المجلة المغربية للدراسات القانونية والاقتصادية
العدد 14، مارس 2025
ISSN(P) :1142-2489
ISSN(E) : 3085-4555
Numéro 14, MARS 2025
Revue Marocaine des Eudes Juridiques et Economiques

Les conditions de recevabilité de la preuve numérique

The admissibility conditions of digital evidence

JELDA Houda

Doctorante chercheuse
Laboratoire des Eudes Juridiques et Politiques à FSJP Settat

Pr. ECHCHARYF Hamid

Enseignant chercheur, à la Faculté des Sciences Juridiques et Politiques
Laboratoire des Eudes Juridiques et Politiques
Université Hassan I Settat

RÉSUMÉ:

À l'ère du numérique, la présence croissante d'éléments électroniques dans les litiges nécessite une réflexion approfondie sur les conditions permettant d'accepter de telles preuves devant les tribunaux. Dans un premier temps, l'article explore les fondements juridiques qui régissent la recevabilité de la preuve numérique. Il s'agit d'analyser les principes généraux du droit de la preuve, tels que l'authenticité, l'intégrité, la pertinence et la fiabilité. Ensuite, nous examinerons les critères techniques et légaux à satisfaire pour que la preuve numérique soit considérée comme recevable devant un tribunal. Ces critères incluent la certification de l'outil utilisé pour collecter la preuve, la conservation de l'intégrité des données, la traçabilité de la chaîne de possession, ainsi que la garantie que la preuve n'a pas été altérée ou falsifiée. Enfin, la recherche de solutions adaptées à ces défis permettra d'assurer une administration de la justice équitable et efficace dans un monde de plus en plus connecté.

Mots clés: Cybercriminalité**,** Preuve numérique, Recevabilité, Procès pénal, Investigation numérique, Droit marocain.

ABSTRACT:

In the digital age, the increasing presence of electronic elements in disputes requires a thorough reflection on the conditions for accepting such evidence in courts. Firstly, the article explores the juridical foundations that govern the admissibility of digital evidence. This involves analyzing the general principles of the law of evidence, such as authenticity, integrity, relevance, and reliability. Next, we will examine the technical and legal criteria to be met for digital evidence to be considered admissible in court. These criteria include the certification of the tool used to collect the evidence, the preservation of data integrity, the traceability of the chain of custody, as well as ensuring that the evidence has not been altered or falsified Ultimately, seeking tailored solutions to these challenges will ensure a fair and efficient administration of justice in an increasingly interconnected world.

Keywords: Cybercrime, Digital evidence, Admissibility, Criminal proccedings, Forensic investigation, Morrocan law.

Introduction:

« Depuis la constatation d'une infraction jusqu'au jugement de son auteur, toute la chaîne pénale est articulée autour de la question cardinale de la preuve[1]*. »*

Internet est un espace virtuel illimité sur le plan géographique et dépourvu de contrôle central, offrant ainsi une nouvelle plateforme permettant aux individus de s'exprimer librement. Toutefois, cet espace n'est pas soumis aux mêmes protections juridiques que le monde réel, en raison de l'anonymat, de la volatilité des preuves, de l'absence de frontières clairement définies. Cette combinaison de facteurs en crée également un terrain propice aux activités criminelles, avec tous les ingrédients nécessaires pour réaliser le crime parfait.

La procédure pénale tend à la recherche de la vérité et la preuve est le moyen de parvenir à l'établissement de la vérité[2]. Dans le même ordre des idées, la preuve a pu être définie comme *« ce qui sert à établir qu'une chose est vraie*[3] *»,* prouver comme *« convaincre quelqu'un de la vérité d'un fait*[4] *».*

Selon le doyen Domat la preuve est *« ce qui persuade l'esprit d'une vérité*[5] *»* car comme le souligne Monsieur le Professeur Pradel*, « c'est d'une certaine recherche de la vérité qu'il faut parler pour décrire correctement la façon de rechercher les objectifs de la justice*[6] *».*

Ainsi, il nous paraît plus juste de définir la preuve pénale comme un moyen de transformer une suspicion, une présomption, ou une croyance, en certitude, ou comme *« tout moyen juridique d'acquérir la certitude d'un fait ou d'une proposition*[7] *».*

En tentant de s'adapter aux évolutions perpétuelles de la société, la preuve est en constante mutation. Car la société connaissait une période de transition avec le progrès technologique, les manières de vivre et les habitudes sociales, et ces mutations avaient pénétré le droit pénal, tout comme la recherche, le recueil, mais surtout l'appréciation des preuves en justices.

---

[1] S. Guinchard et J. Buisson, « Procédure Pénale », 8ème Édition, LexisNexis, 2012, p:287

[2] La vérité est l'objectif essentiel de la procédure pénale, v. H. BEKAERT, La manifestation de la vérité dans le procès pénal, Bruxelles, Bruylant, 1972, p. 10

[3] J. DE CODT, « Preuve pénale et nullités », Revue de droit pénal et de criminologie, 2009, p. 636

[4] N. VERHEYDEN-JEANMART, Droit de la preuve, Bruxelles, Larcier, 1991, p. 7

[5] J. DOMAT, Les lois civiles dans un ordre naturel, 1771, p. 204, référence issue de J. PRADEL, Procédure pénale, 16ème éd., Paris, Cujas, 2011, p. 339

[6] Ibid., p. 304

[7] F. HÉLIE, « Traité de l'instruction criminelle », Tome IV, Paris, Henri Plon, 1866, p. 329. Aussi, la preuve est

« Un mécanisme destiné à établir une conviction sur un point incertain », H. LÉVY-BRUHL, La preuve judiciaire – Étude de sociologie juridique, Paris, Marcel Rivière, 1964, p. 15

La preuve numérique au **Maroc** est une notion relativement récente, qui s'est développée avec l'avènement des technologies de l'information et de la communication. Les premières utilisations de la preuve numérique remontent aux années 2000, avec l'essor des échanges électroniques et la multiplication des transactions en ligne. En 2005, le Maroc a adopté la loi n° 53-05 relative à l'échange électronique de données juridiques, qui a permis de reconnaître la validité juridique des documents électroniques et de garantir leur admissibilité en justice. En 2008, le Maroc a également ratifié la Convention de Budapest sur la cybercriminalité, qui vise à lutter contre les infractions commises par le biais de réseaux informatiques. Cette convention reconnaît aussi la validité juridique des preuves numériques et établit des règles pour leur recevabilité en justice. Depuis lors, le Maroc a continué de renforcer son cadre juridique pour la preuve numérique, en adoptant notamment la loi n° 09-08[1], qui vise à garantir la confidentialité et la protection des données personnelles. Plus récemment, en 2020, le Maroc a adopté la loi n° 43-20[2], qui tend à faciliter l'utilisation de la signature électronique et à renforcer la sécurité et la fiabilité des échanges électroniques.

Il est aisé de comprendre que l'importance du sujet revêt une valeur à haute niveau, car ladite analyse détermine comment peut-on garantir l'équité et l'intégrité du système judiciaire dans un monde de plus en plus numérique, et contribuer à renforcer la confiance des justiciables. L'avènement des technologies de l'information et de la communication a considérablement modifié la façon dont les preuves sont présentées devant les tribunaux. Les preuves numériques sont devenues omniprésentes dans les procès et les enquêtes criminelles, ce qui rend leur admissibilité et leur fiabilité cruciales pour assurer une justice équitable. Ainsi qu'elles sont souvent très complexes et leur analyse peut nécessiter l'intervention d'experts techniques. Il est donc important de disposer de critères clairs et objectifs pour déterminer si une preuve numérique est recevable ou non. Vu qu'elles peuvent être facilement altérées ou falsifiées. Il est donc judicieux de s'assurer que les preuves présentées devant les tribunaux sont fiables et qu'elles ont été recueillies de manière légale.

À cet égard, il nous parait pertinent de signaler que notre étude s'attachera principalement à répondre une problématique fondamentale:

Dans quelle mesure le système législatif marocain actuel a-t-il pu assurer la fiabilité de la preuve numérique dans le procès judiciaire en dépit des défis liés à son admission ?

La nature de notre recherche et les problématiques qui en découlent, nous impose d'adopter une démarche analytique fondée sur l'examen des textes législatifs pertinents relatifs au sujet étudié. Ainsi, il convient dans un premier temps d'aborder les assisses juridiques de la preuve numérique (**Partie 1**), avant d'envisager, dans un second, les enjeux liés à sa recevabilité (**Partie 2**).

[1] Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.
[2] Dahir n° 1-20-100 du 16 joumada I 1442 (31 décembre 2020) portant promulgation de la loi n° 43-20 relative aux services de confiance pour les transactions électroniques.

Partie 1: Les assisses juridiques de la preuve numérique

Chapitre 1: Nomenclatures et sources de la preuve numérique

Chapitre 2: Principes applicables à l'administration de la preuve en Droit pénal

Partie 2: Le défi de recevabilité de la preuve numérique

Chapitre 1: Critères d'appréciations techniques

Chapitre 2: Contraintes liés à la mise en œuvre des preuves numériques

Première Partie: Les assisses juridiques de la preuve numérique

La preuve revêt un rôle primordial dans le système judiciaire particulièrement en matière pénale, où elle constitue un élément déterminant pour établir la vérité et fonder les décisions de justice. Cette partie sera consacrée dans un premier chapitre, à l'étude de la nomenclature et des sources de la preuve numérique (**Premier chapitre**). Et dans un second chapitre, il sera question d'analyser les principes directeurs de preuves en matière pénale (**Deuxième chapitre**). Cette partie fournira une réflexion approfondie pour explorer plus en détail l'utilisation de la preuve numérique dans les procédures judiciaires.

Chapitre 1: Nomenclatures et sources de la preuve numérique

Nous dépendons de plus en plus des technologies numériques pour stocker, échanger et gérer des informations importantes. Cependant, cela soulève également des préoccupations quant à la fiabilité et l'authenticité de ces informations. Ce chapitre présentera la nomenclature de la preuve numérique (**A**) et examinera les sources de preuve numérique (**B**).

A. Nomenclatures:

Les preuves numériques sont classées selon plusieurs catégories, parmi lesquelles la classification en preuves persistantes et preuves volatiles. Pour expliquer ces deux types de preuves numériques, nous présentons d'abord la base sur laquelle cette classification est fondée, puis nous expliquons le contenu de cette classification[1].

Premièrement, la base de la classification:

Cette classification repose sur les deux types de mémoire utilisés dans les ordinateurs pour stocker des données ou des informations, à savoir la mémoire en lecture seule abrégée ROM, et la mémoire vive à accès aléatoire abrégée RAM[2].

Le **1ère type** de mémoire ROM est utilisé pour stocker des données de manière permanente ou stable, et l'utilisateur de l'appareil ne peut pas effacer ces données, mais il peut uniquement diriger l'unité centrale de traitement pour les lire.

Les données stockées dans **le 2ème type** de mémoire RAM sont temporaires et peuvent être perdues en cas de coupure de courant soudaine de l'appareil.

Deuxièmement, le contenu de la classification[3]:

✓ Preuve numérique **volatile**: restent même lorsque l'appareil est éteint de manière incorrecte ou lorsque l'alimentation électrique est coupée de manière inattendue.

[1] ذ مصطفى إبراهيم العربي، "دور الدليل الرقمي في الإثبات الجنائي"، مجلة البحوث القانونية المجلد 4، العدد الأول 2016، جامعة مصراتة كلية القانون، ص 67.

[2] Central Board of Direct Taxes, Department of Revenue, Government of India, "Digital Evidence - Investigation Manual ", chapter 2, 2014, p: 12.

[3] Badil. M, « L'administration de la preuve face aux défis de la cybercriminalité au Maroc », édition 2020, Imprimerie Bilal Fès, pages: 95 – 96 – 97 – 98.

✓ Preuve numérique **non-volatile:** ne sont pas sauvegardées dans la mémoire ROM en cas d'extinction de l'appareil. Il s'agit des données ou des informations stockées dans la mémoire vive de l'ordinateur, qui seront perdues en cas d'extinction inappropriée de l'ordinateur ou de coupure de courant inattendue[1].

B. Sources:

Les sources de preuve numérique sont diverses et nombreuses, et elles peuvent être divisées en deux sections pour faciliter leur présentation.

Tout d'abord, **les sources liées aux appareils électroniques**, qui font référence à tout outil électronique adapté au traitement et au stockage de données, à titre d'exemple:

✓ **les ordinateurs,** qu'ils soient fixes ou portables,

✓ **les appareils portables**, tels que les téléphones mobiles et les tablettes[2].

✓ **Les outils de stockage électronique**, tels que: **L**es disques durs externes qui sont caractérisés par leur grande capacité de stockage - **L**es supports amovibles comprennent les disques compacts, les disques numériques polyvalents et les disquettes[3]- **L**a mémoire Flash ou les clés USB - **L**es cartes mémoire utilisées avec les appareils photo, les ordinateurs, les téléphones portables, les lecteurs de musique numérique et les consoles de jeux vidéo sont également des outils de stockage électronique[4].

✓ **Les appareils photos numériques** incluent des appareils photos utilisés pour la capture d'images fixes et ceux utilisés pour l'enregistrement de vidéos ou d'images animées, généralement équipés d'une fonctionnalité de géolocalisation (GPS).

✓ **Les machines de télécopie** peuvent fournir des données liées aux fichiers stockés, aux numéros de téléphone, aux journaux de réception et d'envoi[5].

✓ **Les appareils de géolocalisation** sont souvent utilisés avec des appareils photos pour déterminer l'emplacement où l'image a été prise ou la vidéo enregistrée.

✓ **Les scanners et les photocopieurs** sont généralement équipés d'une petite mémoire pour stocker les données écrites sur les papiers. Ils peuvent donc être très utiles pour détecter des activités illégales liées à la contrefaçon de documents, telles que la création de fausses factures.

---

[1]Les enquêteurs criminels sont invités à être prudents dans la manipulation de ces données et de leur récupération, afin qu'elles ne soient pas perdues ou endommagées sans justification.

[2] Il est à noter que, en raison du développement scientifique dans le domaine de la fabrication de ces appareils, ils sont susceptibles d'être l'une des sources les plus riches de preuve numérique. Les formes de preuve numérique incluent des documents ou des fichiers électroniques, l'envoi de courriers électroniques, des messages courts, des enregistrements d'appels sortants et entrants, l'historique de navigation sur Internet, les journaux de discussion, les calendriers.

[3] U.S. Department of Justice, office of Justice Programs, National Institute Justice, "*Electronic Crime Scene Investigation: A Guide for First Responders*", Second Edition, 2001, p: 4.

[4] U.S. Department of Justice, office of Justice Programs, National Institute Justice, "*Electronic Crime Scene Investigation: A Guide for First Responders*", Op. Cit, p: 6.

[5] Central Board of Direct Taxes. Op. Cit, p: 12.

Ensuite, **les sources liées aux services d'Internet** permettant aux utilisateurs d'accéder aux sites Web pour obtenir et échanger des informations, et ces services dépendent de moyens électroniques. Nous essayons ci-dessous de signaler certains de ces moyens:

✓ **L'adresse Internet:** Numéro qui permet d'identifier un ordinateur sur le réseau Internet. Dans sa version 4, elle se décompose en une série de 4 nombres allant de 0 à 255. Adresse unique, composée de 4 nombres séparés par des points qui correspond à l'adresse numérique d'un ordinateur connecté à l'Internet, tel un numéro de téléphone[1].

✓ **Cookies:** Témoins de navigation qui conservent la mémoire d'un certain nombre d'opérations et permet à son expéditeur de collecter des données comportementales de l'internaute. Technique de traçage des clients grâce à un fichier créé automatiquement dans les ordinateurs qui permet au serveur de conserver la trace de l'ensemble des sites visités par l'utilisateur[2].

✓ **Proxy:** est un ordinateur ou un ensemble d'ordinateurs agissant en tant qu'intermédiaire entre un client et un serveur Web. Le proxy reçoit des demandes, et vérifie si elles ont été téléchargées auparavant et les enregistre dans sa mémoire cache[3], puis les envoie directement au client sans contacter le serveur Web si elles sont sauvegardées dans cette mémoire cache[4].

✓ **Service de messagerie électronique**: Certaines entreprises, institutions gouvernementales, privées et établissements éducatifs fournissent un service de messagerie électronique sur Internet pour faciliter à l'utilisateur l'exploitation de l'application.

Chapitre 2: Principes applicables à l'administration de la preuve en Droit pénal

La recherche, la collecte, et de manière plus générale, la gestion de la preuve sont encadrées par les principes dérivant du droit à un procès équitable, dont le respect conditionne l'admissibilité devant le tribunal pénal.

A. La présomption d'innocence:

« *Quand l'innocence des citoyens n'est pas assurée, la liberté l'est pas non plus*[5] »[6]

C'est un principe qui garantit un respect théorique de la dignité humaine de chaque personne accusé, à raison ou à tort, même-ci il est dans l'incapacité de protéger efficacement un

[1] QUÉMÉNER. M, CHARPENEL.Y, « *CYBERCRIMINALITÉ: Droit pénal appliqué* », Economica 2010, p: 247
[2] Op.cit, p: 248.
[3] Par conséquent, le serveur proxy peut aider les autorités d'enquête à découvrir la vérité dans les crimes faisant l'objet d'une enquête en leur fournissant des informations sur les sites visités par le coupable et la date de la visite, ainsi que les fichiers audio, vidéo et textuels demandés et la date de la demande, en examinant la mémoire cache du proxy.
[4] Pillou J, Lemainque F, « *Tout sur les réseaux et Internet* », 5ème Édition, Dunod, 2020, p. 167.
[5] L'adage témoigne de l'importance du statut d'innocence et de son lien étroit avec ce qui est le plus cher à l'Homme: Sa liberté. Effectivement, le principe de la présomption d'innocence joue incontestablement le rôle de sauvegarde des libertés individuelles.
[6] MONTESQUIEU, « *De l'esprit des lois* », Tome I, Livre XII, Chapitre II, p.197.

prévenu non définitif contre la réalité des soupçons et des rumeurs lui jetant l'anathème[1]. Ledit principe signifie que toute personne doit être considérée et traitée comme étant innocente quels que soient les soupçons qui pèsent sur elle et jusqu'au moment où un jugement irrévocable[2] rendu retient sa culpabilité.[3] Autrement dit, cette notion signifie qu'un individu est innocent tant que sa culpabilité n'a pas été prouvée par un jugement irrévocable. Elle impose à l'accusation de démontrer la culpabilité de la personne poursuivie, c'est-à-dire de renverser le jeu de la présomption[4]. Ajoutons à cela que ce droit est reconnu en droit interne, celui-ci est garanti par la Constitution dans son article 23[5]. Et aussi prévu par l'article premier du CPP[6].

B. L'intime conviction du juge:

Le principe de l'intime conviction du juge est l'un des principes procéduraux généraux qui prévalent dans les législations modernes et qui sont considérés comme des caractéristiques des pouvoirs du juge pénal, dont les plus importants sont l'acceptation de la preuve et la confiance en elle pour construire les jugements. Le processus de preuve vise enfin de compte à convaincre le juge de la vérité qu'il cherche également à mettre en évidence et à révéler tout ce qui pourrait l'entourer de mystère. Cela lui permet de rendre sa décision dans l'affaire en question. Le principe de l'intime conviction du juge est l'une des caractéristiques distinctives des systèmes de procédure modernes[7]. Cela signifie tout simplement que juge pénal a la liberté dans l'évaluation des preuves qui lui sont présentées et dans l'extraction des éléments de sa conviction de toute preuve qui le satisfait. Le principe est souvent associé à la liberté et est appelé la conviction libre du juge, où le juge dépend d'un processus logique basé sur l'inférence et la déduction, qui aboutit à une conclusion spécifique. La conviction du juge lorsqu'il examine l'action pénale, est basée sur son évaluation des preuves présentées dans l'affaire. Lors de cette évaluation, le juge effectue une opération mentale basée sur la conscience, la perception de toutes les preuves, leur analyse et la déduction de leur valeur probante, qui sont toutes réunies dans son état de certitude.

C. La liberté de la preuve:

[1] JEANCLOS Y. « *Les 7 principes du droit pénal* », 3ème Éd, Hachette Supérieur, 2021, p. 169.

[2] Selon l'article 119 de la Constitution Marocaine: « *Tout prévenu ou accusé est présumé innocent jusqu'à sa condamnation par décision de justice acquis la force de la chose jugée*. ».

[3] ESSAID M.J « *La présomption d'innocence* » Éditions La porte Rabat 1971 p. 17.

[4] BOLZE P. « *Le droit à la preuve contraire en procédure pénale* », Thèse de doctorat, Université Nancy (4) soutenue le 17 décembre 2010, p. 21.

[5] Article 13 de la Constitution Marocaine: «*Nul ne peut être arrêté, détenu, poursuivi ou condamné en dehors des cas et des formes prévus par la loi*.».

[6] La loi n° 22-01 relative à la Procédure Pénale Marocaine.

[7] Principe fréquemment réaffirmé par la Cour de Cassation Française: « *il appartient aux juges du fond d'apprécier souverainement la valeur des éléments de preuve régulièrement produits aux débats et sur lesquels se fonde leur conviction.* », Crim. 3 mars 1959, B. 142 ; 23 janv., 30 avril et 22 mai 1964, B. 27, 143 et 168 ; 21 nov. 1991, B. 427. Note cité dans: RASSAT M. « *Procédure Pénale* », Ellipses, 2017, p. 276.

La liberté de preuve en matière pénale est considérée comme la deuxième règle qui régit le processus de preuve, car elle représente la voie de preuve suivie par toutes les parties du procès.

Le principe, dans son sens commun, vise à la liberté de toutes les parties de recourir à tous les moyens de preuve pour prouver la véracité de leurs allégations. Toutes les parties impliquées dans un procès ont le droit d'utiliser tous les moyens légaux[1] pour prouver leur point de vue.

Il est essentiel que les décisions judiciaires soient fondées sur des éléments de preuve vérifiables et incontestables, pas sur des soupçons ou des hypothèses. Le juge doit toujours fonder sa conviction sur des preuves solides et décisives. Il convient à cet égard de préciser que la preuve pénale est soumise à deux aspects:

Premièrement, Le rôle du juge consiste à examiner l'existence de ces preuves conformément aux exigences légales, puis à former sa conviction quant à leur présence ou leur absence. Lorsque toutes les preuves sont disponibles, la peine prévue pour le crime commis est appliquée. En cas de preuves incomplètes, la peine est réduite. Si les preuves sont simples ou faibles, le juge ne prononce ni une condamnation ni un acquittement, mais il place le suspect dans une position de suspicion[2].

Deuxièmement, le système de conviction intime du juge est un système fondé sur la logique dans la déduction des preuves criminelles. Le juge dispose d'une large marge d'appréciation pour former sa conviction en se basant sur cette preuve, selon la croyance qui s'est formée en lui en toute liberté[3].

Deuxième Partie: Le défi de la recevabilité de la preuve numérique

L'administration de la preuve pénale s'articule autour de deux dimensions fondamentales: d'une part recueil des éléments probatoires menées par les OPJ sous la supervision du procureur du Roi, et d'autre part, l'appréciation de leur recevabilité devant les juridictions compétentes (**Chapitre 1**), Cette administration est également confrontée à divers contraintes, qu'ils soient juridiques, techniques ou pratiques, entourant le processus de collecte des preuves (**Chapitre 2**).

Chapitre 1: Critères d'appréciations techniques

Une preuve est considérée comme irrecevable, si elle est obtenue de manière illégale. Lorsqu'une telle preuve constitue l'unique élément disponible, elle ne saurait être utilisée pour fonder une condamnation. En matière de preuve numérique, des règles spécifiques encadrent

[1] En vertu de l'article 286 du CPPM, la preuve peut être établie par tout mode de preuves et le juge décide d'après son intime conviction.

[2] جودة حسين جهاد، "الإثبات الجنائي بين الشريعة الإسلامية والقانون الوضعي"، دار النهضة العربية، القاهرة، مصر، 1991، ص.11، نقلا عن إبراهيم الحمادي، "ماهيته الدليل الإلكتروني: خصائصه، شروطه وحجيته"، مرجع سابق، ص.130.

[3] رمسيس بهنام، " البوليس العلمي أو فن التحقيق"، منشأة المعارف، الإسكندرية، مصر، 1996، ص. 320، نقلا عن إبراهيم الحمادي، مرجع سابق، ص. 131.

leur collecte, leur conservation et leur présentation, règles auxquelles le système judiciaire doit scrupuleusement se conformer afin d'éviter toute invalidation des procédures. Dés lors, une preuve numérique ne peut être admise que si les conditions suivantes sont respectées:

A. La légalité de la preuve

Bien que le principe de la légalité en matière de crimes est considéré comme étant une règle fondamentale sur laquelle reposent les législations pénales modernes, mais elle ne suffit pas pour assurer une protection accrue. Si cela est faisable, il conviendrait de procéder à l'arrestation ou à la détention ou à toute mesure nécessaire pour le juger avec présomption de culpabilité, cette situation mène à une insuffisance de protection garantie par le principe:

« ***Ni infraction, ni peines, sans texte légal***[1] ». Il était donc nécessaire de renforcer cette règle par une autre règle qui régit l'organisation des procédures prises avant que l'accusé ne soit impliqué de manière à garantir le respect des droits et des libertés individuelles, appelée légitimité procédurale ou légitimité de la preuve pénale, tout en confirmant le principe de présomption d'innocence qui doit être appliqué jusqu'à preuve du contraire[2]. En conséquence, conformément au principe de légitimité procédurale, selon lequel la preuve est obtenue, la preuve n'est pas admissible dans le processus de preuve, sauf si elle est obtenue et présentée à la justice de manière légale[3] et dans le respect de l'équilibre entre le droit de l'État à punir et le droit de l'accusé à garantir les garanties de la dignité humaine[4]. La contestation repose sur la garantie de la liberté de l'accusé, ainsi que sur la preuve de l'autorité de l'État en matière de répression. Par conséquent, le juge doit prouver la disponibilité de cette autorité envers l'accusé par des procédures légales qui respectent les libertés et renforcent les garanties prévues par la loi. Il est donc clair que la légitimité de la preuve pénale exige que la procédure à partir de laquelle la preuve est obtenue soit légitime. Nous nous demandons alors quelle est la valeur de la preuve illégitime.

B. La certitude de la preuve:

Les preuves obtenues à partir d'un ordinateur ou d'Internet doivent être exemptes de doute. Le juge doit présumer l'innocence à toutes les étapes de la procédure et il n'y a pas de place

[1] En principe, nul ne peut être poursuivi qu'en vertu d'une règle de droit préexistante à son acte, tel est l'adage: « *Nullem crimen, nulla puena, sine lege* », V. Bouchard, « *Droit pénal* », Éditions Foucher, 2009, p. 16.

[2] Article 1 de procédure pénale marocain.

[3] Comme le renforce l'adage: « *Fruit de l'arbre empoisonné* », c'est une expression utilisée dans le domaine du droit pour décrire une situation dans laquelle une preuve est obtenue illégalement ou de manière frauduleuse, et ne peut donc pas être utilisée pour étayer une accusation ou une plainte.

L'analogie est que si un arbre est empoisonné, même les fruits qu'il produit seront également empoisonnés. Dans le même ordre d'idée, si la preuve est obtenue illégalement, elle est considérée comme empoisonnée et ne peut pas être utilisée pour soutenir une accusation, même si elle semble pertinente ou probante.

Cette règle découle du principe général du droit selon lequel les tribunaux ne peuvent pas encourager ou récompenser un comportement illégal ou frauduleux. Ainsi, même si une preuve pourrait sembler être la preuve décisive d'une infraction, si elle a été obtenue illicitement, elle ne peut pas être utilisée comme preuve dans une affaire judiciaire.

[4] فاضل زيدان محمد، "سلطة القاضي الجنائي في تقدير الأدلة: دراسة مقارنة"، الطبعة الأولى دار الثقافة والتوزيع عمان 2006، ص: 242-241.

pour la réfuter et présumer le contraire, sauf lorsque la conviction du juge atteint le niveau de certitude[1]. Cela peut être déterminé à partir des preuves électroniques présentées, des captures d'écran et d'autres formes électroniques qui sont disponibles via un accès direct, afin que le juge puisse déterminer la force probante et juger de la culpabilité ou de l'innocence de l'accusé.

Au Maroc, il convient de souligner que la question juridique relative à l'acceptation et la valeur probante de la preuve électronique n'a pas été abordée[2], qu'à travers les dispositions de la loi 53-05[3], où le législateur marocain a égalisé la force probante du document écrit sur support papier et du support électronique, par le biais de l'article 417-1 de la loi 53-05. Ainsi, il ressort de ce texte que le législateur marocain a ciblé l'ensemble des documents que ce soit en papier ou électronique quelle que soit la technologie utilisée. De plus, l'acceptation du document électronique comme moyen de preuve est soumis à deux conditions: **d'une part**, il est nécessaire de vérifier l'identité de la personne qui l'a émis, et **d'autre part**, il doit être conservé selon des conditions garantissant son intégrité. Le document électronique bénéficie d'une force probante équivalente à celle du document établi sur papier, de même que le législateur français[4] a clairement fait référence au principe d'égalité entre le document ordinaire et celui électronique en termes de valeur probante. L'important ici n'est donc pas la forme de la copie, qu'elle soit papier ou électronique, mais l'essentiel aux yeux du législateur est de s'assurer que cette copie est prise et conservée de manière à garantir son intégrité contre toute altération.

Notons que si le législateur marocain a entrepris de modifier les dispositions du DOC pour s'adapter à l'évolution du commerce électronique, il n'a pas pour autant traité le problème de la preuve électronique de manière pénale[5].

C. Le respect du principe du contradictoire:

Ce principe exige que la preuve criminelle soit discutée en général lors de l'audience et que le juge ne puisse fonder sa conviction que sur les éléments de preuve exposer lors le procès et soumis à la libre discussion des parties. Par conséquent, il est nécessaire de présenter toute

[1] MERLE R. et VITU A. « *Traité de droit criminel* », tom 121 édition GUJAS, Paris 1973, p.132.

[2] La loi britannique de 1984 exige que les données soient précises et produites par l'ordinateur de manière fiable afin que la certitude des preuves électroniques soit établie. Au Canada, la jurisprudence considère que les documents informatiques sont parmi les meilleures preuves, ce qui permet de réaliser la certitude souhaitée dans les décisions judiciaires. Certaines lois américaines considèrent également que les copies de données extraites de l'ordinateur sont parmi les meilleures preuves disponibles, et donc la certitude de ces preuves est établie. Les règles fédérales déclarent que la condition essentielle pour l'authentification ou la vérification de la validité ou de l'exactitude de la preuve en tant que condition préalable à son acceptation est qu'elle fournisse une évidence suffisante pour soutenir sa découverte.

[3] Dahir n° 1-07-129 du 19 kaada 1428 (30 novembre 2007) portant promulgation de la loi n° 53-05 relative à l'échange électronique de données juridiques.

[4] Articles 1316-1 et 1316-3 du Code Civil.

[5] إكرام مختاري، " تأثير ثورة التكنولوجيا على وسائل الإثبات الجنائي"، مرجع سابق.

preuve obtenue à l'aide des technologies informatiques lors l'audience[1]. Ces dispositions s'appliquent à toutes les preuves générées par les ordinateurs, ainsi qu'aux témoins de crimes informatiques. Le même principe s'applique également aux experts en systèmes informatiques, quel que soit leur domaine de spécialisation, ils devraient comparaître devant les tribunaux pour discuter leurs rapports, qui visent à montrer la vérité et à révéler la justice[2]. Il autorise l'interrogation des témoins par chacune des 2 parties, dans un souci d'équilibre dans la recherche des indices et des preuves de l'infraction. Il est à l'origine de la confrontation entre le demandeur et le défendeur. Il facilite également le jeu croisé des demandes et des réponses entre les divers acteurs du procès pénal, il dynamise le déroulement du procès en entraînant les acteurs dans des échanges de paroles et de documents pour mieux appréhender les faits incriminées de la part de leur auteur comme de celle de la victime. Ce principe attend la participation des parties et du juge dans le jeu pénal, les explications et les arguments d'une partie pouvant être contestées par l'autre partie appelée à parler contre la première. Dans ce cadre, le jeu de transparence doit être respectées par les différents acteurs du procès pénal afin d'éclairer le juge sur les faits incriminées, sur les circonstances de l'infraction et sur la personnalité de l'accusé. Il est un déterminant processuel d'importance lors de la confrontation entre les parties devant un tribunal indépendant et impartial qui traite les plaideurs sur un pied d'égalité[3].

Chapitre 2: Contraintes liés à la mise en œuvre des preuves numériques

Bien que l'article 286 du CPPM affirme la liberté de la preuve, la difficulté tient au fait que le législateur n'a pas entièrement réglementé le domaine du numérique, tandis que les récents outils technologiques sont désormais utilisés pour découvrir des indices numériques. L'admission de la valeur probatoire des documents informatiques se heurtent à plusieurs obstacles, qui peuvent être classés en deux catégories: d'une part, les contraintes objectives liés à la nature de la preuve numérique (**A**), et d'autre part les contraintes procédurales (**B**).

A. Contraintes objectives de la preuve numérique:

Ces difficultés sont liées à la nature même de la preuve numérique, en raison ses caractéristiques spécifiques, telles que son caractère intangible et les questions d'authenticité, notamment en e qui concerne sa provenance et son intégrité.

1. La preuve électronique est une preuve invisible:

[1] Comme le prévoit l'article 287 du CPPM: « *La juridiction ne peut fonder sa décision que sur des preuves versées aux débats et discutées oralement et contradictoirement devant elle*. ».

[2] MARTY M. « *La légalité de la preuve dans l'espace pénal européen* », Thèse de Doctorat, Université de Bordeaux, Soutenue le 1er avril 2014, p. 84- 85.

[3] JEANCLOS Y. Op. Cit, p. 131-132.

Un enregistrement électromagnétique stocké dans un système informatique sous forme binaire[1], et de manière désorganisée. Par exemple, les disques durs contiennent un mélange de données[2], de sorte que des fichiers innocents peuvent être mélangés à des fichiers liés à des crimes, ce qui crée le problème de violation de la vie privée. Ainsi, il est évident que la preuve numérique diffère des preuves résultant de crimes traditionnels en termes d'effets qui en découlent, ce qui facilite leur prouvabilité par les autorités judiciaires, contrairement au crime de falsification électronique qui est très difficile à prouver étant donné que la preuve de falsification électronique est constituée d'impulsions électroniques sous forme de longues séries de zéros qui sont difficiles à identifier. De plus, la preuve numérique est souvent codée ou cryptée, ce qui permet de la manipuler et de la modifier, ce qui élimine le lien entre le criminel et son crime et empêche la découverte de son identité. Par conséquent, cette preuve constitue un type différent de ce que les enquêteurs judiciaires ont l'habitude de prouver.

2. Le problème d'authenticité de preuve électronique:

L'authenticité de preuve électronique a un caractère virtuel qui ne parvient pas à atteindre ou à égaler le degré d'authenticité de preuve matériel. Par exemple, l'image qui existe dans le monde numérique n'a pas cette existence matérielle que nous connaissons sous forme de papier, mais elle est une série de chiffres. Le problème de l'authenticité a suscité un débat au niveau juridique, ce qui a conduit les législations comparées à supposer l'authenticité de preuve électronique[3]. Le problème est accru devant le silence de législateur. Par conséquent, il est indispensable de se conformer aux règles générales qui encadrent la preuve, lesquelles exigent qu'elle soit officielle pour sa validité. Cependant, l'application pratique rend la tâche extrêmement difficile, en particulier la condition que l'apparence extérieure de l'image ne permet pas de douter de sa conformité.

B. Contraintes procédurales:

Outre les difficultés inhérentes à la nature de la preuve électronique, des contraintes procédurales viennent également compliquer son traitement. Ces derniers peuvent être surmontés par les solutions suivantes:

1. Coûts élevés pour l'obtention de preuve électronique:

Les crimes techniques soulèvent souvent le problème de recourir à l'expertise dans le domaine de la falsification, qu'elle soit traditionnelle ou électronique. Cependant, cette expertise constitue un fardeau lourd sur la justice pénale, compte tenu de l'ampleur des dépenses engagées pour obtenir la preuve numérique. Le problème s'aggrave en l'absence d'organisations spécialisées telles que les universités et les instituts, en particulier dans les pays

[1] Computer Forensics procedures, tools and digital evidence bags, brett pladna what they are, and who should use them. Available at: http://www.intosecwrites.com /text ressources/pdf/bp ladna -comput procedures. pdf.er. forensic. Cité dans: إكرام مختاري، " تأثير ثورة التكنولوجيا على وسائل الإثبات الجنائي"، مرجع سابق، ص.122

[2] Hershensohn J. « I.T. Forensics the collection and presentation of digital evidence ». Available at: https://digifors.cs.up.ac.za/issa/2005/Proceedings/Full/076_Article.pdf. Seen 15/02/2023 at 23:26.

[3] إكرام مختاري، " تأثير ثورة التكنولوجيا على وسائل الإثبات الجنائي"، مرجع سابق، ص. 123.

arabes. Nous proposons donc la création de laboratoires accrédités relevant des institutions de justice pénale, équipés des dernières technologies, avec la nécessité d'échanger des informations avec des centres et des institutions gouvernementaux ou privés étrangers, afin de bénéficier de leur expérience dans le domaine. Il est important de suivre l'exemple des États-Unis en tant que pays leader dans le domaine de technologie, en organisant des séminaires, des conférences et des formations dans le cadre de la coopération internationale, afin de connaître les derniers développements[1].

2. Le manque de connaissances techniques chez le corps de justice pénale:

Il est bien connu que les organismes d'enquête, avec leurs méthodes traditionnelles, collectent des éléments de preuve en saisissant les preuves matérielles, mais dans le contexte du crime actuel qui dépend de l'utilisation de la technologie, ces organismes ne peuvent pas appliquer les procédures traditionnelles de preuve pour les crimes de contrefaçon électronique, en particulier en ce qui concerne les choses immatérielles comme lieu du crime. Ils se retrouvent incapables de traiter ce type de crimes[2], et l'enquêteur lui-même peut détruire la preuve par erreur ou par négligence[3]. Par conséquent, chaque pays doit créer une administration spécialisée dans ce type de criminalité pour recevoir les rapports, poursuivre et traquer ses auteurs, et les présenter devant les tribunaux. Il est également nécessaire de former et de qualifier le personnel de l'appareil d'enquête et d'investigation et de créer une justice spécialisée dans les crimes cybernétiques. Cela nécessite le développement de leurs compétences techniques, en adéquation avec la taille des variables et des développements successifs dans le domaine des crimes technologiques, en même temps, nous appelons à la nécessité de développer des méthodes de recherche de preuves pour suivre ces développements et ne pas être en retard.

3. Le chiffre noir:

Beaucoup de crimes liés à la technologie de l'information sont considérés comme une nouvelle forme de crimes transfrontaliers, où l'acte criminel est généralement commis à distance à l'aide de connexions téléphoniques permettant au criminel de donner des instructions à l'ordinateur pour pénétrer dans les réseaux d'informations dans des zones difficiles d'accès et pour rendre difficile son identification. Ce type de criminalité contemporaine rend la découverte de la preuve difficile. De plus, les victimes de ces crimes sont généralement des banques, des institutions financières ou des projets avec de gros investissements financiers, ce qui les empêche souvent de signaler les crimes par crainte de perturber la confiance de leurs clients et de leur réputation sur le marché. Ainsi, leur intérêt pour la découverte du crime et de ses auteurs est bien moindre que leur perte de réputation, ce qui rend les crimes informatiques

[1] إكرام مختاري، ص.126.

[2] سعيد عبد اللطيف حسن، " إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنيت"، الجرائم الواقعة في مجال تكنولوجيا المعلومات، دار النهضة العربية الطبعة الأولى 1999، ص. 129.

[3] إكرام مختاري، ص.127.

encore plus difficiles à découvrir. Ces raisons font que ces crimes ne sont souvent pas signalés aux autorités judiciaires, ce qui les rend invisibles[1] dans la société, ce que l'on appelle « le chiffre noir »[2].

CONCLUSION:

Si le sujet de cette recherche concerne les preuves obtenues par des moyens électroniques, cela aborde l'un des problèmes créés par la révolution de communication à distance. Comme nous le savons, cette révolution a beaucoup aidé l'humanité dans de nombreux domaines qui étaient auparavant difficiles à atteindre. Il ne fait aucun doute que la révolution de communication à distance a changé de nombreuses notions et termes juridiques traditionnels. Nous entendons maintenant parler de transactions bancaires électroniques, de monnaies électroniques, de documents électroniques, de tribunaux électroniques, de signatures électroniques, de falsification électronique, etc.

L'émergence de ces nouvelles opérations électroniques et la nécessité de les protéger pénalement contre les formes d'attaques sophistiquées qui peuvent être menées contre elles à l'aide de moyens électroniques avancés ont montré qu'il y avait de grandes lacunes au niveau des textes juridiques objectifs et procéduraux, de sorte que ces textes sont devenus insuffisants et incapables de garantir une protection efficace des intérêts et des valeurs créés par la révolution de communication à distance. Si nous acceptons que le droit pénal et la procédure pénale, ainsi que les autres lois, ne suffisent pas à faire face à ce nouveau type de criminalité, et que de nombreux termes scientifiques sont devenus étrangers à la loi, cela ne signifie pas que nous devons rester les bras croisés face à ce vide et à cette révolution juridique, pour ne pas violer le principe de légalité criminelle qui prévoit: pas de crime ni de peine sans texte. Au contraire, le législateur et le pouvoir judiciaire doivent travailler ensemble pour trouver des solutions légales aux problèmes soulevés par les textes et les appliquer dans la pratique.

[1] Par conséquent, nous appelons les chercheurs à accorder une attention particulière à l'étude de la criminalité cachée, car cela est important pour élaborer une stratégie précise pour lutter contre le phénomène ou du moins en atténuer l'ampleur, plutôt que de se concentrer sur l'étude de la criminalité visible. Ce type de criminalité financière a de graves conséquences sur l'économie nationale et sur l'élaboration de politiques criminelles dans notre pays, en plus de la nécessité de renforcer et de mettre à jour les mécanismes de coopération internationale.

[2] GASSIN R. et CINAMONTI S. et BONFILS P. « *Criminologie* », Dalloz, 2011, p. 145.