UNIVERSITÉ DE YAOUNDÉ I
***
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE DE YAOUNDÉ
***
DÉPARTEMENT DE GÉNIE INFORMATIQUE
***
HUMANITÉS NUMÉRIQUES

THE UNIVERSITY OF YAOUNDE I
***
NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE
***
DEPARTMENT OF COMPUTER ENGINEERING
***
DIGITAL HUMANITIES

Résumés des Exposé

Rédigé par :

FANTA YADON Félicité (chef) 22P069

Supervisé par :

M. Thierry MINKA

Les outils de rédaction de mémoires

La rédaction d'un mémoire ne se limite pas à la simple production de contenu : c'est une démarche méthodique et exigeante qui requiert une gestion rigoureuse des sources, le respect de normes académiques strictes et une structuration solide du travail. Face à ces exigences, j'ai entrepris d'analyser différents outils numériques afin d'identifier ceux qui, combinés, offrent un environnement de travail à la fois performant et adapté aux besoins réels. Aucun logiciel ne répond de manière exhaustive à toutes les attentes ; c'est donc dans la complémentarité des solutions que réside la véritable efficacité.

La première catégorie étudiée concerne les plateformes de rédaction. J'ai porté une attention particulière à Overleaf, éditeur LaTeX en ligne qui modernise profondément la production académique. Son accessibilité, sa collaboration en temps réel et son respect des standards professionnels en font un outil de référence. Il se distingue notamment par la qualité exceptionnelle de sa typographie, sa gestion avancée des références croisées et la richesse de ses modèles académiques. Néanmoins, la maîtrise de LaTeX requiert un apprentissage initial non négligeable, pouvant constituer un frein pour les débutants. À l'opposé, Microsoft Word reste l'outil le plus répandu grâce à sa familiarité et sa compatibilité universelle. Il facilite la mise en forme structurée via les styles, automatise la création des sommaires et intègre un suivi des modifications idéal pour les échanges avec un directeur de recherche. Cependant, sa gestion bibliographique reste limitée et il peut devenir instable sur des documents volumineux.

Au-delà des éditeurs, la gestion des références constitue un enjeu souvent sous-estimé. Dans ce domaine, Zotero s'impose comme un allié incontournable. Ce gestionnaire de références libre et multiplateforme permet de centraliser efficacement les sources. Ses points forts résident dans la capture automatique des métadonnées depuis les navigateurs, son intégration fluide avec Word et Overleaf via des extensions dédiées, ainsi que son support de milliers de styles bibliographiques. Sa synchronisation en ligne et ses nombreuses extensions renforcent encore sa flexibilité.

Mon analyse révèle que la véritable valeur de ces outils réside dans leur articulation harmonieuse. Ainsi, plusieurs combinaisons optimisées peuvent être proposées selon les profils. Pour un étudiant en début de parcours ou issu des sciences humaines, l'association Word + Zotero constitue une solution équilibrée : elle allie un environnement familier et une gestion bibliographique enrichie. Pour les disciplines scientifiques nécessitant une typographie soignée et une gestion avancée des équations, la combinaison Overleaf + Zotero est particulièrement pertinente. Zotero assure la gestion et l'exportation BibTeX, tandis qu'Overleaf garantit une présentation académique irréprochable. Enfin, pour les travaux en co-direction ou les thèses collectives, le duo Overleaf + Zotero Groups crée un espace collaboratif efficace : Zotero Groups centralise une bibliothèque partagée tandis qu'Overleaf permet une rédaction simultanée fluide.

En somme, le choix des outils doit s'adapter au profil de l'étudiant et aux exigences du travail à accomplir. S'il est clair que la synergie entre Overleaf et Zotero offre une solution de grande qualité académique, il convient de rappeler que ces instruments, aussi puissants soient-ils, ne remplacent pas la profondeur du contenu. Une maîtrise équilibrée des outils et une recherche rigoureuse demeurent les véritables fondations d'un mémoire réussi.

Bilan de l'investigation numérique sur les Réseaux Sociaux

Ce projet pédagogique d'investigation numérique a constitué une exploration approfondie des dynamiques d'influence et d'engagement sur les réseaux sociaux, à travers la conception méthodique d'un faux profil TikTok consacré à la sensibilisation en cybersécurité. La démarche mise en œuvre a su articuler rigueur technique et responsabilité éthique. Elle s'est appuyée sur l'utilisation d'outils pertinents, tels que les services de messagerie temporaire pour préserver l'anonymat, et sur l'exploitation des outils statistiques intégrés à la plateforme afin d'évaluer précisément l'impact des publications. Le choix d'une thématique centrée sur la cybersécurité s'est avéré particulièrement judicieux : il a permis d'aborder des sujets sensibles tout en maintenant une orientation éducative et préventive claire. La conception des contenus, mêlant supports visuels percutants, tonalité humoristique et messages pédagogiques, a illustré l'importance d'une communication adaptée au public cible pour maximiser l'engagement sans compromettre la qualité informative.

L'analyse des retombées a mis en évidence l'efficacité de la stratégie déployée. Les publications ont suscité des interactions significatives, en particulier celles traitant des thématiques liées aux mots de passe, aux dangers du Wi-Fi public et aux arnaques de phishing. Ces contenus ont enregistré plusieurs centaines de vues et de nombreuses réactions, témoignant de la pertinence et de l'actualité des sujets abordés. Toutefois, l'expérience a également révélé la délicatesse de la frontière entre la sensibilisation légitime et la manipulation potentielle, soulignant ainsi la nécessité d'un cadre éthique strict pour encadrer ce type d'exercice.

Les enseignements tirés de cette expérimentation soulèvent des réflexions essentielles quant à l'usage des faux profils dans un contexte pédagogique. Si cette méthode s'est révélée efficace pour capter l'attention et diffuser des messages de prévention, elle impose d'instaurer des limites claires et des mécanismes de régulation rigoureux. L'expérience a montré que la crédibilité et l'impact des contenus reposaient autant sur leur forme que sur leur fond, et que la maîtrise des codes culturels propres à la plateforme constituait un levier essentiel pour atteindre le public visé. Ces constats confirment la valeur ajoutée des approches immersives dans l'enseignement de la cybersécurité, tout en mettant en lumière la complexité de leur mise en œuvre.

En définitive, cette investigation démontre la pertinence des réseaux sociaux en tant qu'outils de sensibilisation aux enjeux numériques, tout en rappelant la responsabilité qui incombe aux investigateurs dans leur utilisation. L'équilibre entre efficacité pédagogique et intégrité éthique émerge comme la principale leçon de cette expérience. Elle ouvre des perspectives prometteuses pour le développement de pratiques d'investigation numérique innovantes, responsables et encadrées. La généralisation de ce type d'exercices dans les formations spécialisées gagnerait ainsi à s'accompagner de protocoles institutionnels garantissant le respect des individus et la finalité strictement éducative des démarches menées.

Analyse de la falsification de conversations numériques : cas de WHATSAPP

Ce travail pratique a mis en évidence, avec une efficacité particulièrement révélatrice, la facilité avec laquelle il est possible de falsifier des échanges sur la messagerie WhatsApp à l'aide d'outils largement accessibles tels que *Chatsmock* et *Adobe Photoshop*. La reproduction d'une conversation compromettante fictive entre un enseignant et une étudiante a illustré le potentiel considérable de manipulation qu'offrent ces technologies. *Chatsmock* permet de générer en quelques minutes une interface de discussion crédible, tandis que *Photoshop* affine les détails graphiques pour atteindre un degré de réalisme difficilement discernable à l'œil non averti. Cette combinaison technique interroge profondément la fiabilité des captures d'écran en tant qu'éléments de preuve numérique, notamment dans les contextes judiciaires ou disciplinaires où la véracité des échanges revêt une importance cruciale.

L'analyse comparative des différents outils de falsification met en lumière une évolution préoccupante des capacités de manipulation numérique. Bien que *Chatsmock* présente certaines limites liées à la reproduction des interfaces récentes et de certaines fonctionnalités avancées, son couplage avec des logiciels de retouche d'image compense largement ces faiblesses. Par rapport à d'autres solutions telles que *FakeChat* ou *WhatsFake*, la méthodologie employée dans cette étude se distingue par une combinaison équilibrée entre accessibilité et sophistication. Cette situation rend la détection de ces falsifications particulièrement complexe et requiert une expertise forensique capable d'identifier des anomalies fines, qu'elles soient graphiques ou présentes dans les métadonnées associées.

Les implications pour les pratiques d'investigation numérique sont considérables. La démocratisation de ces outils remet en question la valeur probatoire des simples captures d'écran, longtemps considérées comme des preuves fiables. Les enquêteurs doivent désormais développer des compétences techniques renforcées pour authentifier les documents numériques, tandis que les instances judiciaires sont appelées à adapter leurs procédures de collecte et d'évaluation des preuves. Le risque d'utilisation malveillante de ces falsifications dans des contextes de conflits interpersonnels ou professionnels constitue une menace réelle pour la réputation des individus et l'intégrité des procédures légales ou disciplinaires.

En définitive, cette expérimentation met en lumière l'urgence d'une approche critique, méthodique et techniquement outillée dans l'évaluation des preuves numériques. Les recommandations issues de cette analyse préconisent de privilégier l'extraction directe des données depuis les appareils comme méthode d'authentification, de renforcer la formation des acteurs judiciaires et des experts en criminalistique numérique, et d'instaurer des protocoles de vérification rigoureux intégrant l'analyse des métadonnées et la recherche d'artefacts de manipulation. Face à la montée en puissance des techniques de falsification, l'évolution parallèle des méthodes d'investigation est indispensable pour maintenir la confiance dans l'intégrité des preuves numériques.

Contexte africain et montée des cybermenaces

L'Afrique connaît aujourd'hui une transformation numérique rapide, accompagnée d'une augmentation préoccupante des cyberattaques. Selon les données d'INTERPOL (2024), chaque organisation en Afrique subit en moyenne plus de 3 000 attaques par semaine. Cette vulnérabilité accrue s'explique par plusieurs facteurs structurels : une maturité institutionnelle encore limitée en matière de cybersécurité, une pénurie importante d'expertise locale (moins d'un spécialiste pour 100 000 habitants), l'obsolescence des infrastructures informatiques et une forte dépendance vis-à-vis de prestataires étrangers pour l'hébergement des données.

Dans ce contexte, l'investigation numérique s'impose comme un pilier stratégique pour comprendre et contrer les menaces cyber. Elle repose sur une méthodologie rigoureuse comprenant l'identification des incidents, la collecte et la préservation des preuves numériques, leur analyse technique, ainsi que la rédaction de rapports exploitables juridiquement.

I Analyse des incidents majeurs (2015–2025)

L'étude des dix incidents les plus marquants survenus entre 2015 et 2025 met en lumière l'ampleur et la diversité des cybermenaces en Afrique :

— **Afrique du Sud (2021)** — L'attaque par ransomware contre *Transnet* a paralysé les principaux ports du pays, occasionnant des pertes estimées à 60 millions de dollars.

— **Maroc (2025)** — La violation de la *Caisse Nationale de Sécurité Sociale* a exposé les données de 2 millions de salariés et 500 000 entreprises, révélant des failles critiques dans les systèmes d'information.

— **Cameroun (2024)** — L'attaque contre *Eneo* a perturbé les systèmes de facturation électrique, impactant des centaines de milliers d'usagers.

— **Égypte (2024)** — Le ransomware *GhostLocker 2.0* a ciblé simultanément 30 organisations, démontrant un haut degré de sophistication.

— **Maroc (2020–2021)** — Le scandale *Pegasus* a révélé la vulnérabilité des communications aux logiciels espions étatiques.

— **Côte d'Ivoire** — Le piratage de plusieurs banques a reposé sur des campagnes de phishing ciblant des cadres, illustrant l'ingénierie sociale comme vecteur d'attaque majeur.

— **Tunisie (2021)** — L'attaque contre le système de santé a entraîné des retards dans des traitements médicaux essentiels, montrant que les cyberattaques peuvent avoir des conséquences vitales.

— **Éthiopie (2023)** — Le piratage d'*Ethiopian Airlines* a compromis les données de milliers de passagers, illustrant les risques liés au cyber-espionnage industriel.

— **Nigeria (2018)** — Une fraude au *mobile money* chez *MTN* a mis en évidence les failles de sécurité dans les systèmes de paiement électronique.

— **Nigeria (2015–2016)** — Le piratage de la *Banque centrale du Nigeria* a provoqué des pertes de plusieurs dizaines de millions de dollars, révélant les vulnérabilités des infrastructures financières nationales.

Ces incidents mettent en évidence des tendances préoccupantes : sophistication croissante des attaques, impact économique majeur et diversification des secteurs ciblés (infrastructures critiques, systèmes financiers, santé, transport, etc.).

II Recommandations stratégiques

Face à ces défis, plusieurs actions prioritaires s'imposent :

— **Renforcement des capacités locales** : former massivement des experts en cybersécurité pour pallier le déficit de compétences.

— **Création de centres régionaux CERT/CSIRT** : assurer une coordination efficace et une réponse concertée aux menaces transfrontalières.

— **Harmonisation juridique** : aligner les cadres légaux autour de la *Convention de Malabo* afin de garantir une réponse cohérente au niveau continental.

— **Souveraineté numérique** : développer un *cloud africain souverain* et promouvoir l'hébergement local des données pour réduire la dépendance extérieure.

— **Cyber-résilience économique** : mettre en place des fonds de soutien pour les PME et renforcer la gouvernance numérique dans les entreprises publiques.

Ces mesures combinées permettraient de renforcer durablement la sécurité du paysage numérique africain et de mieux anticiper les menaces à venir.

Les Deepfakes Vocaux dans l'Investigation Numérique

Le deepfake vocal représente une avancée technologique majeure issue des progrès récents en intelligence artificielle et en apprentissage profond. Cette technologie permet de **synthétiser et de cloner la voix humaine avec un réalisme saisissant** à partir de simples échantillons audio. Son évolution, marquée par des étapes clés comme le développement de *WaveNet* en 2016 et la démocratisation d'outils open-source, a rendu le clonage vocal accessible au grand public. Si ses applications légitimes dans les domaines de l'accessibilité, du doublage et de la préservation patrimoniale sont prometteuses, le détournement malveillant de cette technologie pose des défis inédits pour la sécurité numérique et l'investigation judiciaire.

Dans le contexte de l'investigation numérique, les deepfakes vocaux menacent fondamentalement l'intégrité des preuves audio en compromettant le **triptyque confidentialité–fiabilité–opposabilité (CRO)**. La facilité avec laquelle on peut créer des enregistrements falsifiés remet en cause la valeur probante des éléments audio dans les procédures judiciaires. L'analyse forensique doit désormais intégrer des techniques de détection sophistiquées capables d'identifier les artefacts subtils laissés par la synthèse vocale. La démonstration pratique réalisée avec *MINIMAX Audio* illustre parfaitement cette menace : l'outil permet de générer des clones vocaux quasi indétectables à l'oreille humaine, soulignant l'urgence de développer des contre-mesures efficaces.

Face à ces risques, plusieurs axes de prévention s'imposent. La **détection technologique** nécessite le développement d'outils spécialisés analysant les signatures acoustiques et les anomalies spectrales caractéristiques des voix synthétiques. La **sensibilisation des utilisateurs** et la **formation des professionnels** constituent un volet essentiel pour reconnaître les tentatives de fraude. Sur le plan réglementaire, l'encadrement juridique doit évoluer pour imposer le **marquage des contenus générés** et définir des sanctions dissuasives. Enfin, le **renforcement des méthodes d'authentification**, combinant reconnaissance vocale dynamique et authentification multi-facteur, représente une protection indispensable contre les usurpations d'identité.

En définitive, le deepfake vocal incarne le double visage de l'innovation technologique : *source de progrès notables dans certains domaines, mais aussi menace potentielle pour la confiance numérique*. La maîtrise de cette technologie et de ses implications devient une compétence essentielle pour les investigateurs numériques. Seule une approche multidimensionnelle, associant vigilance technologique, cadre juridique adapté et éthique rigoureuse, permettra de tirer parti des avantages du deepfake vocal tout en en limitant les utilisations malveillantes.

La Reconnaissance Faciale dans l'Investigation Numérique

La reconnaissance faciale s'est imposée comme un **outil biométrique majeur** dans le paysage technologique contemporain, particulièrement dans le domaine de l'investigation numérique. Son principe fondamental repose sur un système biométrique organisé autour de quatre modules : *l'acquisition des données faciales*, *l'extraction de caractéristiques*, *la comparaison par appariement* et *la prise de décision*. Ce processus permet soit l'identification d'un individu parmi une base de données (recherche 1 :N), soit la vérification d'une identité déclarée (recherche 1 :1).

Les méthodes de reconnaissance ont considérablement évolué, passant des approches classiques telles que l'analyse en composantes principales (PCA) ou les modèles géométriques locaux, aux techniques modernes de **deep learning**, qui offrent une précision accrue mais complexifient la compréhension des mécanismes décisionnels internes.

Si cette technologie présente des **atouts opérationnels indéniables** — notamment sa rapidité de traitement et sa capacité à analyser de vastes volumes de données visuelles — elle soulève également des préoccupations multiples. Sur le plan technique, les performances peuvent chuter significativement en conditions réelles, et les architectures de type « boîte noire » compliquent l'explication des décisions. Les vulnérabilités de sécurité, telles que les attaques adversariales ou les tentatives d'usurpation par deepfakes, remettent en cause la fiabilité des résultats.

D'un point de vue éthique et sociétal, les risques de **biais algorithmiques**, les atteintes potentielles à la vie privée et les effets dissuasifs sur les comportements publics appellent à une vigilance accrue. Juridiquement, l'absence de base légale claire et les questions de responsabilité en cas d'erreur représentent des défis majeurs pour une utilisation régulée.

Pour encadrer de manière responsable le déploiement de cette technologie, **particulièrement dans le contexte camerounais**, plusieurs recommandations s'imposent. Il est essentiel de **documenter rigoureusement** les pipelines techniques et de procéder à des **tests locaux** pour évaluer les performances sur des données représentatives de la diversité démographique. La **protection des données biométriques** doit être renforcée par des mesures de chiffrement et des contrôles d'accès stricts.

Sur le plan éthique, la réalisation d'études d'impact et d'audits de biais réguliers est indispensable. Juridiquement, l'alignement sur le cadre existant — notamment la loi sur les données personnelles — et l'exigence d'une **validation humaine** pour les décisions critiques constituent des garde-fous nécessaires.

En définitive, la reconnaissance faciale représente un **outil puissant pour l'investigation numérique**, à condition d'être déployée dans un cadre strictement défini. Son utilité opérationnelle doit être mise en balance avec les impératifs de protection des droits fondamentaux. La réussite de son implémentation au Cameroun dépendra de la mise en place d'une **gouvernance robuste**, combinant supervision technique continue, conformité juridique et respect des principes éthiques, afin de concilier innovation technologique et préservation des libertés individuelles.

L'Investigation Numérique au Cameroun : Un Pilier de la Police Judiciaire Moderne

L'investigation numérique s'est imposée comme un **pilier fondamental de la police judiciaire moderne**, particulièrement dans un contexte camerounais marqué par la digitalisation accélérée et l'évolution des menaces criminelles. Cette discipline spécialisée permet d'accéder à des preuves invisibles dans le monde physique en récupérant des données supprimées, en analysant les métadonnées et en exploitant l'ensemble des traces numériques laissées par les utilisateurs. Elle offre ainsi une **scène de crime virtuelle** complémentaire aux investigations traditionnelles, permettant d'identifier et de tracer les auteurs grâce à l'analyse des adresses IP, des journaux système et des données de géolocalisation.

La reconstitution chronologique des événements devient ainsi possible avec une précision inédite, tandis que les procédures rigoureuses de collecte et de conservation garantissent l'**admissibilité des preuves devant les tribunaux**.

Les domaines d'application de l'investigation numérique au Cameroun couvrent l'ensemble du spectre criminel. Dans la lutte contre la cybercriminalité, elle a permis le **démantèlement de réseaux de fraude en ligne à Douala** grâce à l'analyse des transactions numériques et au traçage des adresses IP. Face à la criminalité transfrontalière et au terrorisme, l'extraction et l'analyse des messages sur les téléphones saisis dans l'Extrême-Nord ont contribué à **cartographier les réseaux logistiques de Boko Haram**.

La criminalité financière et économique bénéficie également de ces techniques, comme en témoigne le **démantèlement d'un réseau de détournement de fonds publics en 2021** après l'analyse des fichiers numériques provenant d'ordinateurs administratifs. Les crimes violents, la protection de l'enfance contre la pédopornographie, et même les enquêtes judiciaires classiques trouvent dans l'investigation numérique un **allié précieux pour établir des preuves solides et irréfutables**.

Cependant, le déploiement efficace de l'investigation numérique se heurte à plusieurs défis substantiels au Cameroun. L'**explosion du volume et de la complexité des données** représente un obstacle majeur : un smartphone peut contenir plus de 128 Go d'informations à analyser, nécessitant des semaines de traitement. Le **respect des droits fondamentaux**, notamment la protection de la vie privée garantie par l'article 9 de la Constitution, impose un équilibre délicat entre les impératifs d'enquête et les libertés individuelles.

L'évolution technologique rapide exige une **formation continue des enquêteurs**, tandis que le coût des équipements spécialisés — une station forensic complète avoisinant les 25 millions de FCFA — limite l'accessibilité de ces outils. La **pénurie d'expertise**, avec moins de 50 experts certifiés sur l'ensemble du territoire, et la **concentration des compétences à Yaoundé et Douala** compliquent encore la généralisation de ces pratiques investigatrices.

Malgré ces contraintes, l'avenir de l'investigation numérique au Cameroun s'annonce comme un **enjeu stratégique pour la sécurité nationale**. Le renforcement des capacités passe nécessairement par des investissements soutenus dans la **formation des enquêteurs**, l'**acquisition d'équipements modernes** et l'**adaptation du cadre juridique** aux spécificités des preuves numériques.

La **collaboration internationale**, déjà bien établie avec Interpol et Europol, doit être consolidée pour faire face à la dimension transnationale de la cybercriminalité. Face à l'émergence de nouvelles menaces comme les deepfakes, l'intelligence artificielle et le métavers, la police judiciaire camerounaise doit anticiper ces mutations technologiques pour maintenir son efficacité opérationnelle.

En définitive, l'investigation numérique n'est plus une simple compétence spécialisée, mais bien une **condition indispensable pour assurer la souveraineté et la sécurité numérique du pays** dans les années à venir.

Cryptographie et Protocole ZK-NR : Vers une Preuve Numérique Opposable

D'un simple outil de chiffrement, la cryptographie est devenue un **pilier essentiel** pour garantir l'**authenticité** et la **valeur légale** des preuves dans l'espace numérique. Alors que les transactions et les communications dématérialisées se multiplient, il ne suffit plus d'assurer la **confidentialité** des échanges ; il faut aussi pouvoir en **prouver l'origine de manière irréfutable** et empêcher qu'un expéditeur ne nie être à l'origine d'un message compromettant.

C'est dans cet esprit qu'émergent des protocoles comme **ZK-NR** (*Zero-Knowledge Non-Repudiation*), qui visent à concilier la sécurité technique avec les impératifs de l'investigation légale.

Le **protocole ZK-NR** représente une avancée majeure en introduisant une **architecture cryptographique modulaire** et **résistante aux attaques quantiques**. En utilisant des *preuves à divulgation nulle de connaissance* (ZKP), il permet de certifier la validité d'une information — par exemple, l'intégrité d'un document ou l'authenticité d'une transaction — sans en révéler le contenu sensible.

Cette approche préserve la confidentialité des données tout en créant une **trace vérifiable et inaltérable**, renforçant ainsi la **confiance dans les preuves numériques produites**.

Ce protocole s'inscrit dans un paysage plus large, structuré autour du **« trilemme CRO »** (Confidentialité, Fiabilité, Opposabilité), une contrainte théorique qui établit l'impossibilité de satisfaire simultanément une confidentialité absolue, une fiabilité totale et une parfaite opposabilité juridique.

ZK-NR et les primitives qui lui sont associées cherchent à optimiser cet équilibre délicat. Ils permettent notamment de transformer la **chaîne de possession des preuves** en un processus **cryptographiquement scellé**, assurant ainsi une traçabilité complète et une résistance à la falsification depuis la collecte jusqu'à la présentation devant un tribunal.

En définitive, l'émergence de ces technologies marque un **tournant pour l'investigation numérique moderne**. Elles élèvent la preuve digitale du statut de simple donnée collectée à celui de **témoin cryptographique incontestable**, capable de répondre aux exigences rigoureuses des procédures judiciaires.

En réconciliant la **rigueur algorithmique** et le **droit**, des frameworks comme ZK-NR préfigurent une nouvelle ère où la **vérité numérique peut être établie de manière à la fois scientifique et juridiquement opposable**, renforçant ainsi l'intégrité des enquêtes dans un monde de plus en plus dématérialisé.