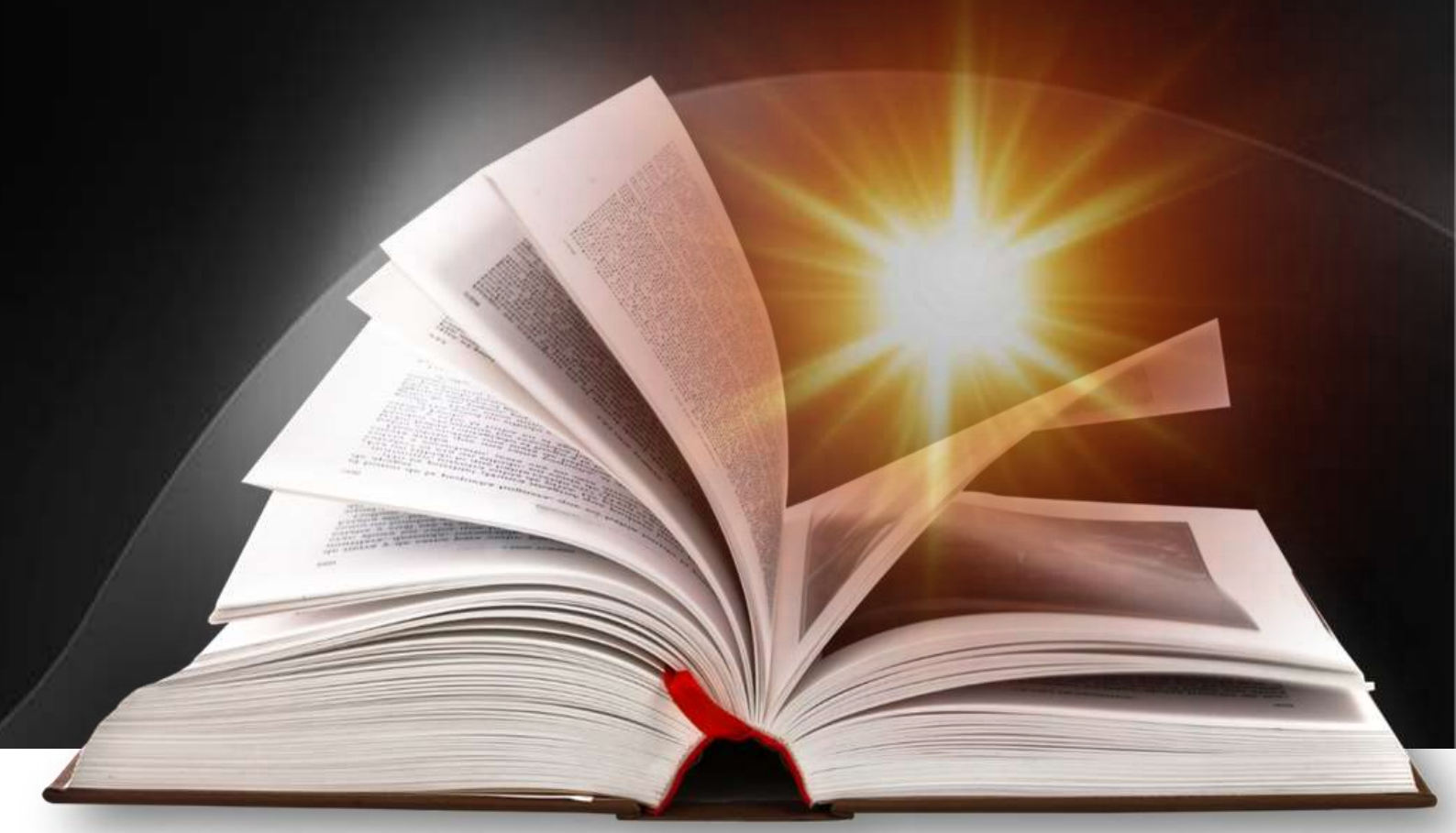
ISSN
: 2790-6248
: 2790-6256

Revue Panafricaine de la Jeunesse

- Pan African Youth Journal -



Volume 3, n°3, Sept - Déc 2024

EDITIONS LUMUMBA
Un nouvel élan de l'édition africaine

Association Panafricaine pour l'Encadrement et la Formation de la Jeunesse

African Scientific Universe

Afrindala Group

© Editions Lumumba

La cybercriminalité et ses atteintes à la vie privée des agents de la Direction des Recettes du Haut-Katanga à Lubumbashi

[Cybercrime and its impact on the privacy of the agents of the Revenue Directorate of Haut-Katanga in Lubumbashi]

FUNGA LUAJI Emery
Université de Lubumbashi / RD Congo

ISSN
: 2790-6248
: 2790-6256

Revue Panafricaine de la Jeunesse

- Pan African Youth Journal -

DOI : https://doi.org/10.58610/RPJ.2790.6248.6256.31

Editions Lumumba I Afriscience I Association Panafricaine pour l'Encadrement et la Formation de la Jeunesse

EDITIONS LUMUMBA
Un nouvel élan de l'édition africaine

Revue Panafricaine de la Jeunesse (RPJ)
ISSN : 2790-6248
e-ISSN : 2790-6256
© Editions Lumumba - APANAEFJ
Bibliothèque Nationale du Congo I Ordonnance loi n° 89-010
du 11 janvier 1989 – Permis d'implantation n° BNC/DPHK/08/2022

Afrindala Group

La Revue Panafricaine de la Jeunesse (RPJ) est une revue scientifique internationale, interdisciplinaire et interactive. Elle se veut un lieu de diffusion de travaux de recherche originaux et substantiels sur diverses questions liées aux enjeux et défis des sociétés africaines, dans toutes les disciplines scientifiques. La RPJ est enregistrée par le Centre International de l'ISSN (International Standard Serial Number) sous les numéros ISSN : 2790-6256 et e-ISSN : 2790-6248.

Les Éditions Lumumba, sous la houlette du label panafricain Afrindala Group, branche scientifique « Afriscience », sont une maison d'édition établie en RD Congo conformément à l'Ordonnance-Loi n° 89-010 du 11 janvier 1989 et opérant sous le permis d'établissement n° BNC/DPHK/08/2022. Enregistrées auprès de l'Agence Internationale de l'ISBN, par l'intermédiaire de l'Agence Francophone pour la Numérotation Internationale du Livre (AFNIL), les Éditions Lumumba sont repértoriées sous l'identifiant éditeur : 978-2-38489.

Le comité scientifique international, composé d'enseignants et de spécialistes d'Afrique et d'ailleurs, assure une diversité d'expertises et de perspectives. En tant que membre de Crossref, une organisation américaine participant à l'indexation globale du contenu scientifique, les Éditions Lumumba bénéficient d'un préfixe DOI (10.58610) pour attribuer un DOI unique à chaque œuvre éditée. Cela permet aux publications d'être accessibles à des milliers de membres de Crossref et à des centaines d'organisations, y compris des institutions scientifiques et universitaires du monde entier, augmentant considérablement la visibilité et l'impact international des travaux publiés.

Les Éditions Lumumba s'appuient sur un vaste réseau de distributeurs et de partenaires internationaux, incluant des universités, des ONG et de grandes plateformes telles que CAIRN.INFO (la plus grande bibliothèque numérique francophone), DILICOM, OpenEdition Books, la plateforme Afriscience, etc.

© Editions Lumumba

Revue Panafricaine de la Jeunesse

— RPJ —

- Pan African Youth Journal –

Revue scientifique internationale, interdisciplinaire et interactive

Périodicité : avril, août et décembre
Prix du numéro : 45 USD
Abonnement annuel : 100 USD
Version numérique disponible sur : www.afriscience.org

Suivez-nous sur nos réseaux sociaux :
@editionslumumba | @afriscience

Imprimé en République Démocratique du Congo

Tél. (+243) 90 43 370 19
Email : contact@editionslumumba.com
Site web : www.editionslumumba.com
Siège : 10, avenue de la Moto croisement boulevard M'siri, ville de Lubumbashi, RD Congo

Editorial

Chères lectrices, chers lecteurs,

C'est avec une ferveur renouvelée et un sens aigu de notre responsabilité intellectuelle que nous vous convions à franchir les portes de cet espace unique, dédié à la célébration de l'intelligence et de la créativité africaines dans toute leur splendeur. La **Revue Panafricaine de la Jeunesse (RPJ)** se positionne ici comme un carrefour où se croisent réflexion académique et innovation pragmatique, dans une quête inlassable de réponses aux défis multiformes de notre époque.

Dans un monde en constante mutation, cette revue se veut une boussole, orientant les esprits curieux vers des territoires inexplorés de la pensée critique. Chaque article, chaque réflexion, chaque témoignage publié dans ces pages transcende les barrières géographiques et culturelles, tissant une toile intellectuelle où l'Afrique dialogue avec le reste du monde. Loin des visions simplistes et uniformisantes, cette revue offre une lecture plurielle et nuancée, où la diversité des perspectives est érigée en moteur de compréhension et de transformation.

Ce numéro particulier s'inscrit dans une dynamique audacieuse : celle de faire rayonner non seulement l'ingéniosité scientifique, mais également la richesse des expériences humaines qui en sont le socle. À travers des contributions d'une rigueur exemplaire, nos auteurs dévoilent des idées qui jaillissent des contextes de résilience et d'espoir, et qui trouvent leur force dans l'intersection de disciplines, de cultures et de visions. Ces pages témoignent d'une Afrique en mouvement, une Afrique créative et porteuse de solutions pour un avenir plus inclusif et durable.

Loin d'être un simple réceptacle de savoirs, cette revue est un espace vivant, animé par une communauté d'auteurs, de chercheurs et de penseurs qui s'engagent à poser des jalons pour le développement scientifique et social. Ensemble, ils bâtissent des ponts entre l'universel et le particulier, entre le local et le global, démontrant que l'innovation africaine est non seulement pertinente, mais essentielle à l'évolution des sociétés contemporaines.

Notre comité éditorial, appuyé par une équipe scientifique d'excellence, veille à garantir une qualité irréprochable à chaque publication. Ce travail collaboratif, empreint de rigueur et d'éthique, reflète notre ambition de faire de la RPJ un vecteur de transformation sociale et une tribune où les voix africaines s'expriment avec force et conviction. Chaque numéro est une invitation à repenser les paradigmes dominants, à déconstruire les stéréotypes, et à envisager de nouvelles façons de concevoir le rôle de l'Afrique dans le monde.

Alors que vous parcourez ces pages, nous espérons que vous serez saisi(e)s par l'ampleur des idées, la profondeur des analyses et la portée des visions qui y sont présentées. Plus qu'une lecture, cette revue est une expérience, une immersion dans un univers où la science et la pensée critique façonnent les contours d'un avenir prometteur.

Plongez dans cette aventure intellectuelle, où l'Afrique se réinvente et inspire le monde. Ensemble, poursuivons le rêve d'un continent qui, par sa richesse intellectuelle et sa créativité, se hisse au rang des acteurs incontournables de la réflexion mondiale.

Bonne lecture et bienvenue dans cet univers d'idées, d'innovations et de découvertes !

L'équipe éditoriale

Equipe de la revue

Comité de rédaction :

- Directeur de Publication : M. le Pr. Basile Mulwani Makelele, RD. Congo
- Rédacteur en chef : M. le Pr. Philippe Kasongo Maloba Tshikala, Belgique
- Rédacteur en chef Adjoint : M. Valery Ngoy Ndala, RD. Congo
- Secrétaire éditorial : William Agbaka, Bénin
- Coordinateur du processus d'adhésion : M. Josué Lwamba, RD Congo
- Gestionnaire administratif : Banon Zinsou Côme, Bénin
- Gestionnaire financière : Clarisse Mwelwa Bilepo, RD Congo
- Coordinateur des partenariats : Fidèle Bukasa Kabwe, RD Congo
- Traducteur en chef : Dr. Fo-Koku D. Woameno, Togo
- Responsable de la publication en ligne : M. Mayou Nkensa, Cameroun

Comité scientifique :

- Dr. Abdoulaye OUEDRAOGO, PhD en Gestion de Projets, Ministère de l'Economie, des Finances et du Plan (MEFP) au Burkina Faso, Burkina Faso
- Dr. Abi-Kaberou Gildas, PhD en Sciences de l'Education, Ecole Normale Supérieure (ENS/Porto-Novo) et à l'Institut de Psychologie de Travail et des Organisations (PTO), Bénin
- Dr. Adaba Koffi Amessou, PhD en Sociologie (Sociologie Politique), Université de Lomé, Togo
- Dr. Adrien Mazanga Nakunyi, PhD en Sciences de l'Education, Université Simon Kimbangu de Lubumbashi, RD Congo
- Dr. Akimou TCHAGNAOU, PhD en Sciences de l'Education et de la Formation, Université André Salifou de Zinder, Niger
- Dr. AMBOMBI EYOLO Azede Espoir, PhD en criminologie, PhD en pédagogie, en psychologie des organisations, Directeur de la chaire MBA, Afrikan campus, Formateur à l'école de police du Congo, Congo Brazza
- Dr. Amoussou Franck, PhD en Linguistique Anglaise Appliquée, Université d'Abomey-Calavi, Bénin
- Dr. Andi Cudai Nur, PhD en Education, Makassar State University, Indonésie
- Dr. Ballo Drisa, PhD en Roman africain, Université des Lettres et des Sciences Humaines de Bamako, Mali
- Dr. Basile Mulwani Makelele, PhD en Psychologie, Université de Lubumbashi, RD Congo
- Dr. Bernard Aristide BITOUGA, PhD en Anthropologie (Anthropologie sociale et culturelle), Université de Douala, Cameroun

- Dr. Bruno Duovany BEKOLO ENGOUDOU, PhD en ethnologie-anthropologie, Université de Douala, Cameroun
- Dr. Carine Nadège BOUMA, PhD en Droit privé, Université de Bamenda, Cameroun
- Dr. Dédé Terence, PhD en Lettres, Université Félix Houphouët-Boigny, Côte d'Ivoire
- Dr. Doba SORO, PhD en Anthropologie Sociologie, Université Polytechnique de Man, Côte d'Ivoire
- Dr. Dre NGONO OSSANGO PANGRACE, PhD en Psychologie, Spécialité : Psychologie du développement humain, Université de Yaoundé, Cameroun
- Dr. ESSOME LELE GIslain Arnaud, PhD en Langue et Linguistique espagnoles, option Sémiotique iconotextuelle, Asociación de Cervantistas ECLLA – Études du Contemporain en Littératures, Langues et Arts, UJM Saint-Étienne UFD LLSL – Littératures, Langues et Sciences du Langage, Univ. Maroua, Cameroun
- Dr. Fidélie NTSHIKALA MBUYA, PhD en Psychologie, Université de Kolwezi, RD Congo
- Dr. Fo-Koku D. Woameno, PhD en Littérature et civilisation américaine, Université de Lomé, Togo
- Dr. Gano Nouhou, PhD en Analyse du discours, Université cheikh Anta Diop de Dakar, Sénégal
- Dr. Gninneyo Sylvestre-Pierre NIYA, PhD en Sciences de l'éducation, Spécialité : Politiques éducatives (Éducation inclusive), Ecole Normale Supérieure/Koudougou, Burkina Faso
- Dr. Ilunga Bumute Christian, PhD en Psychologie, Université de Likasi, RD Congo
- Dr. Jean Pierre Kayembe Kayembe, PhD en Chimie, Rhodes University, South Africa
- Dr. Jeef TSHITAMBA KABALA, PhD en Sciences Politiques et Administratives, Université de Lubumbashi, RD Congo
- Dr. José NGOY WA NGOY TWITE, PhD en Psychologie du travail, spécialité : psychopathologie du travail, Université de Kolwezi, RD Congo
- Dr. Kabiena Kuluila Pierre Valery Dieudonné, PhD en Droit, Université Officielle de Mbuji-Mayi, RD Congo
- Dr. Kabuya-Kabeya Sthilobo Hilaire, PhD en Droit, Université Officielle de Mbuji-Mayi, RD Congo
- Dr. Kaniki Wa Cilombo Joseph-Robert, PhD en Droit, Université Officielle de Mbuji-Mayi, RD Congo
- Dr. KONGUE Toyindou, PhD en Géographie, Option Géographie humaine, rurale et économique, Université de Lomé, Togo

- Dr. KONÉ PATRICE M'BÉTIEN, PhD en Criminologie, Université Félix Houphouet Boigny, Côte- d'Ivoire
- Dr. KOUADIO BAYA BOUAKI, PhD en Sociologie, Université Félix Houphouët-Boigny, Côte d'Ivoire
- Dr. KOUADIO Yao Adoman Francis, PhD en Sociologie politique, West Africa Social Science Laboratory, Côte- d'Ivoire
- Dr. Lago Blé Angelin, PhD en Histoire, Université Jean-Lorougnon Guede, Côte d'Ivoire
- Dr. Lokossou Bonaventure, PhD en audiovisuel et de l'information, de la communication, Université d'Abomey-Calavi, Bénin
- Dr. Matthias Cinyabuguma, PhD en Economie, Banque mondiale, RD Congo
- Dr. MBANGI MBONZALE, PhD en sciences sociales, Université de Lubumbashi, RD Congo
- Dr. MBULA MUSASA M. Serge Caleb, PhD en Sciences (Géologie du Pétrole), Université Pédagogique Nationale (UPN)/Kinshasa, RD Congo
- Dr. Metsena Ndjavoua, PhD en Histoire des Relations Internationales, Université de Maroua (Cameroun)/ Institut Universitaire de Développement International (IUDI), Cameroun
- Dr. Mohamed Atteyoub H. dit Modibo SIDIBÉ, PhD en Sciences Économiques et de gestion, Université des sciences sociales et de gestion de Bamako, Mali
- Dr. Moussa Coulibaly, PhD en Sciences du langage et de la Communication, Université Assane Seck de Ziguinchor du Sénégal, Sénégal
- Dr. Moussa Dourfaye Abdoul-kadze, PhD en santé, Santé publique, épidémiologie, biostatistique, recherche en santé, Hôpital de référence de Maradi, Niger
- Dr. Nebie Boukary, PhD en Sciences du Langage, Université de Fada N'Gourma, Burkina Faso
- Dr. Ngala Ntumba Peter, PhD en Droit, Université Officielle de Mbuji-Mayi, RD Congo
- Dr. NGOIE KAZIMINGI Patrick, PhD en Sciences de l'Education, Université de Lubumbashi, RD Congo
- Dr. Ngoy Ndombe Alain, PhD en Droit, Université de Lubumbashi, RD Congo
- Dr. Nkongolo Mulami Kapweka Alphonse, PhD en Droit, Université Officielle de Mbuji-Mayi, RD Congo
- Dr. Norbert Aimé MELINGUI AYISSI, PhD en Histoire, Université de Douala, Cameroun
- Dr. Ntita Ntita Jean Christ, PhD en Droit, Université Officielle de Mbuji-Mayi, RD Congo

- Dr. Nyebe Atangana Sandrine, PhD en Sciences de l'Education, Membre du Laboratoire BONHEURS, CY Cergy Paris Université, Cameroun
- Dr. Outéndé TOUNDOU, PhD en Physiologie végétale, Agrophysiologie, fertilisation des sols, Université de Lomé, Togo
- Dr. Philippe KASONGO MALOBA TSHIKALA, PhD en Psychologie, Université de Lubumbashi, Belgique
- Dr. Raymond-Bernard AHOUANDJINOU, PhD en socio-anthropologie, andragogue et juriste, Association Internationale des Sociologues de Langue Française et du Centre d'Etudes et de Recherche en Education et Interventions Sociales pour le Développement (CEREID), Bénin
- Dr. Richard Muimbi Kitumba, PhD en Droit, Université de Kabinda, RD Congo
- Dr. SAIDI Hicham, PhD en sciences économiques et gestion, Université Moulay Ismaïl, FSJES – Meknès, Maroc
- Dr. SIDIBÉ OUSMANE, PhD en Linguistique du Discours, Université de San Pedro, Côte d'Ivoire
- Dr. Tamia Jules-Amstrong, PhD en Psychologie, Spécialité : Psychologie du Travail et des Organisations, Université Félix Houphouët-Boigny, Côte d'Ivoire
- Dr. Xie Huifang, PhD en Sciences de l'Education, Université pédagogique d'Etat du Liaoning, Chine
- Prof. Dr. DIEU LOBA ARNAUD, Professeur titulaire CAMES, Université Félix Houphouet Boigny, Côte d'Ivoire.

Revue Panafricaine de la Jeunesse
Revue scientifique internationale
ISSN : 2790-6248 I e-ISSN : 2790-6256
Editions Lumumba
Un nouvel élan de l'édition africaine
Email : contact@editionslumumba.com
Afriscience
African Scientific Universe

La cybercriminalité et ses atteintes à la vie privée des agents de la Direction des Recettes du Haut-Katanga à Lubumbashi

[Cybercrime and its impact on the privacy of the agents of the Revenue Directorate of Haut-Katanga in Lubumbashi]

FUNGA LUAJI Emery
Université de Lubumbashi / RD Congo

Résumé

Cet article explore la cybercriminalité et ses impacts sur la vie privée des agents de la Direction des Recettes du Haut-Katanga (DRH-Kat) à Lubumbashi. Définie comme tout acte illégal impliquant des systèmes informatiques — tels que le vol d'identité, la fraude financière, et la diffusion de contenus illicites — la cybercriminalité représente une menace croissante. Les agents de la DRH-Kat subissent divers risques, notamment la diffamation, l'atteinte à la vie privée et les violations du droit d'auteur, amplifiés par un manque de formation et de sensibilisation. Ces vulnérabilités sont accentuées par l'absence d'un cadre légal adapté et la non-ratification de la Convention sur la cybercriminalité en République Démocratique du Congo (RDC). L'article met en lumière l'évolution des infractions informatiques, qui passent des délits traditionnels aux crimes liés à l'usage des réseaux informatiques comme Internet. Les impacts sont multiples : sociaux, économiques, politiques, individuels et professionnels, freinant le développement technologique et économique. Pour lutter efficacement contre ce fléau, l'article préconise une coopération internationale renforcée et une stratégie nationale basée sur des cadres légaux solides, des programmes de formation, et une sensibilisation accrue.

Mots-clés : cybercriminalité, vie privée, phishing, malwares, RDC, cadre légal, sensibilisation, DRH-Kat, coopération internationale.

Abstract

This article explores cybercrime and its impact on the privacy of agents at the Revenue Directorate of Haut-Katanga (DRH-Kat) in Lubumbashi. Defined as any illegal act involving computer systems—such as identity theft, financial fraud, and the dissemination of illicit content—cybercrime poses a growing threat. DRH-Kat agents face various risks, including defamation, privacy breaches, and copyright violations, exacerbated by a lack of training and awareness. These vulnerabilities are further heightened by the absence of an adequate legal framework and the Democratic Republic of Congo's (DRC) failure to ratify the Cybercrime Convention. The article highlights the evolution of computer offenses, transitioning from traditional crimes to those associated with the use of digital networks like the Internet. The impacts are broad: social, economic, political, individual, and professional, hindering

technological and economic development. To effectively combat this scourge, the article advocates for strengthened international cooperation and a robust national strategy based on solid legal frameworks, training programs, and increased awareness campaigns.

Keywords: cybercrime, privacy, phishing, malware, DRC, legal framework, awareness, DRH-Kat, international cooperation.

0. Introduction

L'essor croissant des technologies de l'information et de la communication favorise le développement des activités médiatiques, bancaires et des services gouvernementaux numérisés. Cette forte avancée technologique contribue également au développement de nouvelles formes d'actes infractionnels, notamment la cybercriminalité. Associé au développement de l'ordinateur, le délit informatique est apparu à la fin des années cinquante. La délinquance informatique est un phénomène récent, lié au développement technologique et à l'utilisation de l'ordinateur. L'avènement des réseaux informatiques transnationaux a conduit à l'émergence des pirates informatiques (Net, 2005). Ce développement des technologies de télécommunication a transformé la délinquance informatique en cybercriminalité. Cela a permis aux délinquants de sortir du champ des comportements criminels strictement liés à l'informatique pour entrer dans celui des actes antisociaux liés au cyberespace, notamment en lien avec les réseaux informatiques, comme Internet.

D'après les Nations Unies, la cybercriminalité recouvre tout comportement illégal impliquant des opérations électroniques qui compromettent la sécurité des systèmes informatiques et des données qu'ils traitent. Dans une acception plus large, elle désigne tout acte illégal commis à l'aide d'un système ou d'un réseau informatique, ou en relation avec celui-ci. Ainsi, parmi ces comportements illégaux particulièrement accentués dans la cybercriminalité, nous trouvons : la fraude financière : l'escroquerie, la fraude à la carte de paiement, le vol, l'atteinte à la propriété intellectuelle ; la diffusion de contenus illicites : la pornographie, la diffusion de matériel raciste et xénophobe ; l'accès illégal. (J., Larivière, 1998 ; SCRS, 2000 ; Statistique Canada, 2002 ; Lexique des termes juridiques, 2007).

Le terme cybercriminalité a été inventé à la fin des années 1990, lorsque l'Internet commençait à se répandre en Amérique du Nord. Il a été employé pour la première fois par un sous-groupe du G8, appelé le « groupe de Lyon », lors d'une réunion tenue à Lyon, en France. Ce terme désigne tous les types de délits perpétrés sur Internet ou via les nouveaux réseaux de télécommunication. Selon M. Benedikt (1992), la cybercriminalité englobe à la fois les nouvelles formes de criminalité spécifiquement liées aux technologies modernes de l'information et les délits déjà connus, mais commis à l'aide de l'informatique plutôt que par des moyens traditionnels. Pour S. Branigan (2005), la cybercriminalité désigne toute criminalité pour laquelle l'ordinateur constitue l'objet ou l'instrument principal de perpétration.

Au regard de ces définitions, le système informatique apparaît comme le principal outil des cybercriminels pour mener à bien leurs actes malveillants. Selon la Convention sur la cybercriminalité (2013), l'ordinateur, Internet et autres dispositifs technologiques sont assimilés à un système informatique. Celui-ci est défini comme tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, assurant, ou dont un ou plusieurs éléments assurent, l'exécution d'un traitement automatisé de données au moyen d'un programme (BPIEPC, 2003).

En effet, de nombreuses méthodes sont utilisées par les délinquants du cyberespace pour commettre leurs actes malveillants avec une grande réussite. Ces méthodes consistent, d'une part, à exploiter la faille humaine, et, d'autre part, à exploiter la faille informatique. En résumé, deux principales méthodes se distinguent.

Les méthodes exploitant la faille humaine visent à manipuler l'intelligence humaine. Parmi elles, on trouve :

- Le **phishing** (une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations personnelles auprès des internautes, généralement des informations bancaires) (Canada, 2003).
- Le **scam** (escroquerie d'origine nigériane, réalisée par des moyens informatiques via le réseau Internet. Son mécanisme est bien orchestré, point par point).

Concernant les méthodes exploitant la faille informatique, elles consistent à exploiter les données et les systèmes informatiques. Le **spam** et le **malware** figurent parmi ces méthodes.

- Le **spam** est une méthode consistant à envoyer des messages non sollicités sur des boîtes aux lettres électroniques, des télécopieurs, des boîtes vocales et des téléphones mobiles. Autrement dit, il s'agit d'envoyer des messages à des inconnus pour leur demander de visiter un site, d'inclure un individu dans une liste de diffusion sans son consentement, ou de diffuser sur un forum de discussion des messages sans rapport avec le thème du forum.
- Le **malware** désigne un ensemble de logiciels malveillants utilisés par les pirates informatiques pour exploiter les failles informatiques des ordinateurs et des réseaux, notamment ceux des utilisateurs sur Internet, à leur insu. Ces pirates emploient ces logiciels pour duper, escroquer les utilisateurs sur Internet, et voler des informations confidentielles. Le malware est classé en plusieurs catégories selon son mode de fonctionnement et d'action. Les malwares peuvent être classés comme suit : le virus, le ver, le wabbit, le cheval de Troie, la porte dérobée (Backdoors en anglais), le logiciel espion, le keylogger, l'exploit, les scamwares ou rogues anti-spyware, es rootkits (D. Carter, 1995).

Nous avons observé que les agents de la Direction des Recettes du Haut-Katanga (DRH-Kat) sont exposés à des comportements criminels qui portent atteinte à leur vie privée. Cette situation soulève plusieurs interrogations :

- Quels sont les différents niveaux de vulnérabilité auxquels la cybercriminalité représente un danger pour les agents de la DRH-Kat ?
- Quelles sont les raisons sous-jacentes à la méconnaissance de la cybercriminalité parmi les agents de la DRH-Kat ?

Nos hypothèses sont formulées de la manière suivante :

- La cybercriminalité constitue un danger à différents niveaux, notamment social, économique, politique, individuel et professionnel, pour les agents de la DRH-Kat.
- Le vide juridique, l'absence de formations adéquates et le manque de sensibilisation des agents sont les principales raisons expliquant la méconnaissance de la cybercriminalité parmi les agents de la Direction des Recettes du Haut-Katanga/Lubumbashi.

Les objectifs de cette étude sont les suivants :

- Identifier les différents niveaux de vulnérabilité auxquels la cybercriminalité représente un danger pour la vie privée des agents de la DRH-Kat à Lubumbashi ;
- Analyser les raisons sous-jacentes à la méconnaissance de la cybercriminalité parmi les agents de la DRH-Kat à Lubumbashi.

1. Méthodologie

Dans le cadre de cette étude, le champ de recherche porte spécifiquement sur la *Direction des Recettes du Haut-Katanga* de l'Assemblée provinciale du Haut-Katanga (D.R.H.KAT), une institution publique cruciale dans la gestion des ressources financières de la province du Haut-Katanga. Le siège de cette direction est situé à Lubumbashi, chef-lieu de la province, précisément dans le Bâtiment Grana, sur l'Avenue Kasaï à l'angle de Moero, en plein centre-ville. Cette localisation stratégique permet une interaction directe avec les principaux acteurs économiques et administratifs de la province, ce qui fait de cet endroit un centre névralgique pour les opérations financières de la région.

Pour mener à bien cette étude, nous avons choisi une approche méthodologique mixte, intégrant une enquête de terrain, des entretiens libres et l'analyse documentaire. L'enquête, qui a constitué l'outil principal de collecte des données, a été enrichie par des entretiens qualitatifs et l'utilisation de la technique documentaire, permettant ainsi de croiser et valider les informations obtenues. L'objectif était de recueillir des données primaires directement issues des participants, tout en analysant des documents institutionnels et administratifs qui fournissent un contexte supplémentaire à notre recherche.

En ce qui concerne l'échantillonnage, un échantillon *occasionnel* de 50 participants a été retenu, comprenant des agents de la Direction des Recettes du Haut-Katanga, des responsables administratifs et des experts financiers travaillant au sein de cette institution. Les participants ont été choisis en fonction de leur expérience et de leur implication dans les

processus de gestion des recettes publiques, leur âge variant entre 25 et 50 ans. Ce groupe d'échantillonnage reflète un éventail d'âges et d'expériences professionnelles permettant une analyse diversifiée des pratiques et perceptions en matière de gestion financière.

Le traitement des données collectées a été facilité par l'application de l'analyse de contenu, une méthode qui permet d'extraire des significations, des thèmes et des patterns à partir des données qualitatives. Cette analyse a été structurée pour extraire les principaux résultats liés à l'efficacité des mécanismes de collecte et de gestion des recettes dans le Haut-Katanga.

Tableau 1 : Répartition des interrogés selon la tranche d'âge et selon le sexe

Tranche d'âge	Sexe	Total	Pourcentage
25-35 ans	11	11	22
35-45 ans	8	8	16
45-55 ans	6	6	12
Total	25	25	**50**

Source : données de notre enquête de terrain.

Ce tableau présente la répartition des participants en fonction de leur tranche d'âge et de leur sexe. Il montre une répartition équilibrée entre hommes et femmes, avec une majorité de participants dans la tranche d'âge de 25-35 ans. Cette distribution permet de couvrir une large gamme de perspectives et d'expériences au sein de la Direction des Recettes du Haut-Katanga.

2. Résultats

La cybercriminalité est un grand danger pour les victimes. Ce dernier risque d'être le lieu de la prédilection de tous les cybercriminels de la planète qui délocaliseront indubitablement leur activité sur l'intégrité de la victime. Les atteintes sont très sonnantes au niveau social, économique, politique, individuel et professionnel.

Tableau 2 : Réactions des participants sur les atteintes engendrées par la cybercriminalité au niveau social.

Atteintes sociales	Fréquence	Pourcentage (%)
Conflits conjugaux	14	28%
Sentiment de culpabilité	9	18%
Atteintes aux droits fondamentaux de la victime	27	54%
Total	**50**	**100%**

Source : données de notre enquête de terrain.

Dans ce tableau n°2, nous notons que les atteintes aux droits fondamentaux (Intégrité et liberté, dignité, honneur et réputation, respect de la vie privée de la victime.) représentent plus de la moitié des cas recensés (54 %),

soulignant l'impact majeur des violations de l'intégrité, de la dignité et de la liberté des victimes. Les conflits conjugaux constituent 28 % des atteintes sociales, traduisant les répercussions de ces violences sur la cellule familiale. Enfin, le sentiment de culpabilité, bien que représentant une part moindre (18 %), demeure une conséquence psychologique non négligeable. Ces résultats mettent en lumière la nécessité d'actions ciblées pour prévenir et atténuer ces atteintes à la cohésion sociale et au bien-être des victimes.

Tableau 3 : Avis des participants sur la baisse de revenu liée à la cybercriminalité subie

Atteintes économiques	Fréquence (f)	Pourcentage (%)
Escroquerie, fraude à la carte de paiement	11	22%
Vol des données confidentielles ou usurpation d'identité	30	60%
Attaques informatiques sur le réseau	9	18%
Total	**50**	**100%**

Il ressort de ce tableau que le vol des données confidentielles et l'usurpation d'identité constituent la principale atteinte économique subie par les participants (60 %), traduisant la vulnérabilité des données personnelles face aux cyberattaques. L'escroquerie et la fraude à la carte de paiement concernent 22 % des cas, mettant en évidence les risques financiers directs liés aux transactions en ligne. Enfin, les attaques informatiques sur le réseau représentent 18 % des atteintes, soulignant les conséquences techniques pouvant impacter la productivité et la sécurité des activités en ligne. Ces résultats illustrent l'urgence de renforcer les mesures de cybersécurité pour limiter les pertes économiques engendrées par la cybercriminalité.

Tableau 4 : Réactions des participants sur les atteintes engendrées par la cybercriminalité à la mise en place de la politique de développement des TIC

Atteintes au niveau politique	Fréquence (f)	Pourcentage (%)
Déstabilisation du climat et du rendement professionnel	16	32%
Espionnage	7	14%
Méfiance entre collègues	27	54%
Total	**50**	**100%**

Source : données de notre enquête de terrain.

Il ressort de ce tableau que la cybercriminalité a un impact significatif sur l'environnement professionnel et politique au sein de la Direction des Recettes du Haut-Katanga. La principale conséquence relevée est la méfiance entre collègues, citée par 54 % des participants, ce qui témoigne d'une détérioration des relations professionnelles et d'un climat de suspicion au sein de l'institution.

Ensuite, la déstabilisation du climat et du rendement professionnel est mentionnée par 32 % des répondants, soulignant l'impact négatif des cyberattaques sur la productivité et la qualité du travail des agents. Enfin, l'espionnage concerne 14 % des cas, révélant des inquiétudes quant à la protection des informations stratégiques et à la sécurité des données.

Tableau 5 : Opinions des participants sur les atteintes engendrées par la cybercriminalité au niveau physique de la victime

Atteintes au niveau physique	Fréquence (f)	Pourcentage (%)
Troubles musculosquelettiques	14	28%
Burn-out	11	22%
Troubles du sommeil	25	50%
Total	**50**	**100%**

Source : données de notre enquête de terrain.

Dans ce tableau, nous notons que la cybercriminalité ne se limite pas aux conséquences économiques ou sociales ; elle affecte également la santé physique des victimes. D'après les résultats de l'enquête, 50 % des participants souffrent de troubles du sommeil, révélant un stress psychologique intense lié aux cyberattaques, à l'usurpation d'identité ou à la fraude en ligne.

Les troubles musculosquelettiques, mentionnés par 28 % des répondants, traduisent une tension physique accrue, souvent due à une posture prolongée devant les écrans ou à un stress prolongé. Enfin, le burn-out, cité par 22 % des participants, met en évidence un épuisement professionnel causé par la pression et l'insécurité numérique ressenties par les victimes.

Tableau 6 : Avis des participants sur les atteintes engendrées par la cybercriminalité au niveau psychologique de la victime

Atteintes au niveau psychologique	Fréquence (f)	Pourcentage (%)
Stress et anxiété	18	36%
Dépression	15	30%
Perte de confiance en soi	17	34%
Total	**50**	**100%**

Source : données de notre enquête de terrain.

Les répercussions psychologiques de la cybercriminalité sont particulièrement marquées, affectant profondément le bien-être des victimes. Le stress et l'anxiété, cités par 36 % des répondants, sont les atteintes les plus courantes, traduisant une insécurité face à la perte de données personnelles, au chantage ou à l'usurpation d'identité.

La dépression, mentionnée par 30 % des participants, témoigne de l'impact prolongé des cyberattaques, qui peuvent altérer la qualité de vie et

engendrer un repli social. Enfin, la perte de confiance en soi, touchant 34 % des victimes, souligne la difficulté de surmonter l'atteinte à la vie privée et l'humiliation ressentie après une cyberattaque.

Tableau 7 : Opinions des participants sur les atteintes individuelles engendrées par la cybercriminalité

Atteintes au niveau individuel	Fréquence (f)	Pourcentage (%)
Être toujours sous des menaces (atteinte à l'intégrité)	9	18%
Être considéré(e) comme un objet (atteinte à la liberté)	16	32%
Être humilié(e) en public (atteinte à la dignité)	25	50%
Total	**50**	**100%**

Source : données de notre enquête de terrain.

La cybercriminalité entraîne des atteintes individuelles significatives, touchant l'intégrité, la liberté et la dignité des victimes. L'humiliation publique, subie par 50 % des répondants, constitue l'atteinte la plus fréquente. Ce phénomène est souvent exacerbé par la diffusion d'informations personnelles, de fausses accusations ou de cyberharcèlement, ce qui peut entraîner un profond traumatisme social et psychologique.

L'atteinte à la liberté, signalée par 32 % des participants, reflète la perte de contrôle sur sa propre identité numérique. Les victimes se sentent traitées comme de simples objets, manipulées ou exploitées sans leur consentement.

Enfin, l'atteinte à l'intégrité, évoquée par 18 % des répondants, illustre la menace constante pesant sur certaines victimes, qui vivent dans la crainte d'une nouvelle attaque, ce qui peut affecter leur bien-être mental et émotionnel.

Tableau 8 : Réactions des participants sur les atteintes engendrées par la cybercriminalité au niveau professionnel de la victime

Atteintes au niveau professionnel	Fréquence (f)	Pourcentage (%)
Absentéisme	28	56%
Contre-performance	9	18%
Rendement déficitaire	13	26%
Total	**50**	**100%**

Source : données de notre enquête de terrain.

Les résultats montrent que **l'absentéisme** est la principale conséquence professionnelle de la cybercriminalité, touchant **56 %** des victimes. Ce phénomène peut s'expliquer par le stress, l'anxiété et la peur liés aux

attaques numériques, incitant les victimes à s'éloigner de leur environnement de travail.

La contre-performance, mentionnée par 18 % des participants, traduit la difficulté des victimes à maintenir leur efficacité professionnelle après une cyberattaque. L'impact psychologique, le temps perdu à gérer les répercussions et la méfiance accrue contribuent à cette baisse de performance.

Enfin, le rendement déficitaire, signalé par 26 % des répondants, met en évidence les effets négatifs durables sur la productivité. La cybercriminalité perturbe les routines de travail, réduit la motivation et peut même entraîner des pertes économiques pour l'entreprise ou l'institution concernée.

Ces données soulignent l'importance de mettre en place des mesures de cybersécurité renforcées, de sensibiliser les employés aux risques numériques et d'offrir un soutien psychologique et technique aux victimes afin de limiter ces impacts négatifs sur le monde professionnel.

Tableau 9 : Avis des participants sur les atteintes familiales engendrées par la cybercriminalité

Atteintes familiales	Fréquence (f)	Pourcentage (%)
Disputes fréquentes	26	52%
Séparation momentanée	19	38%
Divorce	5	10%
Total	**50**	**100%**

Source : données de notre enquête de terrain.

L'analyse des résultats révèle que 52 % des participants estiment que la cybercriminalité engendre des disputes fréquentes au sein des familles. Ces tensions peuvent être causées par le stress, la méfiance et les conflits liés à l'exposition des données personnelles ou à des fraudes en ligne affectant les finances du foyer.

La séparation momentanée, évoquée par 38 % des répondants, témoigne de l'impact psychologique et émotionnel des cyberattaques, qui peuvent fragiliser les relations conjugales. Le sentiment de trahison, l'inquiétude et l'épuisement émotionnel peuvent pousser les victimes à prendre de la distance pour gérer la situation.

Enfin, 10 % des personnes interrogées signalent que la cybercriminalité peut conduire au divorce. Bien que ce pourcentage soit relativement faible, il met en évidence les conséquences extrêmes que peuvent avoir les cyberattaques sur la stabilité des couples, notamment lorsque celles-ci impliquent des atteintes à la vie privée, du chantage ou des pertes financières importantes.

Ces résultats soulignent la nécessité d'une sensibilisation accrue aux risques liés à la cybercriminalité, ainsi que d'un accompagnement psychologique et juridique pour les victimes et leurs familles afin de prévenir les conflits et préserver l'harmonie familiale.

Tableau 10 : Opinions des participants sur les raisons à la base de la méconnaissance de la cybercriminalité

Raisons de la méconnaissance de la cybercriminalité	Fréquence (f)	Pourcentage (%)
Manque de vulgarisation des textes légaux	16	32%
Non ratification de la convention internationale sur la cybercriminalité	6	12%
Manque de sensibilisation des agents	28	56%
Total	**50**	**100%**

Source : données de notre enquête de terrain.

Les résultats montrent que 56 % des participants considèrent que le manque de sensibilisation des agents est la principale cause de la méconnaissance de la cybercriminalité. Cette lacune entraîne une faible capacité de prévention et de réaction face aux menaces numériques.

Le manque de vulgarisation des textes légaux, évoqué par 32 % des répondants, illustre l'insuffisance d'initiatives visant à rendre les lois accessibles et compréhensibles pour le grand public et les professionnels exposés aux risques cybernétiques.

Enfin, 12 % des participants soulignent que la non-ratification de la convention internationale sur la cybercriminalité constitue un frein majeur à une lutte efficace contre ces délits. L'absence d'un cadre juridique international appliqué empêche une coopération optimale avec d'autres nations et limite les moyens d'action face aux cybercriminels.

Ces résultats mettent en évidence la nécessité de renforcer la sensibilisation des agents, d'adapter les textes légaux aux réalités numériques, et d'accélérer l'intégration de la RDC dans les accords internationaux afin d'améliorer la lutte contre la cybercriminalité.

Tableau 11 : Réactions des participants sur les mécanismes de défense mis en pratique pour lutter contre la cybercriminalité

Mécanismes de défense	Fréquence (f)	Pourcentage (%)
Banalisation	30	60%
Saisie de la hiérarchie	18	36%
Porter plainte	2	4%
Total	**50**	**100%**

Source : données de notre enquête de terrain.

Les données révèlent que la majorité des participants (60%) banalisent les atteintes liées à la cybercriminalité, ce qui démontre un manque de prise de conscience ou une résignation face aux menaces numériques. Cette

tendance peut s'expliquer par un défaut d'information, un manque de moyens de recours, ou encore une faible confiance dans les autorités compétentes.

En revanche, 36% des participants choisissent de saisir leur hiérarchie, ce qui suggère une volonté de signaler les incidents, mais dans un cadre interne, probablement par crainte de représailles ou de complications administratives.

Enfin, seulement 4% des victimes osent porter plainte, révélant un faible recours aux voies judiciaires. Ce constat met en évidence un déficit de confiance dans l'efficacité du système juridique ou un manque de mécanismes adaptés à la protection des victimes de cybercriminalité.

Ces résultats soulignent la nécessité de renforcer la sensibilisation, de mettre en place des procédures claires et accessibles de signalement, et d'encourager les victimes à porter plainte afin de lutter efficacement contre la cybercriminalité.

Tableau 12 : Opinions des participants sur les stratégies mises en place pour sauvegarder leurs informations personnelles et professionnelles

Stratégies de sauvegarde	Fréquence (f)	Pourcentage (%)
Utilisation des logiciels de sécurité	19	38%
Stockage des informations hors site	26	52%
Sauvegarde automatique	5	10%
Total	50	100%

Source : données de notre enquête de terrain.

Les résultats dans ce tableau montrent que la stratégie la plus couramment utilisée pour protéger les informations personnelles et professionnelles est le stockage des données hors site (52% des participants). Cela suggère une prise de conscience des risques liés à la cybercriminalité, notamment la perte ou le piratage des informations sensibles.

Ensuite, 38% des participants adoptent l'utilisation de logiciels de sécurité, tels que les antivirus, pare-feu ou logiciels de chiffrement, afin de renforcer la protection de leurs données. Cela témoigne d'une certaine maturité numérique parmi les agents interrogés.

Enfin, seulement 10% des répondants recourent à la sauvegarde automatique, une pratique pourtant essentielle pour prévenir la perte de données. Ce faible taux révèle un manque de sensibilisation ou une méconnaissance des outils de sauvegarde automatique.

Ces résultats soulignent la nécessité d'intensifier les campagnes de formation et de sensibilisation sur l'importance de la sauvegarde régulière et sécurisée des données, ainsi que l'adoption de pratiques de cybersécurité plus rigoureuses au sein des administrations et entreprises.

3. Discussion

Les résultats de cette étude soulignent l'impact considérable de la cybercriminalité sur divers aspects de la vie des agents de la Direction des Recettes du Haut-Katanga (DRHK) à Lubumbashi. Ces atteintes sont multiples : sociales, économiques, politiques, psychologiques, physiques, professionnelles et familiales. Ces constats rejoignent ceux de plusieurs chercheurs qui ont étudié les conséquences de la cybercriminalité et l'importance des mesures de protection pour limiter ses effets dévastateurs. Net (2005) souligne que la montée en puissance de la cybercriminalité expose les individus, notamment les employés des administrations publiques, à des menaces telles que le vol de données et l'usurpation d'identité.

- **Impact social et psychologique de la cybercriminalité**

L'étude révèle que les atteintes aux droits fondamentaux des victimes (54 %) sont la principale conséquence sociale de la cybercriminalité, suivies des conflits conjugaux (28 %) et du sentiment de culpabilité (18 %). Ces résultats sont cohérents avec les travaux de Wall (2007), qui explique que la cybercriminalité affecte la vie privée des individus et peut entraîner une détérioration de leurs relations sociales et familiales. En effet, les cyberattaques et les fuites de données peuvent exposer des informations sensibles, engendrant ainsi des tensions au sein des foyers et de la société.

Sur le plan psychologique, l'anxiété (36 %), la perte de confiance en soi (34 %) et la dépression (30 %) sont les atteintes les plus fréquemment rapportées par les participants. Ces résultats corroborent ceux de Hinduja et Patchin (2018), qui démontrent que les victimes de cyberharcèlement ou de vol d'identité développent souvent un stress post-traumatique et des troubles dépressifs. Ces effets psychologiques sont également observés par Bauman, Toomey et Walker (2013), qui soulignent que la cybercriminalité, notamment le cyberharcèlement, peut avoir des conséquences émotionnelles graves, allant jusqu'à des idées suicidaires dans certains cas extrêmes.

Branigan (2005) explore le phénomène du cyberharcèlement, qui peut impacter gravement la vie personnelle et professionnelle des victimes. Les agents de la DRH-KAT/Lubumbashi sont exposés à de telles menaces, compromettant leur bien-être socioprofessionnel et leur sécurité physique et psychologique.

- **Conséquences économiques et professionnelles**

L'étude met en évidence la prévalence du vol des données confidentielles et de l'usurpation d'identité (60 %), suivis par la fraude à la carte de paiement (22 %) et les attaques informatiques (18 %). Ces résultats rejoignent ceux de Moore, Clayton et Anderson (2009), qui démontrent que l'usurpation d'identité et le vol de données personnelles sont les formes les plus répandues de cybercriminalité ayant un impact économique direct. De même, Anderson et al. (2013) estiment que les pertes mondiales liées à la cybercriminalité s'élèvent à plusieurs milliards de dollars chaque année, ce qui démontre l'ampleur du phénomène et son impact économique global.

Sur le plan professionnel, l'absentéisme (56 %), la baisse de rendement (26 %) et la contre-performance (18 %) sont des effets notables de la cybercriminalité. Ces résultats concordent avec ceux de Willison et Warkentin (2013), qui expliquent que la cybercriminalité engendre un climat de méfiance et de stress au sein des organisations, affectant directement la productivité des employés. Par ailleurs, McGuire et Dowling (2013) montrent que la cybercriminalité peut provoquer un ralentissement des activités et une perte de compétitivité pour les entreprises, en raison des interruptions causées par les attaques informatiques.

- **Impact politique et institutionnel**

Le rapport du SCRS (2000) met en évidence les différentes formes de cybermenaces qui peuvent cibler les institutions gouvernementales. Pour la DRH-KAT/Lubumbashi, cela implique un besoin urgent de stratégies de prévention et de réponse face aux cyberattaques.

L'un des résultats marquants de cette étude est l'impact de la cybercriminalité sur la méfiance entre collègues (54 %), la déstabilisation du climat professionnel (32 %) et l'espionnage (14 %). Ces résultats sont en accord avec les travaux de Broadhurst et Chang (2013), qui expliquent que la cybercriminalité peut compromettre la sécurité institutionnelle et engendrer une perte de confiance au sein des organisations. Ces résultats soutiennent également ceux de Larivière (1998) qui aborde la question de la confiance dans les transactions en ligne et la nécessité de mesures de sécurité robustes pour protéger les données personnelles. Sa recherche montre que la méfiance entre agents dans le cyberspace a un impact direct sur leur vie professionnelle.

De plus, la faible connaissance de la cybercriminalité, due au manque de sensibilisation (56 %), au manque de vulgarisation des textes légaux (32 %) et à la non-ratification des conventions internationales (12 %), met en évidence les lacunes en matière de gouvernance numérique en République Démocratique du Congo. Ces constats sont également faits par Clough (2010), qui insiste sur l'importance d'une régulation juridique et d'une coopération internationale pour lutter efficacement contre la cybercriminalité.

- **Méconnaissance et réponses face à la cybercriminalité**

Benedikt (1992) discute de l'impact des espaces virtuels sur la perception de soi et de l'identité. Dans le contexte des agents de la DRH-KAT/Lubumbashi, il est essentiel de comprendre comment la présence en ligne affecte leur vie privée et leur dignité. L'un des aspects préoccupants relevés dans cette étude est la banalisation de la cybercriminalité (60 %), suivie de la saisie de la hiérarchie (36 %) et du faible taux de plaintes déposées (4 %). Ces chiffres suggèrent un manque de confiance dans les institutions judiciaires et une résignation face aux cyberattaques. Ces résultats sont corroborés par les travaux de Brenner (2010), qui souligne que le manque de sensibilisation et de cadre juridique efficace favorise un climat d'impunité pour les cybercriminels.

Carter (1995) met l'accent sur l'importance des systèmes de sécurité pour protéger les données sensibles. Sa recherche souligne que l'installation des logiciels de sécurité bien adaptés sont nécessaires pour sauvegarder les informations des employés contre les accès non autorisés. Ses résultats diffèrent des nôtres dans ce sens que nous avons trouvé que le stockage hors site est le système de sécurité appliqué par nos participants afin de protéger leurs données personnelles et personnelles. Toutefois, ces résultats rejoignent les recommandations de Von Solms et Van Niekerk (2013), qui insistent sur la nécessité de renforcer les mesures de cybersécurité en milieu professionnel, notamment par la formation des agents, la mise en place de politiques de protection des données et le recours à des outils technologiques adaptés.

4. Conclusion

La cybercriminalité constitue une menace croissante pour la protection des données et la vie privée des agents de la Direction des Recettes du Haut-Katanga. L'étude menée met en lumière l'ampleur des risques encourus par ces agents face aux cyberattaques, notamment les intrusions informatiques, le vol de données et l'usurpation d'identité. Ces menaces sont exacerbées par une sensibilisation insuffisante à la cybersécurité et par des infrastructures de protection parfois défaillantes.

Les résultats obtenus révèlent que la vulnérabilité des agents est en partie due à un manque de formation spécifique en cybersécurité, à l'absence de protocoles stricts de gestion des accès et à une politique de protection des données encore perfectible. De plus, l'usage d'outils informatiques non sécurisés accroît l'exposition aux cyberattaques.

Face à cette situation, il est essentiel de mettre en place des mesures rigoureuses pour protéger les informations sensibles. Cela passe par le renforcement des systèmes de sécurité informatique, la formation continue du personnel sur les bonnes pratiques numériques et l'adoption de solutions technologiques avancées pour détecter et prévenir les cyberattaques. Une coopération étroite avec les autorités compétentes et les experts en cybersécurité est également recommandée pour anticiper et contrer efficacement ces menaces.

En conclusion, la protection de la vie privée des agents de la Direction des Recettes du Haut-Katanga ne peut être garantie sans une approche proactive et intégrée de la cybersécurité. Une prise de conscience collective et des actions concrètes sont impératives pour assurer un environnement numérique sécurisé et fiable.

5. Bibliographie

Net (2005). *Les FAI mis en cause pour l'accès à un site révisionniste*. http ://www.01net.com/editorial/279716/justice/les-fai-mis-en-causepour-l-acces-a-un-site-revisionniste.

Benedikt, M. (1992). *Cyberspace: First Steps. Cambridge, Massachusetts: Massachusetts Institute of Technology* Press.

Branigan, S. (2005). *High-Tech Crimes Revealed: Cyberwar Stories from the Digital Front*. Boston: Addison-Wesley.

Brenner, S. (2004). *U.S. Cybercrime Law: Defining Offenses. Information Systems Frontiers*, 6 (2), 115-132.

Bureau de la protection des infrastructures essentielles et de la protection civile (BPIEPC) (2003). *Les menaces aux infrastructures essentielles canadiennes*. http://www.ocipep.gc.ca/opsprods/other/TA03-001_f.pdf.

Canada (2003). *Loi visant à empêcher la diffusion sur l'Internet de messages non sollicités*. http://www.parl.gc.ca/37/2/parlbus/chambus/senate/bills/public/ pdf/s-23_1.pdf

Carnegie Mellon Computer Emergency Response Team (CERT) (2004). 2004 E-Crime *Watch Survey Shows Significant Increase in Electronic Crimes*. http://www.cert.org/about/ecrime.html.

Carter, D. (1995). *Computer Crime Categories : How Techno-Criminals Operate*. The FBI Law Enforcement Bulletin. http ://nsi.org/Library/ Compsec/crimecom.html.

Convention sur la cybercriminalité (2013)

Larivière, J. (1998). *Les bibliothèques et la nouvelle loi canadienne sur le Droit d'auteur: un commentaire*. http://www.robic.ca/cpi/Cahiers/10-2/03LariviereW97. htm. (Pas cité dans le texte.)

Lexique des termes juridiques (2007).

Service canadien du renseignement de sécurité (SCRS) (2000). *Opérations informatiques (la « cybermenace »)*. http ://www.csis-scrs.gc.ca/fra/operat/ io2_f.html.

Statistique Canada (2002). *Cybercriminalité: enjeux, sources de données et faisabilité de recueillir des données auprès de la police*. Ottawa: ministère de l'Industrie.



PARTENAIRES ET RESEAUX

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE

CAIRN.INFO CHERCHER, REPÉRER, AVANCER

diliCOM LE RÉSEAU DU LIVRE

Banque du Livre asbl

doi

Crossref Content Registration

MEDIATHEQUE DÉPARTEMENTALE du Gers

MOUVEMENT LAUDATO SI' Catholiques pour notre maison commune

parcours formation

MOOC Gestion de Projet

MAXITY

CS4ME CIVIL SOCIETY FOR MALARIA ELIMINATION

10.000 {CODEURS} 2015-2025

UNITED FOR HUMAN RIGHTS

COPAS

RESEAU ELIKYA

FORUM INTERNATIONAL de GOMA pour la RESOLUTION des CONFLITS

Youth for Human Rights International

AGAPE asbl

REVUE PLURIDISCIPLINAIRE AFRICAINE DE L'ENVIRONNEMENT

AS

AGOS EFFICACITÉ SOLIDARITÉ PAIX

IJAS

Scopalto ACADEMIA

Editions Lumumba, un nouvel élan de l'édition africaine

10, avenue de la Moto x boulevard Ms'iri, Quartier Gambela, commune de Lubumbashi, ville de Lubumbashi, République démocratique du Congo
Tél. : 00243 90 433 70 19
Mail : contact@editionslumumba.com
www.editionslumumba.com

Imprimé en République démocratique du Congo

©Edition Lumumba, décembre 2024

Afrindala Group
« New African Generation »
www.afrindalagroup.com

Association Panafricaine pour l'Encadrement et la Formation de la Jeunesse (APANAEFJ)
Courriel : info@apanaefj.org
Site web : www.apanaefj.org

Siège : 10, Avenue de la Moto croisement Boulevard M'siri, Ville de Lubumbashi, RD Congo

APANAEFJ

REVUE PANAFRICAINE DE LA JEUNESSE

Revue scientifique internationale, interdisciplinaire et interactive

Publiée par les Editions Lumumba
Avec le soutien
d'Afriscience

&

Association Panafricaine pour l'Encadrement et
la Formation de la Jeunesse
(APANAEFJ)

Courriel : rpj@apanaefj.org
Site web : www.apanaefj.org
Tél. (+243) 973738975
Siège : 10, avenue de la Moto croisement boulevard M'siri, ville de Lubumbashi, RD Congo