REVUE
DROIT & SOCIETE
مجلة
القانون و المجتمع
دورية علمية محكمة تعنى با لدراسات و الأبحاث في المجال القانوني و الاجتماعي و الاقتصادي.
PERIODIQUE SCIENTIFIQUE A COMITE DE LECTURE, CONSACRE A LA PUBLICATION D'ETUDES ET DE RECHERCHES DANS LES DOMAINES JURIDIQUE, ECONOMIQUE ET SOCIAL
N° 11- OCTOBRE/ DECEMBRE 2023

LA PREUVE NUMERIQUE A L'EPREUVE DE LA CYBERCRIMINALITE EN DROIT MAROCAIN

DIGITAL EVIDENCE AGAINST CYBERCRIME IN MOROCCAN LAW

DOI: 10.5281/zenodo.10054215

ABOU EL JAOUAD Anouar

Doctorant chercheur

Faculté des Sciences Juridiques Economiques et Sociales Mohammedia, Université Hassan II, Casablanca, Maroc

LA PREUVE NUMERIQUE A L'EPREUVE DE LA CYBERCRIMINALITE EN DROIT MAROCAIN

RESUME

Dans le cadre de cet essai, nous nous penchons sur la question de la pertinence et des limitations de l'utilisation de preuves numériques dans le contexte de la procédure pénale marocaine.

L'évolution rapide de la technologie a considérablement modifié la manière dont nous menons nos enquêtes criminelles, et l'importance des preuves numériques ne peut être sous-estimée. Cependant, le Maroc, comme de nombreux autres pays, est confronté au défi de s'adapter à ces nouvelles réalités tout en respectant les droits et les garanties juridiques des accusés.

Nous explorons donc dans quelle mesure la législation marocaine permet l'utilisation de preuves numériques, tout en cherchant à maintenir un équilibre entre la nécessité de lutter contre la cybercriminalité et le respect des droits fondamentaux.

Notre examen de la législation marocaine en matière de preuves numériques met en lumière les défis et les opportunités auxquels notre système judiciaire est confronté. Nous analysons les dispositions juridiques existantes et leur adéquation à l'ère numérique, tout en évaluant les implications pour la protection de la vie privée, la chaîne de garde et l'authenticité des preuves numériques. De plus, nous identifions les lacunes potentielles dans la réglementation et

ABOU EL JAOUAD Anouar

Doctorant chercheur

Université Hassan II, Casablanca, Mohammedia, Maroc

REVUE DROIT & SOCIETE
N° 11- OCTOBRE/ DECEMBRE 2023

formulons des recommandations pour renforcer l'utilisation de preuves numériques dans le cadre de la procédure pénale marocaine, tout en préservant les droits individuels et la justice équitable.

Mots clés: Cybercriminalité, Preuve numérique, Procédure pénale, Conventions internationales, Droit marocain.

.

DIGITAL EVIDENCE AGAINST CYBERCRIME IN MOROCCAN LAW

ABSTRACT

In this essay, we address the question of the relevance and limitations of using digital evidence in the context of Moroccan criminal procedure.

The rapid evolution of technology has significantly altered the way we conduct criminal investigations, and the importance of digital evidence cannot be underestimated. However, Morocco, like many other countries, faces the challenge of adapting to these new realities while respecting the rights and legal guarantees of the accused.

We therefore explore the extent to which Moroccan legislation allows the use of digital evidence, while seeking to maintain a balance between the need to combat cybercrime and respect for fundamental rights.

Our review of Moroccan legislation on digital evidence highlights the challenges and opportunities facing our judicial system. We analyze existing legal provisions and their suitability for the digital age, while assessing the implications for privacy protection, chain of custody and the authenticity of digital evidence. In addition, we identify potential gaps in regulation and make recommendations for strengthening the use of digital evidence in Moroccan criminal procedure, while preserving individual rights and fair justice.

Keywords: Cybercrime, Digital evidence, Criminal procedure, International conventions, Moroccan law.

ABOU EL JAOUAD Anouar

PhD Student

Hassan II University, Casablanca, Mohammedia, Morocco

REVUE DROIT & SOCIETE
N° 11- OCTOBRE/ DECEMBRE 2023

INTRODUCTION

La notion de preuve implique la démonstration de la réalité d'un fait ou d'un droit et est couramment définie dans la doctrine comme étant « ce qui persuade l'esprit d'une vérité ».[1] Elle occupe une place essentielle dans l'ensemble des domaines du droit, y compris le droit pénal, où son rôle est de déterminer la commission d'une infraction et d'identifier son auteur.

Cependant, l'évolution de la technologie a radicalement transformé le paysage de la preuve, notamment en introduisant des éléments de preuve sous forme de documents informatiques ou stockés dans la

[1] J.Domat, « Les lois civiles dans leur ordre naturel », Paris, éd. Cavalier, t.1, 1771, p.204.

mémoire d'appareils électroniques. Cette révolution a donné naissance à une nouvelle branche du droit pénal, à savoir le domaine de la preuve numérique[2] .

Aujourd'hui, les enquêtes judiciaires sont de plus en plus confrontées à des preuves numériques, créant ainsi de nouveaux défis pour les professionnels du droit et les spécialistes de l'enquête. Cette évolution nous amène à examiner de plus près la manière dont la preuve numérique s'intègre dans le cadre de la procédure pénale et la manière dont elle affecte les pratiques et les lois existantes. Dans cet article, nous explorerons les complexités de la preuve numérique, son impact sur le droit pénal, et les implications pour les acteurs du système judiciaire à l'ère numérique.

Le cyberspace est un espace dangereux et nébuleux dans lequel des comportements réprimés en société, qui ont largement envahit le monde virtuel. [3] A cet effet, les preuves numériques deviennent un élément crucial des requêtes liées à la cybercriminalité.

L'article 2 de la loi 05-20 relative à la cybersécurité à définit la « Cybercriminalité » comme : l'ensemble des actes contrevenant à la législation nationale ou aux traités internationaux ratifiés par le Royaume du Maroc, ayant pour cible les réseaux ou les systèmes d'information ou les utilisant comme moyens de la commission d'un délit ou d'un crime. [4]

Etant donné que le numérique engendre de fragilités et s'accompagne de graves menaces, la collecte des preuves numériques en matière de cybercriminalité constitue, un enjeu majeur, pour l'éclatement de la vérité dans ce genre d'affaires.

A travers cette étude, notre ambition sera de dévoiler la question de la preuve numérique en matière de cybercriminalité. Une première partie qui expose le cadre juridique et intérêt de la preuve numérique en matière de cybercriminalité, et une deuxième partie qui met en exergue le défi de la constitution de la preuve numérique en matière cybercriminelle.

I. La preuve pénale numérique : Cadre juridique et intérêt de la preuve numérique en matière de cybercriminalité

a) Cadre juridique de la preuve numérique en matière de cybercriminalité

Les dispositions qui traitent de la preuve numérique trouvent leur fondement dans deux l'ordre juridique interne et l'ordre international.

Dans l'ordre juridique marocain notamment en droit pénal, la preuve est régie par l'article 286

et suivants du Code de procédure pénale. L'article 286 cité ci-dessus, prévoit que « Les infractions peuvent être établies par tout mode de preuves,

[2] Eric Freyssinet, La preuve numérique, un défi pour l'enquête criminelle du 21éme siècle, Lavoisier, Les Cahiers du numérique, 2003/3 Vol. 4, p 206. Article disponible en ligne à l'adresse : https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-205.htm

[3] Manal Badil, Dispositif juridique et institutionnel en matière de lutte contre la cybercriminalité au Maroc, Edition Approches, 2022, p 14.

[4] Dahir n° 1-20-69 du 4 hija 1441 (25 juillet 2020) portant promulgation de la loi n° 05-20 relative à la cybersécurité

hors le cas où la loi en dispose autrement, et le juge décide d'après son intime conviction. La décision doit comporter ce qui justifie la conviction du juge, conformément au huitième alinéa de l'article 365 ci-après.

Si la juridiction estime que la preuve n'est pas rapportée, elle déclare la non culpabilité du prévenu et prononce son acquittement ».

L'article 287 du code de procédure marocaine précise que « La juridiction ne peut fonder sa décision que sur des preuves versées aux débats et discutées oralement et contradictoirement devant elle ».

Par rapport à l'ordre international, il est nécessaire de souligner que le Maroc a ratifié les dispositions de la Convention de Budapest sur la cybercriminalité et le Protocole additionnel à ladite Convention, fait à Strasbourg le 28 janvier 2003, qui est un texte de référence en matière de lutte contre la cybercriminalité à l'échelle internationale. [5]

Ladite convention traite la politique de collecte des éléments de preuve pour la lutte contre la cybercriminalité transfrontalière. Les axes touchant la conservation des données stockées, la conservation et la divulgation rapide des données relatives au trafic ont été évoqués par les dispositions des articles 16 à 18. L'alinéa 1 de l'article 16 de la convention en question dispose que « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification ».

L'article 19 de cette convention a évoqué les points relatifs à la perquisition des systèmes et la saisie de donnée informatique. L'alinéa 1 de l'article en question dispose que « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire:

- A un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées; et
- A un support du stockage informatique permettant de stocker des données informatiques sur son territoire ».

Les articles 20 à 21 de la convention ont mis en lumière la collecte en temps réel des données relatives au trafic et l'interception de données relatives au contenu.

Les dispositions des articles 23 à 34 de cette convention invitent les Etats à agir, par le biais de leurs autorités judiciaires et services de police, dans un but coopératif, afin de permettre à établir la preuve électronique, sans toutefois mener d'enquêtes et de perquisitions transfrontalières. Les informations obtenues doivent être rapidement communiquées. L'article 35 de cette Convention instaure un réseau de contacts H24/7 afin de prêter une assistance immédiate et permanente aux investigations en cours. L'article en question dispose que « Chaque Partie désigne un point

[5] Bulletin officiel du 11 ramadan 1441 (5-5-2020), p 79.

de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes:

- Apport de conseils techniques;
- Conservation des données, conformément aux articles 29 et 30; recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects…etc.

b) Intérêt de la preuve numérique en matière pénale en matière de cybercriminalité

En l'espace de quelques années, l'essor qu'a connu le réseau Internet est frappant. Cet outil sans pareil s'immisce progressivement dans le quotidien de tout un chacun et offre d'innombrables perspectives, dans les domaines les plus divers. [6]

Néanmoins, étant donné que les problèmes de criminalité et d'insécurité s'adaptent à l'évolution de la société, chaque technologie peut avoir des usages détournés ou abusifs et être porteuse de potentialités criminelles. [7]
A l'instar des autres progrès humains, le progrès numérique est générateur de comportements illicites qui portent atteinte à tout le monde. [8]
Il est judicieux de s'interroger sur l'intérêt de la preuve numérique en matière de cybercriminalité.

Avec le développement des moyens d'investigations numérique, l'exigence de vérité semble plus pressante. La preuve numérique est une modalité particulière d'établissement de la vérité qui consiste à avoir recours à des moyens numériques divers et variés qui vont de l'étude des contenus dans les données d'un disque dur, aux messages électroniques, en passant par l'enregistrement numérique. [9]

Les citoyens utilisent de plus en plus les nouvelles technologies d'information, laissant ainsi d'innombrables traces numériques, chaque jour, derrière eux. Dans le domaine de cybercriminalité, ces traces constituent une mine d'informations pour les autorités judiciaires.

L'intérêt pratique de la preuve numérique réside dans la possibilité de traiter rapidement un grand nombre d'informations. Ce traitement automatisé repose sur des procédés algorithmiques. Un algorithme est la description d'opérations à exécuter successivement, pour résoudre un problème donné. [10]

La grande criminalité et le terrorisme confèrent à la preuve numérique une

[6] LE FLOCH (G.), *« Annuaire français de droit international »*, CNRS éd. Paris, Volume 51, n°1, [2005], pp. 464-486.

[7] *Solange Ghernaouti, « Cybersecurité, sécurité informatique et réseaux », 5éme édition, Dunod, 2016, p 41.*

[8] *Manal Badil, Dispositif juridique et institutionnel en matière de lutte contre la cybercriminalité au Maroc, op.cit, p 3.*

[9] *CNEJITA, « Police judiciaire et nouveaux territoires de l'information numérique », Campagne nationale des experts de justice en informatique et techniques associées, Colloque du 13 avril 2010 à la 1ère chambre de la Cours d'appel de Paris. Disponible sur http://cnejita.org/doc/Colloque_20100513_Actes.pdf, p.11*

[10] *G.Chantepie, "Le droit en algorithmiques ou la fin de la norme délibérée", Dalloz IP/ IT 2017, p 522.*

place centrale par rapport à ce genre d'affaires. A cet égard, les différents groupes terroristes se sont dirigés vers le numérique, et ont mis en place une véritable stratégie de communication. [11] Dans ce cadre, la preuve numérique peut contribuer à détecter les auteurs des infractions en question.

L'enjeu majeur de la preuve numérique face à la sophistication des modes opératoires des cybercriminels, est de pouvoir matérialiser la preuve, qui va les incriminer.

La preuve numérique est déterminante pour l'aboutissement d'une l'affaire de cybercriminalité, surtout quand il s'agit d'une affaire de piratage informatique. A cet effet, la preuve numérique constitue bel et bien un véritable outil de commandement des dossiers de cybercriminalité.

Tableau 1 : L'Importance de la Preuve Numérique en Lutte Contre la Cybercriminalité

Aspects de la Preuve Numérique en Matière de Cybercriminalité	Points Clés
Contexte Général	- L'essor rapide d'Internet dans la vie quotidienne. - Les défis de la cybercriminalité dans un monde numérique.
Utilité de la Preuve Numérique	- Les technologies numériques comme sources potentielles de criminalité. - L'intérêt de la preuve numérique pour résoudre des affaires de cybercriminalité.
Collecte de Preuves Numériques	- L'abondance de traces numériques laissées par les citoyens. - Les traces numériques comme ressources précieuses pour les enquêtes judiciaires.
Traitement Automatisé des Informations	- Le rôle des algorithmes dans le traitement de grandes quantités de données numériques. - Rapidité et efficacité dans la gestion de preuves numériques.
Cybercriminalité et Terrorisme	- L'utilisation par les groupes terroristes des moyens numériques. - La prévention et la détection d'infractions grâce à la preuve numérique.
Matérialisation de la Preuve	- L'enjeu de la preuve numérique face à la sophistication des modes opératoires des cybercriminels. - Comment la preuve numérique peut incriminer les coupables.
Rôle de la Preuve Numérique	- Son rôle central dans les affaires de cybercriminalité, en particulier le piratage informatique. - La preuve numérique comme outil essentiel dans la gestion des dossiers de cybercriminalité.

Source : l'auteur

[11] Myriam Quemener, « Terrorisme et numérique », Le droit face à la disruption numérique, adaptation des droits classiques, émergence de nouveaux droits », Gualino Eds, 2018, p 118.

REVUE DROIT & SOCIETE N° 11- OCTOBRE/ DECEMBRE 2023

II- Le défi de la constitution de la preuve numérique en matière cybercriminelle

A- La constitution de la preuve numérique

Dans le cadre de la constitution de la preuve numérique, il est nécessaire de s'interroger sur le procédé de collecte de la preuve numérique en la matière.

Le procédé en question consiste d'abord à collecter les informations numériques mais aussi de procéder à leur stockage et préservation.

A l'instar des autres domaines du droit pénal, la collecte des informations numériques dans le cadre d'une affaire de cybercriminalité suppose qu'on se trouve dans un contexte de flagrance, d'enquête préliminaire, et ce, en concordance avec les dispositions du code de procédure pénale marocaine.

Les experts en matière de cybercriminalité sont tenus de faire preuve de maitrise dans le domaine de cybercriminalité.

Le Maroc a mis en place une stratégie nationale de cybersécurité, afin de collecter la preuve numérique. A cet égard, le Maroc a créé des organismes chargés de recueillir la preuve numérique en matière de cybersécurité.

Parmi ces organismes, figure la Direction Générale de la Sûreté Nationale (DGSN), qui a veillé à la mise en place d'unités spécialisées en matière de recherches et enquêtes sur la cybercriminalité, aussi bien au niveau central que sur le plan régional.

Parmi ces organismes, figure le Laboratoire d'analyse des traces numériques relevant de la Brigade Nationale de la Police Judiciaire.

Le Laboratoire d'analyse des traces numériques cité ci-dessus, procède à la recherche et à l'extraction de la preuve numérique incriminant les faits et informe les Officiers de Police Judiciaire, pour entamer la procédure, après accord du Parquet compétent.

L'organisme en question travaille sur des supports numériques physiques, ordinateurs, DVR, CD, terminaux mobiles, support amovibles, smartphones, ect., saisies à l'occasion des perquisitions judiciaires ou sur les scènes de crime, afin d'en extraire les données et rechercher les éléments de preuves en relation avec l'affaire. [12]

Ledit organisme travaille avec des procédures standardisées. Toutes les preuves sont recueillies selon les normes de préservation de leur intégrité et traçabilité, en utilisant les conditionnements spécifiques à chaque type de preuve. S'il s'agit par exemple, d'un GSM, il est transporté dans une cage de Faraday, afin de l'isoler et d'éviter tout risque de modification de son contenu, ect. [13]

Cet organisme réalise également une copie intégrale bit à bit des supports numériques, objets des expertises, avec des logiciels forensiques dédiés, en plus d'un blocage en écriture. Les expertises sur la copie sont réalisées, afin de rechercher d'éventuelles preuves, tout en veillant à garder le matériel initial intact, gage de traçabilité et d'intégrité. [14]

[12] Marouane Hejjouji, Revue de la Police, n 42, décembre 2021, p 61.
[13] Ibid
[14] Ibid

Quand il s'agit des pièces à conviction sur Internet, des captures d'écran sont réalisés par l'organisme en question. Dans ce cas d'espèce, un procès-verbal de constatation est établi, en précisant la date, l'URL, ect. Concernant les vidéos ou les messages audio, ils sont transcrits dans leur intégralité dans le procès-verbal technique qui sera joint à la procédure. [15]

Par rapport à la perquisition du matériel informatique, le prélèvement passe d'abord dans la salle de préservation des pièces à conviction, dont dispose la Brigade Nationale de la Police Judiciaire, avant de commencer l'expertise proprement dite. C'est un nouveau mécanisme mis en place au Maroc, pour assurer la traçabilité de la preuve. Le chargé de cette salle, est tenu de vérifier leur conditionnement et leur intégrité, et leur intégrité, et les entreposer selon leurs natures dans l'endroit approprié. Elles sont ensuite prises en charge par le service qui va effectuer l'expertise, qui est tenu par la suite de les restituer à la salle de préservation après la fin de l'expertise. [16]

Parmi les organismes chargés de recueillir la preuve numérique en matière de cybercriminalité, figure le Service du Renseignement Criminel et d'Appui aux Enquêtes, relevant de l'Office National contre la Criminalité liés aux nouvelles technologies, attaché à la Brigade Nationale de la Police Judiciaire.
Ledit service est une entité spécifique qui intervient dans l'élucidation des affaires criminelles les plus complexes. Ledit service peut intervenir dans les affaires de cybercriminalité.
Cette entité experte dispose d'outils techniques lui permettant d'analyser un grand flux d'information, de les trier, de ressortir les plus pertinentes et de faire des recoupements, afin d'associer une personne à un endroit, un numéro de téléphone à une activité, relier entre des personnes elles, ect. [17]
Pour mener à bien la collecte des preuves numériques en matière de cybercriminalité, l'entité en question en question fait appel aux bases de données mise à sa disposition. Il peut formuler des réquisitions, sous la supervision du Parquet compétent, aux fournisseurs d'accès à Internet, aux opérateurs de téléphonie et même à d'autres partenaires privés. [18]
Les enquêteurs dudit service peuvent tomber sur une adresse IP à l'étranger. A cet égard, ledit service fait intervenir les canaux de coopération, via une commission rogatoire internationale, Interpol, le Bureau de Liaison Arabe, le point de contact de la Convention de Budapest ou les Officiers de Liaison accréditées au Maroc. [19]

[15] Ibid
[16] Ibid
[17] Noureddine Najih, Revue de la Police, n 42, décembre 2021, p 64.
[18] Ibid
[19] Ibid

Tableau 2 : Processus de Collecte de Preuve Numérique en Matière de Cybercriminalité au Maroc

Étape	Description
Procédé de Collecte de Preuve Numérique	- Collecte, stockage et préservation des informations numériques. - Contextes de flagrance et d'enquête préliminaire en accord avec le Code de procédure pénale marocain.
Maîtrise des Experts en Cybercriminalité	- Nécessité d'une expertise spécialisée en cybercriminalité. - Stratégie nationale de cybersécurité au Maroc.
Organismes de Collecte de Preuve Numérique	- La Direction Générale de la Sûreté Nationale (DGSN) avec des unités spécialisées. - Le Laboratoire d'analyse des traces numériques de la Brigade Nationale de la Police Judiciaire.
Traitement des Preuves Numériques	- Copie intégrale bit à bit des supports numériques. - Standardisation des procédures pour préserver l'intégrité des preuves.
Preuves sur Internet	- Captures d'écran avec procès-verbal de constatation. - Transcription des vidéos et messages audio dans les procès-verbaux techniques.
Salle de Préservation des Pièces à Conviction	- Vérification de l'intégrité et du conditionnement des preuves. - Mécanisme de traçabilité pour assurer la préservation.
Service du Renseignement Criminel et d'Appui aux Enquêtes	- Entité spécifique pour les affaires criminelles complexes. - Capacité d'analyser et recouper de grandes quantités d'informations.
Réquisitions et Coopération Internationale	- Réquisitions aux fournisseurs d'accès à Internet et opérateurs de téléphonie. - Utilisation de la coopération internationale et des commissions rogatoires.

Source : l'auteur

B- Les limites à la constitution de la preuve numérique en cybercriminalité

Les limitations liées à la constitution de la preuve numérique sont de plusieurs ordres. Parmi ces obstacles, figure la distance qui peut séparer l'État de poursuites et celui de l'arrestation. Les progrès accomplis dans le domaine de la technologie et des télécommunications sont allés de pair avec une recrudescence de la délinquance. Pour rechercher la preuve, « l'enquête judiciaire est de plus en plus une enquête de confrontation des données et une enquête de traçabilité qui requiert d'aller chercher les preuves à l'étranger ». [20]

Au niveau international, en vertu de la théorie de la souveraineté des États, toute une multitude de règles pénales propres à chaque pays cohabitent. Un problème se pose alors lorsqu'une infraction peut intéresser plusieurs États à la fois. En ce sens, la difficulté d'application du droit marocain territorialisé et souverainiste face à une délinquance virtuelle, mondiale et sans frontière, pose problème.

[20] AGHROUM (C.), *« Police judiciaire et nouveaux territoires de l'information numérique »*, Campagne nationale des experts de justice en informatique et techniques associées, Colloque du 13 avril 2010 à la 1ère chambre de la Cours d'appel de Paris. Disponible sur http://cnejita.org/doc/Colloque_20100513_Actes.pdf, p 42.

Une autre difficulté se décline à savoir la traçabilité du fait de ces outils d'anonymisation, mais aussi des outils de cryptage qui permettent de chiffrer les données. « Ces chiffrements utilisés par la criminalité organisée ou le terrorisme sur Internet sont parfois très difficiles à casser ». [21]

Parmi les obstacles de la preuve numérique en matière de cybercriminalité, figure le problème de l'inadaptation du droit procédural à l'environnement numérique. Certes, la loi marocaine autorise un large éventail de méthodes d'investigation et autorise des instruments d'enquête tels que la perquisition.
Néanmoins, la perquisition suscite des observations en ce qui concerne des données se trouvant sur des données numériques. D'autant plus que les données informatiques ne sont pas tangibles et la perquisition au sens de l'article 59 du code de procédure pénale marocaine ne vise que des choses tangibles. [22]

En effet, loi marocaine n'autorise pas la saisie des données informatiques immatérielles, intangibles sans saisir le matériel informatique. Ce qui cause un préjudice tant pour les chargés de la perquisition, que pour les personnes sujets de cette perquisition. [23]

L'environnement technologique évolue rapidement, soulevant des défis pour garantir la force de la preuve.

Une preuve numérique est une modalité particulière d'établissement de la vérité qui consiste à avoir recours à des moyens numériques variés qui vont de l'étude des contenus dans la mémoire d'un disque dur, aux messages électroniques, en passant par l'enregistrement numérique. Elle peut-être facilement altérée, déplacée ou effacée, et doit par conséquent être préservée rapidement. [24]

Sur le plan pratique, l'environnement numérique souffre de la difficulté d'administrer la preuve du délit, surtout qu'elle est caractérisée par le fait qu'elle ne se trouve pas à l'endroit où l'on découvre l'infraction. En effet, la preuve peut se trouver dans un appareil numérique perquisitionné chez des fournisseurs ou bien des prestataires techniques détenant les données de trafic... [25]

Parmi les autres limites de la preuve numérique figure le problème de traçabilité qui devient de plus en plus difficile, du fait des outils de cryptologie permettant de chiffrer les données. Les chiffrements utilisés par les fraudeurs sont parfois très difficiles à casser et extrêmement complexes. A cet effet, le responsable du système informatique doit s'assurer de conserver les données non pas en local où ils risquent d'êtres altérés par des cyber-délinquants, mais sur un système tiers en redirigeant la sauvegarde vers une machine distante via le réseau, bien que si les cyber-délinquants sont experts, ils peuvent en détourner ceci. [26]

L'environnement technologique évolue rapidement, soulevant des défis pour garantir la force de la preuve.

Les spécificités du monde numérique rendent difficiles la preuve de l'infraction et l'identification de son auteur. La difficulté réside dans la localisation de l'auteur de l'infraction.
Par ailleurs, la localisation d'un fraudeur est limitée par des imprécisions résultant

[21] Ibid.
[22] Amina Dik, Régles pénales relatives aux délits informatiques, La Revue du Droit Marocain, p 43.
[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] Ibid

REVUE DROIT & SOCIETE
N° 11- OCTOBRE/ DECEMBRE 2023

 ISSN: 2737-8101

principalement des adresses IP non fixes et attribuées par les fournisseurs d'accès d'internet, ou de certains pays qu'ils utilisent. En plus, il est très difficile d'établir un lien entre la localisation de la machine responsable de l'infraction, et de l'identité de la personne à laquelle le fait incriminé est imputable. [27]
A cet effet, plusieurs types d'attaques commises par les cyber-délinquants laisse à méditer sur ce point. On peut citer l'usurpation d'adresse IP ou IP spoofing. C'est une technique qui consiste à utiliser l'adresse IP d'une autre machine pour en usurper l'identité. Le fraudeur peut accéder à un réseau sécurisé sous couvert de l'identité d'un autre… [28]

CONCLUSION :

En conclusion, l'importance de la preuve numérique en matière de cybercriminalité au Maroc est indéniable. L'évolution rapide des technologies numériques a créé de nouveaux défis pour les autorités judiciaires, les enquêteurs et les experts en cybercriminalité. Cependant, le pays a mis en place une stratégie nationale de cybersécurité, avec des organismes spécialisés tels que la Direction Générale de la Sûreté Nationale et le Laboratoire d'analyse des traces numériques, pour collecter, traiter et préserver les preuves numériques de manière efficace et conforme à la loi.

Le processus de collecte de preuve numérique comprend des étapes soigneusement réglementées, de la collecte initiale à la préservation des preuves. Les experts en cybercriminalité doivent faire preuve de maîtrise dans ce domaine en constante évolution, et les normes de préservation de l'intégrité et de traçabilité sont strictement respectées. De plus, le recours à la coopération internationale et aux réquisitions aux fournisseurs de services est courant pour enquêter sur des affaires de cybercriminalité qui peuvent avoir des ramifications internationales.

L'ensemble de ces éléments montre que le Maroc prend au sérieux la lutte contre la cybercriminalité et reconnaît l'importance de la preuve numérique dans le processus judiciaire. Cela renforce la capacité du pays à détecter, enquêter et poursuivre les auteurs d'infractions numériques, en particulier dans le contexte de la criminalité organisée et du terrorisme. La collecte de preuves numériques au Maroc s'inscrit dans un cadre réglementé visant à garantir l'équité, la transparence et la légalité des enquêtes.

En fin de compte, le processus de collecte de preuves numériques au Maroc est une composante essentielle de la lutte contre la cybercriminalité, et il illustre l'engagement du pays à faire face aux défis de la criminalité dans un monde de plus en plus numérique.

[27] Ibid
[28] Ibid

BIBLIOGRAPHIE

OUVRAGES

G.Chantepie, "Le droit en algorithmiques ou la fin de la norme délibérée", Dalloz IP/ IT 2017

J.Domat, « Les lois civiles dans leur ordre naturel », Paris, éd. Cavalier, t.1, 1771

LE FLOCH (G.), « Annuaire français de droit international », CNRS éd. Paris, Volume 51, n°1, [2005],

Manal Badil, Dispositif juridique et institutionnel en matière de lutte contre la cybercriminalité au Maroc, Edition Approches, 2022

Myriam Quemener, « Terrorisme et numérique », Le droit face à la disruption numérique, adaptation des droits classiques, émergence de nouveaux droits », Gualino Eds, 2018

Solange Ghernaouti, « Cybersecurité, sécurité informatique et réseaux », 5éme édition, Dunod, 2016

ARTICLES SCIENTIFIQUES

Amina Dik, Régles pénales relatives aux délits informatiques, La Revue du Droit Marocain

E. Freyssinet, La preuve numérique, un défi pour l'enquête criminelle du 21éme siècle, Lavoisier, Les Cahiers du numérique, 2003/3 Vol. 4, p 206. Article disponible en ligne à l'adresse : https://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-205.htm

REVUES

Revue de la Police, n 42, décembre 2021.

COLLOQUES

CNEJITA, « Police judiciaire et nouveaux territoires de l'information numérique », Campagne nationale des experts de justice en informatique et techniques associées, Colloque du 13 avril 2010 à la 1ère chambre de la Cours d'appel de Paris. Disponible sur http://cnejita.org/doc/Colloque_20100513_Actes.pdf.