International Journal of Economic Studies and Management (IJESM)
ISSN 2789-049X
Int. J. Econ. Stud. Manag. 6, No.1 (JANUARY-2026)

Le rôle de la Conformité Règlementraire dans la répréssion de la Cybercriminalité au Maroc

The Role of Regulatory Compliance in combatting Cybercrime in Morocco

Professeur. Abderrahim FARACHA
Professeur Universitaire
Faculté des sciences juridiques économiques et sociales Ain Chock (FSJES Casa)
L'Ecole Supérieure de Technologie de Casablanca (ESTC)
L'Université Hassan II - Casablanca - Maroc

Fairouz AMMI AL MASBAHI
Laboratoire de Recherche en Management des Organisations (LAREMO)
L'Ecole Supérieure de Technologie de Casablanca (ESTC)
Université Hassan II – Casablanca – Maroc

Résumé : La transformation numérique rapide au Maroc expose les organisations à une menace croissante de cybercriminalité. Face à cette réalité, la conformité réglementaire s'impose comme un pilier essentiel pour la prévention et la gestion des risques cybernétiques. Cet article examine les défis posés par la cybercriminalité, le cadre réglementaire marocain existant, et les obstacles à une mise en œuvre efficace de la conformité. Il met en lumière les lacunes actuelles en matière de gouvernance et de compétences, et propose des pistes d'amélioration basées sur une approche intégrée et proactive pour renforcer la résilience cybernétique du pays.
Mots-clés : Conformité Réglementaire, Maroc, Cyber sécurité, Cybercriminalité.

Abstract: Cybercrime poses a growing threat in Morocco amid rapid digital transformation. Increased reliance on information technologies has expanded cyber risks for organizations and institutions. Regulatory compliance plays a key role in preventing and managing these threats. This paper examines the main cybercrime challenges, the Moroccan regulatory framework, and compliance-related difficulties. It highlights existing limitations in governance and implementation. The study concludes by proposing integrated and proactive compliance-based approaches to strengthen cyber resilience.

Key Concepts: *Cybercrime, Regulatory Compliance, Governance.*

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.**18297841**

1. Introduction

L'ère numérique a inauguré une période de modernisation sans précédent pour les économies et les administrations publiques mondiales, et le Maroc ne fait pas exception. La dématérialisation des services, l'essor fulgurant des technologies de l'information et de la communication (TIC), ainsi que la généralisation des échanges numériques ont profondément remodelé les dynamiques opérationnelles des organisations. Cependant, cette avancée technologique s'accompagne d'une recrudescence significative des risques liés à la cybercriminalité, qui est devenue une menace stratégique majeure pour la sécurité économique, institutionnelle et sociale des nations. Les cyberattaques, le vol de données, la fraude financière en ligne et les atteintes aux systèmes d'information sont des manifestations courantes de cette criminalité numérique. Leurs conséquences sont multiples, allant des pertes financières directes à l'atteinte à la réputation, en passant par l'érosion de la confiance des utilisateurs et des partenaires économiques. Dans un environnement caractérisé par une interconnexion croissante et une dépendance accrue aux infrastructures numériques, la cybercriminalité se complexifie et se professionnalise, rendant les mécanismes de défense traditionnels souvent insuffisants.

Au Maroc, l'accélération de la digitalisation des services bancaires, le développement du commerce électronique et la mise en œuvre de l'administration électronique ont amplifié l'exposition des entités publiques et privées aux cyber menaces. Cette évolution contraint les acteurs économiques et institutionnels à réévaluer leurs stratégies de gestion des risques numériques. Dans ce contexte, la conformité réglementaire émerge comme un outil central de prévention et de gouvernance. Elle vise à garantir le respect des normes juridiques, techniques et organisationnelles en matière de cyber sécurité et de protection des données. Loin d'être une simple obligation légale, la conformité s'inscrit désormais dans une démarche proactive de gestion des risques et de responsabilisation. Elle implique la mise en place de contrôles internes rigoureux, de procédures de surveillance continues et de programmes de sensibilisation pour réduire les vulnérabilités et renforcer la résilience des systèmes d'information. Néanmoins, sa mise en œuvre effective se heurte à des défis tels que la complexité du cadre réglementaire, le manque de compétences spécialisées et une coordination insuffisante entre les parties prenantes.

Cet article se propose d'analyser comment la conformité réglementaire peut efficacement contribuer à prévenir et à atténuer l'impact de la cybercriminalité au Maroc, tout en assurant la sécurité des systèmes, la protection des données et la consolidation de la confiance des

citoyens et des investisseurs. Pour ce faire, nous identifierons et analyserons les enjeux de la cybercriminalité dans le contexte marocain, examinerons les défis et limites des mécanismes de conformité existants, et explorerons des perspectives et recommandations pour optimiser l'efficacité des dispositifs actuels.

Revue de littérature

1.1. Définition et Typologie

1.1.1. Rappel de la Conformité Règlementaire

La conformité Règlementaire est devenue un pilier majeur de la gouvernance des institutions financières. Elle est à la fois une protection contre les différents risques et un levier de confiance et de réputation grâce à l'intersection entre diverse disciplines à savoir: le droit, la finance et l'éthique. La Conformité est un pôle essentiel quant au bon fonctionnement de établissements financiers; en effet, il s'agit d'une fonction de veille, de contrôle et d'accompagnement qui garantit que la banque agit en accord avec le cadre légal, réglementaire et éthique; tant sur le plan national qu'international. En effet, la conformité est mise en place dans le but de garantir la solidité, la résilience et la fiabilité des institutions bancaires face aux différents risques courants.

1.1.2. Définition et Caractéristiques de la Cybercriminalité

La cybercriminalité englobe l'ensemble des infractions pénales perpétrées via les technologies de l'information et de la communication (TIC) ou ciblant directement les systèmes d'information, les réseaux numériques et les données. Avec l'accélération de la transformation numérique, elle est devenue une forme de criminalité complexe, en constante évolution et transnationale, affectant aussi bien les États que les organisations publiques, les entreprises privées et les individus. Elle se distingue par son caractère immatériel, la rapidité de propagation des attaques et la difficulté d'identifier les auteurs, ce qui complexifie les efforts de prévention et de répression.

La cybercriminalité se caractérise par l'utilisation des technologies numériques comme outil, cible ou environnement de l'acte criminel. Ses traits fondamentaux incluent :

- **Caractère Immatériel :** Les cybercriminels opèrent à distance, souvent depuis des juridictions étrangères, ce qui réduit les risques d'interpellation et complique la poursuite judiciaire.
- **Exploitation des Vulnérabilités :** Elle tire parti des failles techniques des systèmes d'information, mais aussi des vulnérabilités humaines et organisationnelles, telles que

le manque de sensibilisation des utilisateurs ou l'insuffisance des dispositifs de contrôle interne.

- **Capacité d'Adaptation :** Les cybercriminels ajustent constamment leurs méthodes en fonction de l'évolution des technologies et des normes de sécurité, ce qui rend la lutte contre ce phénomène particulièrement dynamique et exigeante.

La Cybercriminalité dans le domaine économique et financier :

La cybercriminalité à caractère financier représente un enjeu stratégique majeur en raison de ses répercussions directes sur la stabilité économique et la résilience des systèmes financiers. Elle se manifeste par une diversité de pratiques illicites, incluant les fraudes en ligne sophistiquées, les intrusions non autorisées dans les infrastructures de paiement électronique et l'exploitation des plateformes numériques à des fins de blanchiment de capitaux. Dans le contexte marocain, la croissance rapide du e-Banking, des services de paiement mobile et du commerce électronique a considérablement accru l'exposition des institutions financières aux cyber menaces. Les impacts économiques de ces attaques sont multidimensionnels : ils engendrent non seulement des pertes financières immédiates, mais aussi des coûts indirects substantiels liés à la restauration et à la sécurisation des systèmes, aux sanctions réglementaires potentielles, ainsi qu'à la dégradation de la confiance et de la réputation des organisations concernées. La cybercriminalité financière constitue donc un défi incontournable, nécessitant la mise en place de mécanismes de gouvernance et de conformité robustes pour préserver la stabilité et la crédibilité du secteur financier marocain.

1.1.3. Typologie de la Cybercriminalité

La typologie des actes de cybercriminalité est en constante évolution, mais les menaces les plus prégnantes peuvent être synthétisées comme suit :

a) **Infractions contre la Confidentialité, l'Intégrité et la Disponibilité des Systèmes :**

- **Piratage (Hacking) :** Accès non autorisé à un système ou à un réseau, souvent dans le but d'exfiltrer des données ou d'en prendre le contrôle.
- **Attaques par Déni de Service Distribué (DDoS) :** Surcharge d'un serveur ou d'un réseau pour le rendre indisponible aux utilisateurs légitimes, perturbant ainsi les services en ligne.

- **Sabotage et Destruction de Données :** Introduction de logiciels malveillants (malwares) visant à altérer, supprimer ou rendre inaccessibles des informations cruciales.

b) **Infractions à Caractère Économique et Financier :**

- **Rançongiciel (Ransomware) :** Cryptage des données d'une victime, suivi d'une demande de rançon pour leur déchiffrement. Cette menace est devenue l'une des plus lucratives et perturbatrices pour les entreprises.

c) **Fraude en Ligne et Phishing :** Utilisation de techniques d'ingénierie sociale pour obtenir des informations confidentielles (identifiants bancaires, mots de passe) en vue de réaliser des transactions frauduleuses.

- **Usurpation d'Identité Numérique :** Utilisation illégale des données personnelles d'un individu pour commettre des actes frauduleux, souvent à des fins financières.

d) **Cyber-espionnage et Cyber-guerre :**

- **Espionnage Numérique :** Collecte illégale et clandestine d'informations sensibles (secrets commerciaux, données gouvernementales) par des acteurs étatiques ou des groupes criminels organisés.
- **Attaques contre les Infrastructures Critiques :** Tentatives de compromission des systèmes de contrôle industriel (SCADA) des services essentiels (énergie, eau, transport), pouvant avoir des conséquences dévastatrices.

1.2. Les différents Enjeux de la Cybercriminalité au Maroc

Au Maroc, les enjeux liés à la cybercriminalité sont particulièrement complexes et multidimensionnels, touchant à la fois la protection des infrastructures critiques, la sécurité des données sensibles, et la confiance numérique. Ces enjeux sont cruciaux pour des secteurs stratégiques comme la finance, l'administration publique et l'industrie. La perception et l'assurance des citoyens et des investisseurs envers l'écosystème numérique national sont directement influencées par la gestion de ces risques. Une cyberattaque majeure peut non seulement entraîner des pertes financières considérables et nuire à la réputation des organisations ciblées, mais aussi compromettre la sécurité nationale en exposant les infrastructures vitales à des vulnérabilités accrues.

La digitalisation accélérée des services publics et privés au Maroc, impulsée par des initiatives telles que Maroc Digital 2020, intensifie l'exposition du Royaume aux cyber-risques. Dans ce contexte, les efforts doivent se concentrer sur la sécurisation des actifs

stratégiques, le renforcement des dispositifs de gouvernance et la préservation de la confiance des parties prenantes. Une gestion efficace de ces défis exige une approche intégrée, combinant prévention technique, conformité réglementaire et sensibilisation continue des acteurs aux risques numériques. Les enjeux se déclinent comme suit :

1.2.1. Enjeux Organisationnels

Pour les organisations publiques et privées, la cybercriminalité représente un risque stratégique majeur, capable d'affecter la continuité des activités, la sécurité des données et la réputation institutionnelle. Une cyberattaque peut provoquer des interruptions de service, compromettre des informations sensibles et entraîner une perte de confiance durable de la part des clients et des partenaires. Ces menaces imposent aux organisations de renforcer leur gouvernance en matière de cybersécurité, d'intégrer la gestion des risques cybernétiques dans leurs stratégies globales et de mettre en place des dispositifs de contrôle interne et de conformité adaptés.

1.2.2. Enjeux Réglementaires

Les enjeux juridiques de la cybercriminalité résident principalement dans l'adaptation des cadres réglementaires aux évolutions technologiques rapides. La lutte contre la cybercriminalité nécessite des normes juridiques claires définissant les infractions, les responsabilités et les sanctions applicables. Au Maroc, la réglementation en matière de cybersécurité et de protection des données personnelles vise à encadrer l'utilisation des systèmes d'information et à renforcer la responsabilité des acteurs. Cependant, l'efficacité de ces dispositifs dépend de leur mise en œuvre effective, de la capacité des autorités à assurer leur contrôle et de la coopération entre les acteurs publics et privés.

1.2.3. Enjeux Sociaux et Confiance Numérique

La cybercriminalité impacte également la confiance numérique, un élément fondamental pour le développement de l'économie digitale. Les atteintes à la vie privée, le vol de données personnelles et les escroqueries en ligne peuvent dissuader les citoyens et les entreprises d'adopter les services numériques. Dans ce contexte, la confiance numérique devient un enjeu social majeur, conditionnant l'adhésion des usagers aux technologies et la réussite des politiques de transformation numérique. La prévention de la cybercriminalité apparaît ainsi comme un facteur clé de renforcement de cette confiance.

- **Confiance des Citoyens**

Les cyberattaques telles que l'usurpation d'identité, le phishing, les ransomwares ou le vol de données personnelles ont un impact direct sur la perception de sécurité des citoyens. Ces incidents peuvent entraîner une réticence à utiliser les services numériques, par crainte de voir leurs informations personnelles compromises. Le renforcement de la confiance des citoyens passe par des mesures de protection robustes et une communication transparente sur les risques et les moyens de s'en prémunir.

- **Confiance des Investisseurs**

Pour les investisseurs, la confiance numérique est un indicateur de la stabilité et de la maturité du marché numérique d'un pays. Un environnement où la cybercriminalité est endémique peut dissuader les investissements étrangers et freiner l'innovation. La mise en place d'un cadre réglementaire solide et de mécanismes de cyber sécurité efficaces est donc essentielle pour attirer et retenir les investissements dans le secteur numérique marocain.

1.3. Cadre Réglementaire Marocain et Conformité

Le Maroc a progressivement mis en place un arsenal législatif et réglementaire visant à encadrer la cyber sécurité et la protection des données, en réponse à l'intensification de la cybercriminalité et à la nécessité de se conformer aux standards internationaux. Ce cadre juridique est constitué de lois nationales, de décrets d'application, de directives institutionnelles et de recommandations internationales, tous concourant à renforcer la sécurité des systèmes d'information et à instaurer un environnement numérique fiable.

1.3.1. Lois et Organismes de luttes Nationaux :

Plusieurs instruments législatifs fondamentaux structurent la cyber sécurité et la protection des données au Maroc :

- **Loi n° 09-08** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (2009) : Cette loi encadre la collecte, le traitement et la conservation des données personnelles, établissant les principes de consentement, de confidentialité et de sécurité des informations. Elle a été complétée par des textes d'application et des décisions de la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP).
- **Loi n° 05-20 relative à la cyber sécurité (2020)** : Cette loi vise à renforcer la sécurité des systèmes d'information des administrations publiques, des établissements et entreprises publics, ainsi que des infrastructures d'importance vitale. Elle définit les obligations en matière de gestion des risques, de notification des incidents et de mise en œuvre de mesures de sécurité techniques et organisationnelles.
- **Loi n° 88-13 (2016) :** Encadre la diffamation et l'injure sur Internet.
- **Articles clés du Code Pénal Marocain (via Loi n° 07-03) :**

- **Article 607-3 :** Incrimine l'accès frauduleux à un STAD (système de traitement automatisé de données).
- **Article 607-4 :** Sanctionne l'interception illégale de données informatiques.
- **Articles 607-10 et 607-11 :** Concernent la fabrication et la mise à disposition d'équipements dédiés aux cybers crimes, ainsi que les confiscations et interdictions.

- **Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP) :** Organe indépendant chargé de veiller à l'application de la Loi 09-08 et de protéger les droits des individus en matière de données personnelles.
- **Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) :** Rattachée à l'Administration de la Défense Nationale, la DGSSI est l'autorité nationale en matière de cyber sécurité. Elle est chargée de définir la stratégie nationale de cyber sécurité, d'élaborer les normes et standards, et de coordonner les actions de prévention et de réponse aux incidents cybernétiques.

1.4. Conformité et Cyber crimes :

La conformité en matière de cyber sécurité ne se limite pas à la stricte application de la loi. Elle implique une approche intégrée de gouvernance, combinant :

- **L'adoption de politiques internes de sécurité claires et régulièrement mises à jour.**
- **La mise en place de processus robustes de gestion des risques cybernétiques.**
- **La formation et la sensibilisation continues des employés aux bonnes pratiques numériques et aux menaces émergentes.**
- **La réalisation d'audits réguliers pour vérifier le respect des normes et identifier les axes d'amélioration.**

Cette approche holistique est essentielle pour bâtir une culture de cyber sécurité au sein des organisations et garantir une protection efficace contre les menaces en constante évolution.

1.4.1. Défis et Limites de la Conformité Réglementaire

Malgré les avancées législatives et institutionnelles, la mise en œuvre effective de la conformité réglementaire en matière de cyber sécurité au Maroc se heurte à plusieurs défis et limites. Ces obstacles peuvent freiner l'efficacité des dispositifs mis en place et compromettre la résilience globale face à la cybercriminalité.

1.4.2. Complexité du Cadre Réglementaire

Le paysage réglementaire marocain, bien que de plus en plus étoffé, peut s'avérer complexe et fragmenté. La multiplicité des textes (lois, décrets, circulaires) émanant de différentes autorités peut rendre difficile pour les organisations, notamment les PME, de comprendre et d'appliquer l'ensemble des obligations. Cette complexité génère parfois une

incertitude juridique et des difficultés d'interprétation, ralentissant l'adoption de mesures de conformité adéquates.

1.4.3. Manque de Compétences Spécialisées

Le Maroc, à l'instar de nombreux pays, fait face à une pénurie de professionnels qualifiés en cyber sécurité et en conformité. Ce déficit de compétences se manifeste à plusieurs niveaux : manque d'experts techniques pour la mise en œuvre et la maintenance des systèmes de sécurité, insuffisance de juristes spécialisés dans le droit du numérique, et besoin de personnel formé à la gestion des risques cybernétiques. Cette lacune limite la capacité des organisations à évaluer correctement leurs risques, à déployer des solutions de sécurité efficaces et à assurer une veille réglementaire constante.

1.4.4. Insuffisance de la Sensibilisation et de la Culture Cyber sécurité

Malgré les efforts, la sensibilisation aux risques cybernétiques et l'adoption d'une culture de cyber sécurité restent des défis majeurs. De nombreux incidents sont le résultat d'erreurs humaines ou d'un manque de vigilance de la part des utilisateurs. L'absence d'une culture forte de la cyber sécurité au sein des organisations et auprès du grand public rend les individus et les systèmes plus vulnérables aux attaques d'ingénierie sociale et aux malwares.

1.5. Coordination et Coopération entre les Acteurs

La lutte contre la cybercriminalité est une responsabilité partagée qui nécessite une coordination et une coopération efficaces entre les différents acteurs : autorités publiques (gouvernement, forces de l'ordre, régulateurs), secteur privé, institutions académiques et société civile. Or, des lacunes peuvent exister dans la fluidité des échanges d'informations, le partage des meilleures pratiques et la mise en œuvre d'actions concertées, ce qui peut affaiblir la réponse globale face aux menaces.

1.5.1. Évolution Rapide des Menaces

La nature dynamique et l'évolution rapide des menaces cybernétiques constituent un défi permanent. Les cybercriminels développent constamment de nouvelles techniques et exploitent de nouvelles vulnérabilités, rendant les dispositifs de sécurité et les cadres réglementaires rapidement obsolètes s'ils ne sont pas régulièrement mis à jour. Cette course à l'armement exige une veille technologique et réglementaire constante, ainsi qu'une capacité d'adaptation rapide des organisations et des autorités.

3. Méthodologie

L'approche méthodologique adoptée dans cet article repose sur une **démarche mixte (qualitative et quantitative)**, privilégiant l'analyse et la synthèse. Elle vise à la fois à décrypter les dynamiques complexes de la cybercriminalité au Maroc, à évaluer l'efficacité du

cadre réglementaire en vigueur et à formuler des recommandations stratégiques fondées sur des données empiriques.

3.1.Type de Recherche

Cette étude adopte une démarche **qualitative, descriptive et analytique**, structurée autour des objectifs suivants :

- L'identification et la contextualisation des enjeux et impacts de la cybercriminalité dans le contexte marocain.
- L'examen critique des mécanismes de conformité réglementaire existants (Loi 05-20, Loi 09-08).
- L'analyse des défis et des limites rencontrés dans la mise en œuvre effective des politiques de cyber sécurité.
- La proposition de recommandations stratégiques pour le renforcement de la prévention et de la gouvernance numérique.

L'approche qualitative est privilégiée pour sa capacité à capturer la complexité des interactions entre acteurs, pratiques et régulations, et à fournir des analyses nuancées des perceptions et des comportements.

3.2.Sources de Données et Méthodes de Collecte

La recherche qui a été effectuée s'appuie sur une **triangulation** de sources, garantissant la validité et la fiabilité des conclusions. Le tableau ci-dessous synthétise les sources mobilisées, la population ciblée et les méthodes de collecte associées ; comme montré dans le tableau ci-dessous :

Type de Source	Population/Cible	Méthode de Collecte	Objectif Principal
Sources Secondaires	Textes législatifs, Rapports institutionnels (DGSSI, CNDP), Littérature académique, Rapports internationaux.	Analyse Documentaire et Codage Thématique.	Établir le cadre légal et conceptuel ; contextualiser les enjeux par une analyse comparative.
Sources Primaires (Qualitatif)	12 Experts (IT, Conformité, Administration publique).	Entretiens Semi-Directifs (enregistrés et retranscrits).	Recueillir des analyses approfondies sur les défis de mise en œuvre et la coordination institutionnelle.
Sources Primaires (Quantitatif)	50 Utilisateurs de services numériques (citoyens et professionnels).	Questionnaires Exploratoires (codés).	Mesurer la perception des risques, la confiance numérique et l'attente de conformité réglementaire.

a. Sources Secondaires (Analyse Documentaire)

L'analyse documentaire a porté sur de différents rapports et textes législatifs, tels que:

- **Textes législatifs et réglementaires marocains :** Analyse exhaustive de la Loi n° 09-08 sur la protection des données personnelles, de la Loi n° 05-20 relative à la cyber sécurité, du Code pénal (Loi 07-03) et des décrets sectoriels pertinents.
- **Rapports institutionnels :** Consultation des publications de la CNDP, de la DGSSI, ainsi que des rapports émanant du Ministère de l'Industrie et de l'Économie numérique et de la Banque Centrale du Maroc.
- **Publications académiques et études sectorielles :** Revue de la littérature scientifique, d'ouvrages spécialisés sur la cyber sécurité, la conformité et la gouvernance numérique.
- **Rapports internationaux :** Utilisation des analyses de l'UNODC, de l'OCDE et de la Banque Mondiale pour contextualiser et réaliser une analyse comparative des enjeux.

b. Sources Primaires (Enquête de Terrain)

La sélection des participants a été réalisée selon une **méthode non probabiliste par choix raisonné** ; basée sur la pertinence des acteurs et leur connaissance approfondie du sujet. La population cible comprenait les institutions financières, les administrations publiques et les entreprises privées opérant dans des secteurs stratégiques.

3.4. Collecte et Traitement des Données

Pour la Collecte des données : Les entretiens ont été enregistrés et retranscrits intégralement. Les documents législatifs et rapports ont été analysés et codés thématiquement. Les questionnaires ont été codés pour identifier les perceptions et les tendances quantitatives.

Pour l'Analyse des données, nous avons utilisé ce qui suit :

- **Analyse Thématique :** Identification des principaux axes et sous-axes (enjeux, défis, bonnes pratiques, recommandations) selon un modèle d'analyse thématique rigoureux.
- **Triangulation des Sources :** Comparaison systématique des données documentaires, des entretiens et des questionnaires pour renforcer la validité et la fiabilité des conclusions.
- **Identification des Écarts :** Analyse des divergences entre le cadre réglementaire formel et les pratiques effectives de cyber sécurité sur le terrain.

3.5. Résultats Empiriques

Les données collectées ont permis de dégager plusieurs constats clés, à savoir :

- **Constats issus des entretiens semi-directifs :** Dix des douze experts ont souligné un manque de compétences spécialisées dans la cybersécurité au sein des organisations publiques et privées, freinant la mise en œuvre efficace des dispositifs réglementaires. De plus, la majorité des experts (9 sur 12) ont indiqué une coordination insuffisante entre les différentes institutions (CNDP, DGSSI, ministères), ce qui limite l'efficacité des mesures préventives.

- **Constats issus des questionnaires exploratoires :** Soixante-huit pour cent (68 %) des répondants considèrent que la sécurité des services en ligne est un enjeu majeur, tandis que 54 % déclarent ne pas avoir confiance dans l'intégrité des plateformes numériques de certaines administrations ou banques. Enfin, 75 % estiment que la protection des données personnelles devrait être renforcée par des mesures plus visibles et transparentes.

Ces résultats mettent en évidence une perception partagée de vulnérabilité et d'insuffisance dans la gouvernance de la cyber sécurité, justifiant la nécessité d'améliorer la coordination, les compétences et la culture organisationnelle.

3.6. Limite de l'Étude

- L'échantillon qualitatif reste restreint, ce qui limite la généralisation des résultats à l'ensemble du pays.
- La disponibilité et la transparence des répondants peuvent influencer la profondeur des informations recueillies.
- Les données secondaires peuvent présenter un décalage temporel par rapport aux menaces cyber actuelles, étant donné la rapidité des évolutions technologiques et criminelles.

3.7. Approche Éthique

L'étude a été menée dans le respect strict des principes éthiques de la recherche : garantie de la confidentialité et de l'anonymat des participants, obtention du consentement éclairé pour tous les entretiens et questionnaires, et utilisation des informations exclusivement à des fins académiques.

3.8.Perspectives et Recommandations pour une Cyber sécurité Renforcée

Pour surmonter les défis actuels et renforcer la résilience du Maroc face à la cybercriminalité, une approche intégrée et proactive est indispensable. Les perspectives d'amélioration et les recommandations stratégiques s'articulent autour de plusieurs axes majeurs.

3.8.1. Renforcement du Cadre Législatif et Réglementaire

- **Harmonisation et Simplification :** Il est crucial de poursuivre l'harmonisation et la simplification du cadre réglementaire pour le rendre plus accessible et compréhensible par toutes les entités, y compris les PME. Cela pourrait inclure la consolidation de certains textes ou la publication de guides pratiques.
- **Adaptation Continue :** Le cadre législatif doit être régulièrement mis à jour pour intégrer les nouvelles formes de cybercriminalité et les avancées technologiques. Cela implique une veille juridique et technologique constante.

- **Finalisation du Cadre International :** L'adhésion formelle et la pleine application des conventions internationales pertinentes, notamment la Convention de Budapest sur la cybercriminalité, sont cruciales. Cela faciliterait l'entraide judiciaire internationale et la lutte contre la cybercriminalité transnationale.

3.8.2. Développement des Compétences et Sensibilisation

- **Formation Spécialisée :** Investir massivement dans la formation de professionnels de la cyber sécurité et de la conformité, en développant des cursus universitaires et des certifications professionnelles adaptés aux besoins du marché.
- **Création d'un diplôme lié à la Cybercriminalité/Sécurité reconnu par l'Etat :** Un Master Spécialisé caractérisé par une formation robuste assurée par les spécialistes et d'une durée de 2 ans**.**
- **Sensibilisation Accrue :** Mettre en place des campagnes de sensibilisation nationales ciblées pour le grand public, les entreprises et les administrations, afin de développer une culture de cyber sécurité solide et de promouvoir les bonnes pratiques.

3.8.3. Amélioration de la Gouvernance et de la Coopération

- **Coordination Renforcée :** Établir des mécanismes de coordination plus efficaces entre les différentes autorités et institutions impliquées dans la cybersécurité (DGSSI, CNDP, autorités judiciaires, etc.) pour une réponse plus cohérente et rapide.
- **Partenariats Public-Privé :** Encourager les partenariats entre le secteur public et le secteur privé pour le partage d'informations sur les menaces, le développement de solutions innovantes et le renforcement des capacités.
- **Coopération Internationale :** Renforcer la coopération avec les organisations internationales et les pays partenaires pour échanger des expertises, coordonner les actions de lutte et mutualiser les ressources.

3.8.4. Innovation et Recherche

- **Soutien à la Recherche et Développement :** Encourager la recherche et le développement dans le domaine de la cybersécurité pour anticiper les menaces futures et développer des solutions innovantes adaptées au contexte marocain.

- **Veille Technologique :** Mettre en place des dispositifs de veille technologique pour suivre l'évolution des menaces et des solutions de sécurité, afin d'adapter en permanence les stratégies de défense.

4. Conclusion

Le but de cet article était d'analyser la relation entre la cybercriminalité et la conformité réglementaire au Maroc. Nous l'avons constaté et bien que le pays dispose d'un cadre juridique solide (notamment les lois n° 05-20 et n° 09-08), un décalage persiste entre la loi et son application effective. L'efficacité de la conformité est limitée par un manque de compétences spécialisées et une coordination institutionnelle insuffisante, ce qui fragilise la sécurité des systèmes et la confiance des citoyens et investisseurs. La conformité réglementaire est donc une condition nécessaire, mais pas suffisante, pour contrer efficacement les cybers menaces.

Pour atteindre une véritable cyber-résilience, le Maroc doit passer d'une simple conformité formelle à une culture de sécurité intégrée. Cela exige un investissement dans le capital humain, une gouvernance agile et une harmonisation avec les standards internationaux. En comblant l'écart entre le droit et la pratique, le Maroc pourra transformer la sécurité numérique en un avantage stratégique pour son économie.

REFERENCES

[1] Arner, D. W., Buckley, R. P., Zetzsche, D. A., & Veidt, R. (2020). Sustainability, FinTech and financial inclusion. European Business Organization Law Review, 21(1), 7–35.

[2] Baldwin, R., Cave, M., & Lodge, M. (2012). Understanding regulation: Theory, strategy, and practice (2nd ed.). Oxford University Press.

[3] Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements.

[4] Black, J. (2019). Regulation and compliance. In P. Cane & H. M. Kritzer (Eds.), The Oxford handbook of empirical legal research (pp. 1–23). Oxford University Press.

[5] Brenner, S. W. (2013). Cybercrime and the law: Challenges, issues, and outcomes. Northeastern University Press.

[6] Clough, J. (2020). Cybercrime: Investigating high-technology computer crime (3rd ed.). Cambridge University Press.

[7] Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP). (2022). Guide de conformité en matière de protection des données personnelles. Royaume du Maroc.

[8] Direction Générale de la Sécurité des Systèmes d'Information (DGSSI). (2021). Référentiel national de cybersécurité. Royaume du Maroc.

[9] ENISA. (2022). ENISA threat landscape. European Union Agency for Cybersecurity.

[10] Europol. (2022). Internet organised crime threat assessment (IOCTA). European Union Agency for Law Enforcement Cooperation.

[11] Florêncio, D., & Herley, C. (2018). A large-scale study of web password habits. World Wide Web Journal, 21(1), 1–20.

[12] GAFI. (2023). Cyber-enabled fraud and money laundering. Groupe d'Action Financière.

[13] ISO/IEC. (2023). ISO/IEC 27002: Information security controls. International Organization for Standardization.

[14] Kshetri, N. (2021). Cybersecurity management: An organizational and strategic approach. University of Toronto Press.

[15] Levi, M., & Reuter, P. (2006). Money laundering. Crime and Justice, 34(1), 289–375.

[16] NIST. (2023). Cybersecurity framework 2.0. National Institute of Standards and Technology.

[17] Power, M. (2009). The risk management of everything: Rethinking the politics of uncertainty. Demos.

[18] Royaume du Maroc. (2009). Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Bulletin Officiel.

[19] Royaume du Maroc. (2020). Loi n° 05-20 relative à la cybersécurité. Bulletin Officiel.

[20] UNODC. (2021). Cybercrime and anti-money laundering. United Nations Office on Drugs and Crime.

[21] Wall, D. S. (2017). Crime, security and information communication technologies. Routledge.

[22] Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society (3rd ed.). SAGE Publications.

[23] Chihab, S., & Ammi Al Masbahi, F. (2025). Vers une intelligence artificielle régulée : innovations et défis dans la lutte contre la criminalité financière. International Journal of Economic Studies and Management, 5(6), 721–739. https://doi.org/10.5281/zenodo.17578885