départements d'audit informatique, l'emplacement des salles de serveurs, l'architecture logique des pare-feu, des routeurs, et la gestion des serveurs de logs. C'est à ce niveau de granularité que le chercheur peut appréhender le "droit en action" (*law in action*). Par exemple, une attention particulière a été portée à l'application *accesspaycongo*, utilisée pour centraliser des flux transactionnels spécifiques. La description dense a permis de documenter la manière dont les auditeurs traquent visuellement les anomalies logiques, repèrent les ports applicatifs anormalement ouverts (véritables portes virtuelles pour l'intrusion) et analysent les fichiers journaux (*audit trails*).

Au-delà de la technique pure, cette immersion a permis de capter la dimension informelle des logiques de suspicion managériale. Au sein du système bancaire kinois, la suspicion n'est pas uniquement un algorithme de détection des fraudes ; elle s'incarne dans des rituels quotidiens de contrôle des corps et des accès informatiques, notamment lors de la réinitialisation des mots de passe ou du contrôle rigoureux de l'usage du code PIN par les collaborateurs. La description dense met en relief le fait que le contrôle de la cyber-fraude est un processus social négocié, où les cadres de sécurité luttent en permanence contre la négligence humaine, le contournement des règles par les employés de base et les pressions diffuses qui s'exercent au sein de l'organisation.

2. Stratégies d'échantillonnage et dynamique de constitution du corpus sous contrainte de secret

2.1. Le choix raisonné et la technique de la « boule de neige »

En raison de la nature confidentielle des données relatives à la délinquance informatique et bancaire, l'accès à un échantillon de professionnels ne pouvait s'opérer par des méthodes probabilistes ou aléatoires. La constitution du corpus a nécessité une stratégie d'échantillonnage par choix raisonné, combinée à la technique de la « boule de neige », formalisée par Patrick Biernacki et Dan Waldorf (1981, pp.141-163).

La technique de la boule de neige est particulièrement adaptée aux populations cachées, marginales ou, comme c'est le cas ici, protégées par des barrières institutionnelles denses. La démarche a consisté à identifier initialement deux informateurs clés, reconnus pour leur expertise au sein de la communauté de la sécurité informatique à Kinshasa. Après avoir établi une relation de confiance et présenté les garanties académiques requises, ces premiers répondants ont activé leurs propres réseaux professionnels pour nous introduire auprès d'autres homologues exerçant dans des établissements concurrents. Cette méthode par cooptation en chaîne a permis de franchir la méfiance initiale des acteurs.

Les critères d'inclusion dans l'échantillon étaient particulièrement stricts : les participants devaient être des cadres supérieurs ou des experts techniques directement décisionnaires ou opérationnels dans la chaîne de production de la réaction sociale face au risque de fraude numérique. Le corpus final a été stabilisé à 12 participants de haut niveau, couvrant la diversité du paysage bancaire en RDC en incluant des représentants de 6 banques commerciales majeures de la place ainsi que deux inspecteurs de haut rang exerçant au sein de la Direction des Contrôles des Intermédiaires Financiers (DCIF) de la Banque Centrale du Congo. Ce croisement entre régulateurs étatiques et opérateurs privés a garanti une triangulation optimale des perspectives discursives.

2.2. Le principe de saturation théorique comme indicateur de clôture empirique

La taille finale du corpus d'enquête n'a pas été fixée *a priori* selon des critères statistiques, mais a été déterminée au cours de la recherche par l'application du principe de saturation théorique. Ce concept, pilier de la démarche qualitative, a été formalisé par Barney Glaser et Anselm Strauss (1967, pp.61-65). Dans le cadre de la théorie ancrée, la saturation désigne le moment de la collecte de données où l'ajout de nouveaux entretiens ou d'observations empiriques supplémentaires n'apporte plus d'éléments conceptuels inédits, de nouvelles catégories analytiques ou de variations significatives dans la compréhension du phénomène étudié.

Sur notre terrain kinois, le protocole de codage en temps réel des entretiens a révélé un point d'inflexion empirique précis. A partir du dixième entretien mené auprès des cadres bancaires, les récits de pratiques d'étiquetage moral des cyber-délinquants, les descriptions des processus de fraude (notamment les schémas récurrents d'ingénierie sociale ou de spoliation de comptes dormants par complicité interne) ainsi que l'exposition des défaillances réglementaires nationales ont commencé à se répéter de manière systématique et redondante. Pousser l'échantillon jusqu'à 12 participants, en intégrant les inspecteurs de la Banque Centrale, a permis de valider définitivement la robustesse de nos catégories empiriques (Glaser & Strauss, 1967, p.65). A ce stade, la structure conceptuelle de l'arbre thématique était stabilisée : les données brutes confirmaient et enrichissaient les catégories préexistantes sans exiger la création de nouvelles variables explicatives. La collecte a donc été scientifiquement close.

2.3. Le protocole de double anonymisation éthique

Mener une recherche qualitative sur la cyber-fraude au sein d'un marché financier aussi concurrentiel et interconnecté que celui de Kinshasa exige des garanties éthiques de protection absolue des sources. Pour lever la censure des participants, qui risquaient des sanctions disciplinaires ou des poursuites

judiciaires en cas de violation du secret professionnel, un protocole de double anonymisation stricte a été mis en œuvre.

Premièrement, l'anonymisation a visé les identités individuelles des répondants. Leurs noms, prénoms et fonctions précises ont été expurgés des transcriptions et remplacés par des pseudonymes construits combinant un titre générique et des initiales aléatoires (ex. « M. Laurent K. », « Inspecteur Alain K.»). Deuxièmement, cette protection individuelle a été doublée d'une anonymisation institutionnelle. Les dénominations commerciales des banques de la place (Rawbank, Access Bank, BCDC, etc.) ont été systématiquement masquées et substituées par des codes alphabétiques génériques (Banque A, Banque B, Banque C, etc.) dans l'ensemble des analyses, des citations de verbatims et des tableaux synoptiques. Ce double bouclier de confidentialité a neutralisé le risque de préjudice réputationnel ou concurrentiel pour les établissements concernés, permettant aux acteurs de s'exprimer librement sur les failles systémiques de leurs propres organisations.

Le tableau synoptique ci-dessous fournit la cartographie détaillée du corpus d'enquête stabilisé en juin 2025 sous le sceau de ce protocole éthique :

Tableau 1 : Cartographie synoptique du corpus d'enquête (Données de terrain, Juin 2026)

Code bancaire (Anonymisé)	Institution opérationnelle (Anonymisée)	Fonction dans la Banque	Ancienneté de l'Entretien	Date, Heure et Lieu de répondant (Kinshasa/Gombe)
« M. Laurent K. »	Banque A	Responsable de la Protection des Données	14 ans (8 ans au poste)	Lundi 22 juin 2025 à 17h00 – Siège Social (Gombe)
« M. Arnauld N. »	Banque B	Directeur de la Sécurité des Systèmes d'Information (RSSI)	3 ans (3 ans au poste)	Mardi 30 juin 2025 à 10h00 – Siège Social (Gombe)
« Mme Dorcas M. »	Banque C	Analyste Senior Conformité & AntiMoney Laundering (AML)	7 ans (4 ans au poste)	Mercredi 17 juin 2025 à 14h30 – Direction Générale
« M. Christian T. »	Banque D	Responsable Risques Opérationnels & Fraude	5 ans (3 ans au poste)	Jeudi 18 juin 2025 à 11h00 – Siège Social (Gombe)
« Mme Carine B. »	Banque E	Directrice de l'Expérience Client & Réclamations	9 ans (5 ans au poste)	Vendredi 19 juin 2025 à 16h00 – Direction Commerciale
« M. Patrick W. »	Banque F	Chef de Département Audit Interne & Sécurité Numérique	11 ans (6 ans au poste)	Lundi 22 juin 2026 à 09h00 – Siège Social (Gombe)
« M. Jean-Paul L. »	Banque A	Auditeur des Systèmes d'Information	4 ans (2 ans au poste)	Mercredi 24 juin 2025 à 15h30 – Siège Social (Gombe)
« Mme Sarah K. »	Banque B	Gestionnaire de Comptes Nationaux & PME (Gestion des flux)	6 ans (4 ans au poste)	Jeudi 25 juin 2025 à 13h00 – Siège Social (Gombe)
« M. Eric M. »	Banque C	Ingénieur Sécurité Réseaux & Tests d'Intrusion (VAPT)	3 ans (3 ans au poste)	Vendredi 26 juin 2025 à 10h30 – Direction Technique

« **M. Olivier N.** »	Banque E	Responsable des Affaires Juridiques & Contentieux	8 ans (6 ans au poste)	Lundi 29 juin 2025 à 14h00 – Direction des Affaires Juridiques
« **Inspecteur Alain K.** »	Banque Centrale	Cadre à la Direction des Contrôles des Intermédiaires Financiers	12 ans (7 ans à la DCIF)	Mercredi 01 juillet 2025 à 11h00 – Siège BCC (Gombe)
« **Inspectrice Marie M.** »	Banque Centrale	Analyste des Risques Prudentiels & Systèmes de Paiement BCC	10 ans (5 ans à la DCIF)	Jeudi 02 juillet 2025 14h30 – Siège (Gombe)

Ce matériel empirique a été collecté principalement en langues française et anglaise, cette dernière étant la langue d'usage des documentations techniques, des rapports de tests d'intrusion et des normes de sécurité internationales (ISO 27001) appliquées au sein des banques. Le corpus a été enrichi par une phase d'observations régulières menée à la Banque Centrale du Congo, permettant de confronter le discours des assujettis à la rationalité de l'organe de régulation.

3. Le croisement des techniques de collecte : participation observante et clinique de l'entretien

3.1. La participation observante transparente

La collecte des données empiriques s'est structurée autour d'un croisement méthodologique précis, visant à faire converger les discours et les pratiques pratiques réelles de contrôle. La première technique mobilisée est la participation observante, reformulée de manière critique par le sociologue Loïc Wacquant dans son ouvrage de référence *Corps et Âme. carnets d'un apprenti boxeur* (2000, p.12). S'opposant à l'observation participante classique qui exige souvent du chercheur de dissimuler son identité ou de feindre une passivité totale, la participation observante de Wacquant implique une immersion active où le chercheur assume de manière transparente son statut scientifique auprès des enquêtés, tout en s'insérant dans les routines de l'espace social étudié.

Sur le terrain des banques de la Gombe, cette posture de chercheur universitaire officiellement mandaté par l'Ecole de Criminologie de l'Université de Kinshasa a ouvert l'accès aux départements de contrôle. La participation observante a permis d'assister de manière directe à la matérialité des processus de sécurisation. Durant des sessions d'observation en bureau, il a été possible de voir les ingénieurs réseaux effectuer des tests d'intrusion applicatifs (*VAPT - Vulnerability assessment and penetration testing*), de documenter l'identification des

ports de communication vulnérables et d'observer les rituels de gestion des alertes de sécurité au sein du centre d'opération de sécurité (*SOC*). Cette présence a également permis d'observer la manipulation concrète de l'application *accesspaycongo* lors des audits de flux de paiement, offrant l'opportunité d'enregistrer les réactions spontanées des auditeurs face à l'émergence d'une alerte de fraude, réactions qui échappent par définition au cadre formel des entretiens programmés.

3.2. L'entretien semi-directif approfondi et la non-directivité

En complément des observations, des entretiens semi-directifs approfondis ont été menés auprès des 12 participants. Cette technique s'est appuyée sur les fondements méthodologiques posés par Carl Rogers (1942, p.85), qui a théorisé l'approche clinique non-directive. Adapté aux sciences sociales, l'entretien semi-directif rogérien permet de concilier la rigueur d'un guide d'entretien thématisé (qui garantit que toutes les dimensions de la recherche seront abordées) et une liberté d'expression maximale accordée à l'enquêté grâce à des techniques de relance neutres et à une écoute active.

L'usage d'un guide d'entretien fluide a permis de structurer l'échange autour de cinq grands axes sémantiques : les représentations subjectives de la donnée comme ressource stratégique, les figures morales associées aux hackers, l'explication des architectures logiques de contrôle (normes ISO 27001), l'exposition clinique d'études de cas réels vécus au sein des établissements (notamment deux fraudes majeures documentées de 26 000 USD et 45 000 USD), et enfin, l'analyse critique des pressions politiques subies par la direction Expérience Client lors de la gestion des réclamations complexes. La non-directivité a permis de désamorcer la méfiance de ces cadres de haut niveau : en se sentant écoutés par un chercheur neutre n'adoptant pas une posture d'inspecteur ou de censeur, les répondants ont pu formuler des récits détaillés, révélant les failles organisationnelles et les accommodements informels qui sous-tendent la réalité quotidienne de la cybersécurité à Kinshasa.

4. Le protocole de traitement des données : l'analyse de contenu thématique

4.1. Découpage et codage selon Laurence Bardin (1977)

Le volume important de matériau empirique recueilli, constitué par les transcriptions intégrales des entretiens semi-directifs et les notes détaillées de participation observante a fait l'objet d'un traitement systématique par la méthode de l'analyse de contenu thématique. Le protocole opérationnel appliqué est celui défini par Laurence Bardin (1977).

Conformément à la méthodologie de Bardin, la première phase a consisté en une « lecture flottante » du corpus textuel pour s'imprégner des données,

suivie d'une phase de découpage des textes en « unités de signification » (ou unités d'enregistrement). Une unité de signification correspond à un segment de phrase, une phrase entière ou un paragraphe véhiculant une idée unique et autonome relative à l'objet de recherche. Ces unités de signification ont été extraites puis regroupées de manière inductive au sein de catégories sémantiques, pour former un arbre thématique cohérent permettant de confronter nos hypothèses théoriques aux données brutes du terrain kinois.

4.2. La tripartition de la grille d'analyse (Les trois axes de codage)

L'arbre thématique final issu du codage selon Bardin s'est structuré de manière herméneutique autour de trois axes de codage majeurs, reflétant les dynamiques profondes de la réaction sociale face à la cyber-fraude :

- Le codage des représentations de la menace : Cet axe s'est attaché à isoler toutes les occurrences discursives, métaphores et lexiques associés à la figure du délinquant informatique. Les analyses ont révélé une catégorisation morale binaire opérée par les RSSI, séparant le « hacker positif » (l'expert de sécurité interne) du « hacker négatif » (le cyber-prédateur externe), ainsi qu'une sémantique valorisant la donnée financière comme la « mine d'or » ou « l'or noir de l'internet ». De plus, une attention centrale a été portée à la figure de l'« *insider* opportuniste », l'employé interne collaborant à la fraude en raison d'une vulnérabilité économique.
- Le codage des pratiques de contrôle : Cet axe a regroupé les descriptions techniques et rituelles des barrières de sécurité déployées par les institutions bancaires. Il comprend la classification des outils de surveillance logique (*audit trail*, contrôle des logs système, paramétrage des pare-feu, exécution des tests d'intrusion VAPT) et des dispositifs de surveillance physique et corporelle (claustration des corps, biométrie faciale, blocage de l'accès aux médias sociaux sur le lieu de travail, contrôle strict des impressions papier). Ce codage a mis en évidence l'alignement sur la théorie de la prévention situationnelle de Ronald Clarke (1980) et le panoptisme de Michel Foucault (1975).
- Le codage des dysfonctionnements de la réaction sociale : Cet axe a répertorié toutes les données textuelles mettant en relief les limites structurelles de l'appareil de contrôle. Il a permis d'isoler les discours relatifs à la violence économique de la Banque Centrale du Congo (le mécanisme de « débit d'office » punitif appliqué aux comptes de règlement), l'évaluation critique de l'invalidation de la Loi n°20/017 due à la non-opérationnalisation de l'Autorité de Protection des Données Personnelles (APDP), l'absence chronique de jurisprudence, et les

témoignages cliniques décrivant les pressions politiques intenses et le clientélisme informel visant à étouffer les enquêtes pour fraude à Kinshasa.

5. Réflexivité éthique

5.1. Les cinq obstacles structurels du terrain bancaire kinois

L'analyse réflexive du déroulement de l'enquête révèle que l'accès à un terrain aussi fermé que le secteur financier congolais constitue en soi un objet d'étude criminologique. Enquêter sur la cyber-fraude et la compromission des données personnelles confronte le criminologue à ce que Jeanne Favret-Saada (1977) qualifie d'objets frappés de « secret » ou de haute sensibilité sociale. La recherche s'est heurtée à cinq obstacles structurels majeurs qu'il convient de déconstruire :

- *L'extrême sensibilité politique et technique de la gouvernance des données :* La moindre discussion portant sur la sécurité des flux ou les failles logiques de l'application *accesspaycongo* était perçue par les cadres dirigeants comme une menace pour la stabilité de l'institution.
- *L'impératif de confidentialité drastique :* Les banques commerciales s'imposent un droit de réserve absolu. Révéler des cas réels de spoliation de comptes dormants ou des montants précis de détournement (tels que les cas documentés de 26 000 USD et 45 000 USD) risquerait d'éroder la confiance de la clientèle, capital immatériel le plus précieux de ces entreprises.
- *Le soupçon d'espionnage industriel lié au statut de chercheur en criminologie* **:** Les répondants ont fréquemment manifesté une attitude défensive initiale, assimilant la démarche universitaire à une investigation policière masquée ou suspectant le chercheur d'agir pour le compte d'un cabinet d'audit concurrent.
- *La crainte de l'instrumentalisation des résultats :* Plusieurs directions générales ont opposé une fin de non-recevoir à nos requêtes de peur que les conclusions écrites ne soient utilisées par le régulateur (BCC) pour appliquer des sanctions punitives de débit d'office.
- *L'absence quasi totale d'antécédents de recherche :* Les départements stratégiques de sécurité informatique n'accueillent pratiquement jamais de chercheurs externes, fonctionnant en autarcie totale.

Ces résistances s'apparentent aux barrières d'accès décrites par Dominique Monjardet (1996, p. 14) lors d'enquêtes sur les institutions de contrôle. Plus le chercheur s'approche du noyau dur du pouvoir ou de la gestion de la déviance, plus l'organisation déploie des stratégies de dissimulation pour protéger sa façade institutionnelle.

5.2. Du statut de menace à l'outil d'aide à la décision

Pour surmonter ces barrières et lever les censures managériales, plusieurs stratégies de contournement et de légitimation ont été déployées tout au long de l'immersion. Le premier levier de crédibilisation a été l'usage systématique de la lettre de recherche officielle délivrée par l'École de Criminologie de l'Université de Kinshasa. Ce document institutionnel a fonctionné comme un sauf-conduit académique, dissipant le soupçon d'espionnage en réinscrivant formellement l'enquête dans le champ de la production de connaissances scientifiques. Cette caution a été renforcée par la signature d'un engagement éthique de confidentialité absolue, matérialisé par le protocole de double anonymisation décrit précédemment.

Par ailleurs, le dépassement de la méfiance a nécessité ce que Jean-Pierre Olivier de Sardan qualifie, dans son article fondamental « La politique du terrain », de « négociation permanente de l'accès au terrain » (*In Enquête*, 1995, pp. 71-109). Plutôt que de masquer la sensibilité du sujet ou de jouer un rôle passif, nous avons choisi de problématiser ouvertement les enjeux de la recherche avec les décideurs lors des premiers contacts. Plusieurs managers de la sécurité (RSSI) ont trouvé la recherche pertinente précisément en raison de son acuité intellectuelle et de son ancrage dans la réalité de l'année 2025. Ils ont manifesté le besoin d'obtenir le regard extérieur, distancié et théorique d'un chercheur universitaire sur des routines de contrôle qu'ils savent perfectibles mais qu'ils ne peuvent critiquer en interne.

Dès lors, le positionnement de l'enquêteur s'est inversé : de menace potentielle pour la réputation de l'établissement, la recherche a été requalifiée par les décideurs en un outil d'aide à la décision. Les cadres de sécurité ont compris que documenter scientifiquement l'existence des interférences politiques (le choc des pouvoirs) et l'impact des bas salaires sur la rationalisation de la fraude (l'agent qui a un salaire de 150 USD voire 300 $ USD mais gérant des flux de 1 500 000 USD) pouvait servir de levier interne pour exiger de leurs directions générales des augmentations budgétaires, un renforcement de la formation technique des équipes, ou une sanctuarisation de leur statut face aux pressions extérieures. C'est ce pacte de confiance et d'intérêt scientifique partagé qui a ouvert les portes d'institutions initialement hermétiques, permettant une triangulation adéquate des données empiriques et garantissant la validité scientifique de cette recherche doctorale.

Conclusion

Cette recherche s'est donnée pour objet d'analyser en profondeur les dynamiques complexes de la réaction sociale, tant institutionnelle qu'étatique, face au risque de cyber-fraude bancaire et aux défis majeurs de la protection des données à caractère personnel au sein du système financier de la République Démocratique du Congo. Dans un contexte métropolitain kinois marqué par une numérisation fulgurante des flux financiers et une asymétrie croissante des menaces, la problématique centrale s'est articulée autour de la confrontation entre le « droit des livres » (*law in books*), incarné par la Loi n°20/017 de 2020 et les directives de la Banque Centrale du Congo et le « droit en action » (*law in action*) vécu quotidiennement par les gestionnaires de la sécurité. Pour répondre à cette interrogation, le dispositif méthodologique a privilégié une démarche qualitative, combinant l'ancrage ethnographique à la Gombe, la participation observante, l'échantillonnage théorique par choix raisonné indexé sur le principe de saturation (Glaser & Strauss, 1967), et l'analyse de contenu thématique (Bardin, 1977).

La mise en œuvre de ce protocole a permis d'aboutir à trois grands ordres de résultats empiriques et théoriques. D'une part, la recherche démontre la robustesse technique de la réaction formelle interne des banques commerciales. Face aux graves carences de l'état civil congolais et au péril de la multi-identité, les établissements déploient des technologies de prévention situationnelle avancées (reconnaissance faciale KYC, cryptage des flux, dispositifs panoptiques d'audit trail). Ce faisant, les banques exercent un pouvoir disciplinaire qui se substitue de manière corporatiste aux défaillances de l'Etat pour sanctuariser l'espace transactionnel. D'autre part, l'étude met en relief la puissance coercitive de la Banque Centrale du Congo, qui parvient à discipliner le marché privé grâce à la violence économique de la sanction du « débit d'office » immédiat appliqué aux comptes de règlement des banques non conformes à l'Instruction n°42 sur la monétique.

Cependant, le résultat le plus saillant et le plus critique de cette investigation réside dans la mise au jour des limites structurelles de cet échafaudage réglementaire. Un fossé profond sépare la sophistication des textes légaux de l'effectivité de leur application. La Loi n°20/017 du 25 novembre 2020 demeure un fétiche juridique à portée essentiellement symbolique (Carbonnier, 1969 ; Bourdieu, 1986), neutralisée par la non-opérationnalisation budgétaire et humaine de l'Autorité de Protection des Données Personnelles (APDP) et par l'analphabétisme technique d'un appareil judiciaire ordinaire incapable d'interpréter un fichier de log (*audit trail*). Surtout, l'enquête clinique révèle l'existence d'un « choc des pouvoirs » permanent, où la rationalité technique du contrôle interne se heurte à la violence informelle des élites politiques kinoises.

Les interférences clientélistes et la « politique du ventre » (Bayart, 1989) s'immiscent régulièrement au cœur des flux bancaires pour étouffer les enquêtes de fraude complexes, générant une anomie organisationnelle et contraignant les auditeurs à développer des stratégies d'auto-censure prudentielle face aux réseaux criminels connectés au régime.

La contribution majeure de cet article sur le plan épistémologique est de démontrer que derrière la neutralité apparente du "code" informatique, des algorithmes de sécurité et des pare-feu, se cachent des rapports de force humains, politiques et sociologiques profonds. La cyber-sécurité en milieu bancaire africain ne peut être appréhendée comme une simple situation-problème (Kienge-kienge, 2005)

d'ingénierie logicielle ou de conformité juridique abstraite. Elle est un champ de lutte où se confrontent la rationalité bureaucratique globale (isomorphisme par rapport au RGPD ou aux normes ISO 27001), les contraintes du capitalisme international (exigences du réseau SWIFT) et les logiques néo-patrimoniales locales propres aux Etats en mutation. Seule une ethnographie criminologique compréhensive, capable de s'insérer au plus près des acteurs et de négocier l'accès aux secrets institutionnels, s'avère apte à déconstruire ces dynamiques informelles pour en restituer la complexité systémique.

En guise d'ouverture, deux perspectives de recherche future s'imposent à la lumière des résultats de cette étude. Il s'avère indispensable de mener des études comparatives au sein de la sous-région de la SADC et de la CEMAC, afin d'évaluer si le mimétisme juridique des standards occidentaux (tels que le RGPD ou la Convention de Malabo) produit les mêmes effets purement symboliques et les mêmes résistances étatiques dans d'autres pays d'Afrique centrale. Face à la surveillance panoptique croissante exercée par la Banque Centrale sur le réseau bancaire traditionnel, les réseaux de cyber-prédation se déplacent massivement vers l'écosystème du *Mobile Money* et de la finance décentralisée. Ce secteur fluide, caractérisé par l'informalité des agents de terrain et l'absence de traçabilité d'état civil, constitue la nouvelle frontière de la cyber-fraude en Afrique subsaharienne. Les recherches ultérieures devront adapter le protocole qualitatif formalisé dans cet article pour pénétrer les mailles de ce filet financier informel.

Références bibliographiques

AYRES, I., & BRAITHWAITE, J. (1992). *Responsive regulation: Transcending the deregulatory beach*. New York, NY: Oxford University Press.

BALDWIN, R., CAVE, M., & LODGE, M. (2012). *Understanding regulation: Theory, strategy, and practice* (2nd ed.). Oxford, United Kingdom: Oxford University Press.

BARDIN, L. (1977). *L'analyse de contenu*. Paris, France: Presses Universitaires de France (PUF).

BAYART, J.-F. (1989). *L'État en Afrique: La politique du ventre*. Paris, France: Éditions de l'Espace de politique / Fayard.

BECCARIA, C. (1764). *Des délits et des peines*. Livourne, Italie: Marco Coltellini.

BECKER, H. S. (1963). *Outsiders: Studies in the sociology of deviance*. New York, NY: The Free Press.

BECK, U. (1986). *La société du risque: Sur la voie d'une autre modernité*. Francfort-sur-leMain, Allemagne: Suhrkamp Verlag.

BIERNACKI, P., & WALDORF, D. (1981). Snowball sampling: Problems and techniques of chain referral sampling. *Sociological Methods & Research*, 10(2), 141-163. Beverly Hills, CA: Sage Publications.

BOURDIEU, P. (1986). La force du droit: Eléments pour une sociologie du champ juridique. *Actes de la recherche en sciences sociales*, 64(1), 3-19. Paris, France: Éditions du Seuil.

CARBONNIER, J. (1969). *Flexible droit: Pour une sociologie du droit sans rigueur*. Paris, France: Librairie Générale de Droit et de Jurisprudence (LGDJ).

CHAMBLISS, W. J. (1978). *On the take: From petty crooks to presidents*. Bloomington, IN: Indiana University Press.

CLARKE, R. V. (1980). Situational crime prevention: Theory and practice. *British Journal of Criminology*, 20(2), 136-147. London, United Kingdom: Oxford University Press.

COHEN, L. E., & FELSON, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588-608. Washington, DC: American Sociological Association.

COMMAILLE, J. (2015). *À quoi sert le droit ?*. Paris, France: Gallimard.

CRESSEY, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Glencoe, IL: The Free Press.

DELEUZE, G. (1990). Post-scriptum sur les sociétés de contrôle. *Pourparlers (19721990)*, 240-247. Paris, France: Éditions de Minuit.

DIMAGGIO, P. J., & POWELL, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147-160. Washington, DC: American Sociological Association.

FAVRET-SAADA, J. (1977). *Les mots, la mort, les sorts: La sorcellerie dans le Bocage*. Paris, France: Gallimard.

FOUCAULT, M. (1975). *Surveiller et punir: Naissance de la prison*. Paris, France: Gallimard.

FOUCAULT, M. (2004). *Sécurité, territoire, population: Cours au Collège de France (19771978)* (F. Ewald & A. Fontana, Éds.). Paris, France: Gallimard / Seuil.

GARLAND, D. (2001). *The culture of control: Crime and social order in contemporary society*. Chicago, IL: University of Chicago Press.

GEERTZ, C. (1973). *The interpretation of cultures: Selected essays*. New York, NY: Basic Books.

GIDDENS, A. (1984). *The constitution of society: Outline of the theory of structuration*. Berkeley, CA: University of California Press.

GLASER, B. G., & STRAUSS, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Chicago, IL: Aldine Publishing Company.

LYON, D. (1994). *The electronic eye: The rise of surveillance society*. Minneapolis, MN: University of Minnesota Press.

KIENGE – KIENGE, R. (2005), *Le contrôle policier de la délinquance des jeunes à Kinshasa, une approche ethnographique en criminologie*, Thèse de doctorat : Université catholique de Louvain- la-Neuve.

MITNICK, K. D., & SIMON, W. L. (2002). *The art of deception: Controlling the human element of security*. Indianapolis, IN: Wiley Publishing.

MONJARDET, D. (1996). *Ce que fait la police: Sociologie de la force publique*. Paris, France: Éditions de la Découverte.

MOROZOV, E. (2013). *To save everything, click here: The folly of technological solutionism*.

New York, NY: PublicAffairs.

OLIVIER DE SARDAN, J.-P. (1995). La politique du terrain: Sur la production des données en anthropologie. *Enquête: Anthropologie, Histoire, Sociologie*, 1(1), 71109. Marseille, France: Éditions Parenthèses.

ROGERS, C. R. (1942). *Counseling and psychotherapy: Newer concepts in practice*. Boston, MA: Houghton Mifflin Company.

SHEARING, C. D., & STENNING, P. C. (1983). Private security and private justice: The recognition of an under-examined phenomenon. *Crime and Justice*, 5, 193229. Chicago, IL: University of Chicago Press.

SUTHERLAND, E. H. (1949). *White-collar crime*. New York, NY: Dryden Press.

VAUGHAN, D. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. Chicago, IL: University of Chicago Press.

WACQUANT, L. (2000). *Corps et Âme: Carnets d'un apprenti boxeur*. Marseille, France: Éditions Agone.

WALL, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge, United Kingdom: Polity Press.

WARUSFEL, B. (2017). La souveraineté numérique et le droit. Dans L. Carayon (Éd.), *La souveraineté numérique* (pp. 45-58). Paris, France: Éditions de l'Harmattan.

WEICK, K. E. (2001). *Making sense of the organization*. Malden, MA: Blackwell Publishing.