Revue-IRS

Revue Internationale de la Recherche Scientifique (Revue-IRS)

ISSN: 2958-8413

Vol. 4, No. 6, Novembre 2026

This is an open access article under the CC BY-NC-ND license.

La preuve numérique en matière pénale : Spécificités techniques et procédurales et appréciation par le juge

Pr. TENNOURI Asmae
Enseignante chercheure
Faculté des sciences économiques, juridiques et sociales Souissi
Université Mohammed V
Laboratoire de recherche en management des organisations, droit des affaires et développement durable

SAJIDE Asmaâ
Doctorante
Faculté des sciences économiques, juridiques et sociales Souissi
Université Mohammed V
Laboratoire de recherche en management des organisations, droit des affaires et développement durable

Résumé: La preuve numérique constitue un moyen important pour la manifestation de la vérité en matière pénale. Toutefois, ses caractéristiques soulèvent des difficultés liées à la collecte, à la conservation et à l'analyse des données numériques. Ainsi, son exploitation nécessite le respect des garanties techniques et procédurales qui permettent d'assurer la fiabilité des éléments recueillis et la régularité de leur production devant les juridictions pénales.

En outre, la preuve numérique pose la question de son appréciation par le juge pénal qui est appelé à en vérifier l'authenticité, la pertinence et la cohérence avec les autres éléments du dossier. Cette appréciation peut nécessiter le recours à une expertise technique, sans pour autant se substituer au pouvoir d'appréciation du juge.

Mots clés : preuve numérique, procédure pénale, constitution de la preuve, recevabilité, spécificités techniques.

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.**24331339**

1 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] »

De nos jours, la transformation numérique de la société a profondément modifié les méthodes de commission des infractions, ainsi que celles des enquêtes et de poursuites pénales. Ainsi, le recours aux dispositifs électroniques et l'usage d'Internet a entrainé l'émergence de nouvelles formes de criminalité, laissant derrière elles des traces numériques exploitables par les autorités judiciaires. Dans ce contexte, la preuve numérique occupe désormais une place importante dans la manifestation de la vérité.

En effet, la preuve se définit comme étant tout fait pertinent qui permet d'établir la culpabilité ou l'innocence d'une personne lors d'un procès[2]. Ainsi, la preuve numérique consiste en « *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* »[3]. Dans ce cadre, on peut dire que la preuve électronique joue un rôle central dans la résolution des affaires judiciaires et s'impose comme un élément décisif dans les enquêtes pénales. Elle permet d'obtenir des informations sur les auteurs des actes criminels, notamment les données de localisation et les contenus des échanges et communication électroniques. Il convient de souligner également que la preuve numérique ne se limite pas seulement à la cybercriminalité, mais concerne bien d'autres infractions classiques, telles que l'escroquerie et le blanchiment d'argent[4].

La collecte et l'administration de la preuve numérique nécessitent le respect de certaines exigences procédurales. En effet, la valeur probante de la preuve numérique repose largement sur les conditions dans lesquelles elle a été recueillie et conservée. Le respect des règles procédurales relatives à la perquisition et à la saisie constitue, à cet égard, une garantie essentielle. On peut dire en d'autres termes que la fiabilité de la preuve numérique ne résulte pas uniquement de son contenu technique, mais avant tout de la régularité des conditions dans

[1] Guinchard (S.) et Buisson (J.), Procédure Pénale, édition LexisNexis, 8ème édition, 2012, p. 287.
[2] UNODC, Étude détaillée sur la cybercriminalité, New York, 2013, p. 157.
[3] BOOS (R.) ; La lutte contre la cybercriminalité au regard de l'action des Etats, thèse de doctorat en droit privé et sciences criminelles, Université de LORRAINE, France, 2017, p. 202.
[4] DIRAND (C.) ; Les réquisitions de données de connexion : un régime européen en construction, Mémoire pour l'obtention d'un Master droit parcours métiers du droit, Avignon Université, 2024, p. 8.

lesquelles elle a été recherchée, saisie, et conservée. Ainsi, en matière pénale où prévaut le principe de loyauté et de légalité de la preuve, la maîtrise des règles relatives à la perquisition et à la saisie numérique apparaît comme une condition déterminante de son efficacité et de sa recevabilité.

L'étude de la preuve numérique en matière pénale revêt aujourd'hui une grande importance et ce en raison de la place qu'occupent les technologies de l'information dans la commission des infractions. En effet, les communications électroniques, les données de connexion, les contenus stockés sur des supports numériques et dans des environnements dématérialisés constituent des éléments déterminants pour l'identification des auteurs des infractions, l'établissement des circonstances des faits, ainsi que pour la reconstitution de la chronologie des événements.

Ainsi, compte tenu de ses particularités techniques qui la distinguent de la preuve traditionnelle, il a été nécessaire d'adopter des règles juridiques spécifiques, adaptées à sa nature et à ses caractéristiques, notamment en matière de perquisition et de saisie. De surcroît, la manipulation des données immatérielles, susceptibles d'être altérées ou supprimées rapidement exige un encadrement procédural rigoureux. Dans cette perspective, les réformes introduites par le code de procédure pénale en matière de perquisition et de saisie numériques traduisent l'importance croissante accordée à la preuve numérique dans le système pénal actuel. Elle témoigne, en effet, de la volonté du législateur d'adapter les mécanismes classiques d'investigation aux exigences techniques du numérique et aux garanties fondamentales du procès pénal.

Comme il a été précédemment souligné, la preuve numérique présente des caractéristiques techniques et procédurales inédites, susceptibles de compliquer son administration et son évaluation par les juridictions pénales. Dans ce contexte, les questions qui se posent sont les suivantes : **quelles sont les spécificités techniques et procédurales de la preuve numérique ? et dans quelle mesure le juge peut-il l'apprécier et en tenir compte tout en conciliant l'efficacité judiciaire avec le respect des principes du procès équitable ?**

Afin de répondre à ces questions, nous allons traiter, en premier lieu, la question relative aux spécificités techniques et procédurales de la preuve numérique (1) et, en second lieu, celle relative à l'appréciation de la preuve numérique par le juge (2).

1. Les spécificités techniques et procédurales de la preuve numérique

La preuve numérique présente de nombreuses caractéristiques techniques et procédures la distinguant de la preuve classique tangible. Dans ce cadre, nous allons traiter, d'une part, le point relatif à la nature particulière de la preuve numérique (1.1.) et, d'autre part, celui relatif aux spécificités procédurales de cette dernière (1.2.).

1.1.La nature particulière de la preuve numérique

A ce niveau nous allons traiter, dans un premier temps, la question relative aux caractéristiques techniques de la preuve numérique (1.1.1) et, dans un second temps, il sera nécessaire de mettre en relief les différentes formes et sources de ladite preuve (1.1.2).

1.1.1. Les caractéristiques techniques de la preuve numérique

La preuve numérique présente de nombreuses caractéristiques qui leur est propres. Elle se distingue, en premier lieu, par son caractère immatériel qui constitue, en effet, l'une de ses spécificités fondamentales. Contrairement aux preuves traditionnelles, la preuve numérique n'existe pas sous une forme physique tangible. Elle se manifeste par des informations codées, stockées et transmises sur des supports électroniques, qu'il s'agisse de fichiers, de base de données, de courriels, de journaux de connexion, ou de tout autre flux de données numériques. Cette immatérialité rend la preuve particulièrement vulnérable aux altérations, suppressions, ou manipulations. Par conséquent, la collecte et la conservation de la preuve numérique nécessitent le recours à des mesures techniques spécifiques qui garantissent son intégrité et sa fiabilité.

De surcroît, le caractère immatériel de la preuve numérique implique que sa présentation devant les juridictions passe par des procédés de matérialisation, notamment par des impressions ou par la réalisation des copies sur des supports physiques, et ce afin d'en permettre l'appréciation dans le cadre du procès. Il convient de préciser à ce stade que l'extraction, l'impression ou la réalisation d'une copie des données informatiques, qui constituent des éléments de la preuve numérique, ne confèrent pas à cette dernière la nature d'une preuve tangible au sens traditionnel du terme. Cette opération ne constitue qu'un procédé technique de matérialisation de la preuve numérique, ayant pour but de la rendre visible, accessible et exploitable par les parties et par le juge dans le cadre de l'instance[5].

[5] طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، مجلة الحقوق، المجلد 12، العدد 1، ص. 44.

La preuve numérique se caractérise également par sa nature volatile[6], qui constitue en réalité l'une des principales spécificités et sources de fragilité. En effet, les données informatiques et les traces numériques peuvent être facilement supprimées, modifiées ou manipulées, ce qui complique considérablement les investigations menées par les autorités compétentes[7].

Dans ce cadre, les cybers délinquants ont tendance à recourir à une pluralité de procédés informatiques destinés à la dissimulation et à la détérioration des éléments de preuve, notamment la détérioration des systèmes informatiques, l'introduction de fausses données dans lesdits systèmes, l'altération des données qui y sont stockées, ou encore la modification des programmes informatiques, et ce sans laisser de traces apparentes permettant d'établir l'existence de telles modifications ou altérations.

En outre, le caractère volatile de la preuve numérique pose avec acuité particulière la question des données informatiques qui, par nature, ne sont pas destinées à être durablement conservées, notamment les données de trafic et de localisation[8]. Ces dernières sont souvent générées d'une manière automatique et transitoire, et supprimées après un délai limité, ce qui limite considérablement la période pendant laquelle elles peuvent être collectées.

Il convient de souligner également qu'il en va de même des données à caractère personnel transmises dans le cadre des communications électroniques, qui ne peuvent être conservées que pour des finalités strictement déterminées, telles que des besoins techniques, commerciaux ou lorsque l'utilisateur donne expressément son consentement[9]. En dehors de ces hypothèses, les données doivent être effacées ou rendues anonymes dès lors qu'elles ne sont plus nécessaires à la réalisation de la finalité poursuivie.

Ainsi, la preuve numérique se distingue par son caractère scientifique et technique, dans la mesure où son identification, extraction et analyse requièrent, d'une part, des compétences techniques spécialisées[10] et, d'autre part, des programmes et logiciels adéquats à sa nature.

Au Maroc, plusieurs organismes ont été créés afin de recueillir la preuve numérique, notamment le Laboratoire d'analyse des traces numériques qui relèvent de la Brigade Nationale de la Police

[6] ENYEGUE (C.) ; « L'enquête pénale à l'épreuve de l'internet », Revue Internationale du chercheur, Volume 5 : Numéro 1, 2024, p. 930.

[7] ENYEGUE (C.) ; « L'enquête pénale à l'épreuve de l'internet », op.cit., p. 930.

[8] FRANSSEN (V.), BERRENDORF (A.), et CORHAY (M.) ; « La collecte transfrontière de preuves numériques en matière pénale. Enjeux et perspectives européennes », RIDP, 2019, p. 2. Disponible sur : https://www.penal.org/sites/default/files/Franssen%20collecte%20transfrontiere_0.pdf

[9] FRANSSEN (V.), BERRENDORF (A.), et CORHAY (M.) ; « La collecte transfrontière de preuves numériques en matière pénale. Enjeux et perspectives européennes », op.cit., p. 2.

[10] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، دار الفكر الجامعي، 2020، مصر، ص. 158.

judiciaire[11]. Cet organisme est chargé de rechercher et d'extraire les éléments de preuve numérique à partir des supports informatiques physiques saisis lors de la perquisition judiciaire, en se basant sur des procédures standardisées. Ainsi, il utilise des conditionnements spécifiques à chaque type de preuve afin d'en garantir la préservation, l'intégrité et la valeur probante[12].

On peut ajouter à ce qui a été précédemment mis en relief que la preuve numérique se distingue également par son caractère transnational. En effet, les données informatiques, susceptibles de constituer une preuve numérique, peuvent être hébergées sur des serveurs situés à l'étranger, ce qui soulève de nombreux défis juridiques et procéduraux.

1.1.2. Les différentes formes et sources de la preuve numérique

La détermination des différentes formes et sources de la preuve numérique revêt une importance majeure, dans la mesure où c'est cette classification qui permettra d'apprécier la valeur probante des éléments recueillis.

S'agissant des différentes formes de la preuve numérique, on peut dire qu'elles se déclinent principalement en quatre formes, chacune d'elles représente des caractéristiques et des enjeux spécifiques. Il s'agit, en effet, des images numériques, des enregistrements sonores, des données de dispositifs connectés, ainsi que des textes numériques[13] :

- Les images numériques constituent une représentation visuelle des faits liés à l'infraction. Elles peuvent être présentées soit sous forme imprimée, soit directement sur des supports électroniques (photos, vidéos, captures d'écran).
- Les enregistrements sonores regroupent les données audios, captées et stockées à l'aide de dispositifs numériques, notamment les conversations téléphoniques et les communications vocales via Internet.
- Les données de dispositifs connectés, tels que les Smartwatches et autres objets connectés. Ces dispositifs peuvent fournir des informations précieuses, à savoir la géolocalisation, les relevés biométriques et les traces d'activité permettant de reconstituer les faits ou de corroborer d'autres éléments de preuves.
- Les textes numériques englobent l'ensemble des contenus écrits, produits à l'aide de supports numériques, tels que emails, les SMS, les messages instantanés et les publications en ligne.

[11] ABOU EL JAOUAD (A.) ; La preuve numérique à l'épreuve de la cybercriminalité en droit marocain, rev. Droit et société, n°11, 2023, p. 13.
[12] Ibid.
[13] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص. 145.

Il convient de souligner à ce stade que les preuves numériques peuvent être extraites tant des appareils et programmes informatiques utilisés par le cyber délinquant que de ceux appartenant à la victime.

S'agissant des appareils informatiques qui appartiennent au cyber délinquant ou la victime, on peut citer, en premier lieu, l'ordinateur qui constitue une source essentielle dans la constitution de la preuve numérique. Ce dernier se compose de deux éléments indissociables que sont le matériel (*hardware*) et le logiciel (*software*)[14], formant ainsi un ensemble d'éléments informatiques[15]. Dans ce cadre, et afin de pouvoir extraire les éléments de preuve nécessaires à la manifestation de la vérité, un examen doit porter à la fois sur les aspects matériels et immatériels de l'ordinateur.

En ce qui concerne l'examen du *hardware*, on peut dire qu'il permet d'identifier un volume important de données informatiques susceptibles de constituer des éléments de preuve. Il permet, en effet, d'accéder au contenu de certaines données dont le traitement permettrait de révéler la valeur probante des informations qu'elles contiennent, y compris les données supprimées, modifiées ou dissimulées. On doit souligner à ce stade qu'à l'issue de cet examen, l'ensemble des données exploitées par le cyber délinquant est susceptible d'être mis en évidence, notamment les sites internet consultés, les courriels échangés, les programmes informatiques utilisés, ainsi que les fichiers téléchargés ou stockés sur le système[16].

Alors que pour l'examen du *software*, on peut dire qu'il repose sur l'analyse de la structure logique des programmes installés sur l'ordinateur, notamment ceux téléchargés via Internet. Cette analyse vise principalement à déterminer l'origine des fichiers existants, leur mode d'installation, ainsi que leur utilisation effective dans la commission de l'infraction. En outre, cet examen englobe l'ensemble des données stockées dans l'ordinateur et celles susceptibles d'être récupérées par des techniques d'investigation numérique[17].

De surcroît, l'examen peut porter sur les systèmes de connexion à Internet, afin de rechercher les éléments de preuve permettant de déterminer le lieu de commission de l'infraction. De même, cette méthode conduit à l'identification de l'adresse IP qui permet de reconnaître l'ordinateur ou l'appareil connecté au réseau Internet.

[14] عبد الرزاق رفيق، جرائم النصب والاحتيال عبر الانترنيت. دراسة مقارنة، الطبعة الأولى، مكتبة الرشاد سطات، 2019، المغرب، ص. 203.
[15] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص. 145.
[16] عبد الرزاق رفيق، جرائم النصب والاحتيال عبر الانترنيت، المرجع السابق، ص. 203.
[17] عبد الرزاق رفيق، جرائم النصب والاحتيال عبر الانترنيت، المرجع السابق، ص. 204.

Ainsi, sont susceptibles de faire l'objet d'un examen et de constituer des sources d'extraction des éléments de preuve numérique, les supports et les dispositifs suivants :

- Les appareils portables, qui constituent aujourd'hui des vecteurs majeurs de la preuve numérique, en raison de la diversité des données qu'ils contiennent, notamment les communications électroniques (appels, messages, courriels), les historiques de navigation, les contenus multimédias, ainsi que les métadonnées associées qui permettent d'identifier les utilisateurs, de retracer leurs activités et de situer les faits dans le temps et l'espace.
- Les outils de stockage des données[18], qui désignent l'ensemble des dispositifs et services qui permettent de conserver, organiser et rendre accessibles les données informatiques, notamment :

➢ Le stockage local physique, qui inclut les supports de stockage directement rattachés à un appareil ou pouvant lui être connecté, à savoir les disques durs internes ou externes, les clés USB et les cartes mémoire.[19]

➢ Le stockage en réseau local (NAS- Network Attached Storage), qui consiste en des systèmes de stockage partagés, connectés à un réseau local et accessibles depuis plusieurs appareils.[20]

➢ Le stockage cloud (stockage infonuagique), qui repose sur des serveurs distants accessibles via Internet. Ce mode de stockage permet de conserver des fichiers sur des infrastructures hébergées par des prestataires de services. Parmi les services de stockage Cloud les plus répandus figurent Google Drive, OneDrive, Dropbox, iCloud et Proton Drive[21].

- Les appareils de géolocalisation[22], qui sont utilisés d'une manière autonome ou intégrée à d'autres dispositifs, tels que les téléphones mobiles, les véhicules, ou encore les objets connectés. Ils permettent de déterminer avec précision la position géographique d'une personne, d'un objet, ou d'un événement à un moment donné, contribuant ainsi à la reconstitution du déroulement des faits.
- Les objets connectés, qui occupent une place croissante dans le champ de la preuve numérique. Il s'agit notamment des montres et bracelets connectés qui sont capables

[18] https://www.netapp.com/fr/data-storage/what-is-data-storage/ (consulté le 17/12/2025)
[19] https://www.dropbox.com/fr_CA/resources/storage-devices (consulté le 17/12/2025)
[20] https://www.ibm.com/fr-fr/think/topics/network-attached-storage (consulté le 17/12/2025)
[21] https://www.dropbox.com/fr/resources/what-is-cloud-storage (consulté le 17/12/2025)
[22] JELDA (H.) et ECHCHARYF (H.) ; « Les conditions de recevabilité de la preuve numérique », Revue Marocaine des Eudes Juridiques et Economiques, Numéro 14, Mars, 2025, p. 424.

d'enregistrer des données relatives à l'activité physique, aux déplacements, aux horaires, et à la localisation de leurs utilisateurs, les systèmes de domotique, tels que les caméras de surveillance intelligentes, les alarmes et les sonnettes connectées[23], ainsi que les véhicules connectés, qui collectent des informations relatives aux trajets, à la vitesse, aux arrêts et aux habitudes de conduite.

On peut noter à ce stade que les données générées par ces objets, qui sont souvent horodatés et associés à des métadonnées précises, permettent d'établir des comportements, de confirmer une présence ou une absence sur un lieu donné, ou encore de corroborer d'autres éléments de preuve numérique.

Il convient de souligner également que les institutions publiques et privées, ainsi que les exploitants de réseaux publics de télécommunication, constituent à leur tour des sources susceptibles de fournir les éléments de preuve nécessaires à l'enquête. Dans ce cadre, l'art. 64-1 du CPP prévoit que l'officier de police judiciaire peut mandater toute personne, institution publique ou privée, ou toute administration publique détentrices de données utiles à l'enquête, y compris celles stockées dans des STAD ou dans tout autre système informatique, afin de les lui fournir, même sous forme électronique. Cet article prévoit également que l'officier de police judiciaire peut demander à tout exploitant de réseaux publics de télécommunication de mettre à sa disposition l'ensemble de données nécessaires à la manifestation de la vérité et auxquelles le suspect a eu accès.

1.2.Les spécificités procédurales liées à la preuve numérique

Outre ses caractéristiques techniques spécifiques, la preuve numérique se caractérise également par ses spécificités procédurales, notamment en matière de collecte et de conservation. Dans ce cadre, nous allons traiter, en premier lieu, la question relative aux modalités de collecte et de conservation des éléments de la preuve numérique (1.2.1.) et, en second lieu, celle relative à l'existence d'autres mesures qui permettent sa constitution (1.2.2.).

1.2.1. Les modalités de collecte et de conservation des éléments de la preuve numérique

Les modalités de collecte et de conservation de la preuve numérique diffèrent de celles applicables à la preuve traditionnelle et ce en raison de la nature immatériel et volatile de la première.

[23] https://www.dovit.com/blog/systeme-domotique-qu-est-ce-que-c-est-et-comment-ca-fonctionne/ (consulté le 18/12/2025)

La collecte des éléments de preuve numérique repose sur un ensemble de techniques d'enquête prévues par le code de la procédure pénale, comprenant notamment les perquisitions et les saisies des données informatiques et des supports électroniques.

S'agissant de la perquisition, on peut dire que la perquisition classique se distingue fondamentalement de celle numérique, dans la mesure où la première se réalise dans un espace géographique déterminé, tandis que la seconde se caractérise par son caractère transfrontalier. À ce titre, la perquisition numérique peut porter sur des systèmes informatiques ou des données localisées à l'étranger dès lors qu'ils sont accessibles à partir du système initial situé sur le territoire national[24]. En outre, la perquisition classique s'effectue, en principe, en présence du propriétaire du domicile, de l'occupant des lieux, ou du détenteur des biens saisis. En revanche, la perquisition numérique peut, dans certaines hypothèses, être engagée sans la présence de la personne concernée, voire à son insu, ce qui soulève d'importantes questions quant aux garanties procédurales et à la protection des droits fondamentaux.

Au Maroc, avant la réforme du CPP, les dispositions de ce dernier se révélaient inadaptées à la nature immatérielle de la preuve numérique, dans la mesure où elles étaient principalement conçues pour appréhender des éléments de preuve à caractère matériel. En revanche, le CPP dans sa version réformée a pris en considération l'immatérialité de certains éléments de preuve.

Dans ce cadre, l'art. 59 du dudit code prévoit que lorsque la nature du crime ou du délit est de nature à être établie par la saisie des documents ou autres objets se trouvant en la possession des personnes soupçonnées d'avoir participé à la commission de l'infraction, ou détenant des documents, données, outils, programmes informatiques ou tout autre objet ayant un lien avec les faits criminels, l'officier de police judiciaire se transporte immédiatement au domicile de ces personnes afin d'y procéder à une perquisition. Cette dernière peut être effectuée dans tous les lieux et sur tous les biens meubles où peuvent se trouver des éléments de preuve utiles à la manifestation de la vérité.

De surcroît, le législateur marocain, à travers les dispositions du CPP, prévoit qu'une perquisition numérique peut être effectuée au moyen des systèmes informatiques et des dispositifs électroniques, chaque fois que la nécessité de l'enquête l'exige, tout en procédant à la saisie de l'ensemble des données, preuves et traces numériques utiles à la manifestation de

[24] ENYEGUE (C.) ; « L'enquête pénale à l'épreuve de l'internet », op.cit., p. 933.

la vérité, y compris celles ayant fait l'objet d'un déchiffrement ou ayant été récupérée après avoir été supprimées[25].

La question qui se pose à ce stade est de savoir dans quelle mesure les composantes immatérielles des systèmes informatiques peuvent faire l'objet d'une perquisition.

En effet, la perquisition des composantes immatérielles des systèmes informatiques a soulevé des défis juridiques majeurs. L'art. 19 de la Convention de Budapest sur la cybercriminalité prévoit que les Etats doivent adopter les mesures législatives nécessaires permettant à leurs autorités, d'une part, de perquisitionner et d'accéder aux systèmes informatiques et aux données qui y sont stockées, ainsi qu'aux supports de stockage informatique permettant de stocker les données informatiques sur leur territoire, et, d'autre part, d'étendre la perquisition ou l'accès aux données stockées dans un autre système informatique situé sur leur territoire national du moment où les données sont légalement accessibles à partir du système initial ou disponible pour celui-ci.

Dans ce cadre, le législateur marocain prévoit qu'au cours d'une perquisition, les autorités compétentes peuvent accéder aux données intéressant l'enquête en cours, qu'elles soient stockées dans un système informatique implanté sur les lieux où se déroule la perquisition ou encore dans un autre système, dès lors qu'elles sont accessibles à partir du système initial[26].

On peut noter également que les données, auxquelles il a été accédé, peuvent être conservées sur un support électronique, ou encore donner lieu à la saisie dudit support, lequel est placé dans une enveloppe, un contenant ou un sachet, puis scellé par l'officier de police judiciaire.

En effet, la saisie a pour objet de placer sous contrôle de l'autorité judiciaire l'ensemble des biens et documents de nature à contribuer à la manifestation de la vérité[27], tout en assurant la préservation des éléments de preuve contre tout risque de disparition ou de détérioration.

Ce point conduit à s'interroger sur les mécanismes juridiques et techniques de la saisie des données et des programmes informatiques, ainsi que sur les conditions selon lesquelles cette saisie doit être mise en œuvre.

Dans ce cadre, le législateur marocain prévoit que la saisie des données et programmes informatiques s'effectue soit par la mise sous scellés des supports matériels contenant les données utiles, soit par la réalisation de copies de celles-ci[28].

[25] Art. 59 du CPP.
[26] ENYEGUE (C.) ; « L'enquête pénale à l'épreuve de l'internet », op.cit., p. 933.
[27] DIK (A.) ; « Règles pénales procédurales relatives aux délits informatiques », op.cit., p. 46.
[28] Art. 59 du CPP.

Ainsi, le procureur général du roi ou le procureur du roi, selon le cas, peuvent ordonner la suppression définitive des données ou programmes informatiques originaux du support matériel qui n'a pas encore été mis à la disposition du tribunal, et ce après qu'une copie en a été effectuée, lorsque leur détention ou leur utilisation est illicite, lorsqu'ils constituent une menace pour la sécurité des personnes ou des biens, ou encore lorsqu'ils sont contraires aux bonnes mœurs. Cependant, la suppression des données pourrait avoir des conséquences préjudiciables et ne devrait être effectuée qu'après décision du juge du fond. Dans ce contexte, il apparaît plus prudent de rendre ses données temporairement inaccessibles, en raison du caractère réversible de cette mesure[29].

Viens à ce niveau la question relative à la conservation de la preuve numérique. En effet, la conservation des données et traces informatiques joue un rôle très important dans l'efficacité des enquêtes judiciaires et ce vu qu'à défaut d'une conservation adéquate, lesdites données et traces risqueraient d'être altérées, détruites ou de perdre leur valeur probante.

Dans ce cadre, les autorités judiciaires disposent des mécanismes concrets pour assurer la protection des preuves numériques, tels que la mise sous scellés des appareils et supports informatiques et la réalisation de copies des données qui y sont stockées. Toutefois, le CPP ne prévoit pas des procédures autonomes dédiées à la preuve numérique et n'instaure pas des mesures formelles de conservation accélérée inspirées des normes internationales, telles que celles prévues par la Convention de Budapest.

1.2.2. Autres mesures permettant la constitution de la preuve numérique

Outre la perquisition et la saisie numériques, il existe bien d'autres techniques d'enquête qui permettent la constitution de la preuve numérique. Parmi ces techniques on peut citer l'enquête sous pseudonyme[30]. Cette dernière constitue une technique qui s'applique à de nombreuses infractions, notamment celles qui portent atteinte aux STAD ou commises par des moyens électroniques.

Dans ce cadre, le législateur marocain autorise les enquêteurs à utiliser une identité d'emprunt et à se comporter comme des délinquants et ce afin de pouvoir procéder à la constitution des preuves relatives à chaque infraction. C'est une technique connue sous le terme de « l'infiltration ». En effet, conformément aux dispositions de l'art. 82-3-1 du CPP, l'infiltration consiste en une technique d'enquête qui permet aux officiers ou aux agents de police judiciaire,

[29] DIK (A.) ; « Règles pénales procédurales relatives aux délits informatiques », op.cit., p. 47.
[30] BENTELHI (H.) ; L'enquête pénale à l'épreuve de la cybercriminalité, Mémoire pour l'obtention d'un Master de Droit pénal et sciences criminelles, Panthéon-Assas Université Paris, 2024, p. 50.

sous le contrôle du ministère public, de surveiller des personnes suspectes, en se présentant comme auteur, coauteur, complice ou encore bénéficiaire des actes criminels faisant l'objet de l'enquête. Cette démarche implique l'usage d'une identité, ou d'une qualité d'emprunt, ou encore le recours à toute personne habilitée à cet effet pour interagir par des moyens de communication électronique avec une ou plusieurs personnes suspectées d'avoir commis l'infraction en question.

Il importe de préciser que, dans le cadre de l'enquête sous pseudonyme, l'enquêteur peut, soit s'introduire au sein d'un réseau de cyber délinquants et prendre part aux échanges électroniques qui s'y déroulent, soit utiliser le profil de la victime, après avoir obtenu son consentement, afin d'établir une communication avec l'auteur de l'acte criminel[31].

De surcroît, la preuve numérique peut être également constituée par le biais de l'interception des appels téléphoniques et, plus généralement, par l'interception des communications effectuées au moyen des dispositifs de communication à distance, ainsi que par l'interception de toute autre forme de communication électronique ou de communications réalisées à l'aide des technologies modernes. Il convient de souligner à ce niveau que le contenu des communications interceptées peut être enregistré et servir de preuve par la suite[32].

Ainsi, la constitution de la preuve numérique peut résulter de la captation, la fixation, la transmission et l'enregistrement des sons et des images, ainsi que des données électroniques et des données de géolocalisation.

Dans ce cadre, le législateur marocain autorise le recours à des dispositifs techniques spécifiques permettant, d'une part, de localiser les personnes suspectes et de surveiller leurs déplacements et, d'autre part, de capter, fixer, transmettre et enregistrer les propos tenus par une ou plusieurs personnes, que ce soit dans des lieux ou dans des moyens de transport publics ou privés. Ces dispositifs permettent également la captation d'images d'une ou plusieurs personnes dans un lieu public ou privé[33].

Ces dispositifs visent, en effet, à accéder aux données électroniques et aux informations stockées ou consultées au moyen des dispositifs de communication électronique. Il convient dans ce cadre de procéder à l'enregistrement, la conservation et la transmission desdites données et informations, soit sous la forme dans laquelle elles ont été stockées dans le système

[31] BENTELHI (H.) ; L'enquête pénale à l'épreuve de la cybercriminalité, *op.cit*., p.51.
[32] L'art. 108 du CPP.
[33] L'art. 116-1 du CPP.

informatique, soit telle qu'elles apparaissaient à l'écran de l'utilisateur d'un STAD, ou encore sous la forme sous laquelle elles ont été introduites, modifiées ou transmises.

S'agissant des données affichées à l'écran et introduites par saisie de caractères, les enquêteurs peuvent recourir à l'utilisation d'un keylogger. Il s'agit d'un logiciel d'espionnage permettant d'enregistrer d'une manière continue l'ensemble des frappes effectuées sur le clavier au niveau du système d'exploitation. Ce dispositif technique permet de mémoriser les données saisies par l'utilisateur, qu'il s'agisse de mots de passe, d'identifiant, de messages ou de toute autre information introduite manuellement. L'intérêt d'un tel dispositif réside dans sa capacité à capter l'information au moment même de sa création, avant toute opération de chiffrement ou de transmission, ce qui en fait un outil particulièrement efficace pour faire face aux contraintes techniques, à savoir celles liées à la protection des données ou aux mécanismes d'authentification renforcée[34].

Par conséquent, le défaut de la mise en place d'un tel dispositif peut compromettre l'efficacité de l'enquête, en exposant la procédure à des contraintes techniques, notamment les mécanismes de double authentification, qui subordonnent l'accès aux données à une validation par l'utilisateur, généralement matérialisée par l'envoi d'un code temporaire par message ou par courrier électronique[35].

Il convient de préciser que l'ensemble des opérations précitées est effectué à l'insu des personnes concernées. Toutefois, afin d'en garantir la légalité et d'assurer la protection de la vie privée, le législateur marocain a subordonné le recours à ses opérations à l'obtention d'une autorisation préalable délivrée, selon le cas, par le procureur général du roi ou par le juge d'instruction.

Ainsi, il importe de souligner que le contenu des enregistrements, ainsi que les données électroniques stockées dans des systèmes informatiques, font l'objet d'une transcription dans un PV, lequel est annexé au dossier de la procédure[36].

Finalement, on peut dire que les logiciels d'investigation numérique occupent aujourd'hui une place centrale dans la collecte, l'analyse et la conservation des preuves dans le cadre des enquêtes pénales. Parmi ces outils on peut citer le logiciel Magnet AXIOM qui est un logiciel développé par Magnet Forensics et qui permet non seulement la récupération des données supprimées, mais également la centralisation et l'analyse des preuves provenant des

[34] BENTELHI (H.) ; L'enquête pénale à l'épreuve de la cybercriminalité, *op.cit*., p.55.
[35] Ibid.
[36] Art. 116-5 du CPP.

sources diverses, telles que des ordinateurs, les téléphones mobiles ou les services cloud, au sein d'un même dossier d'enquête. Ainsi, sa puissance réside dans sa capacité à traiter simultanément plusieurs types de données, ce qui offre une vision globale des activités numériques de la personne concernée[37].

De même, le logiciel Forensic Toolkit (FTK), développé par AccessData, est un logiciel qui permet de scanner des supports de stockage afin d'identifier et d'extraire les éléments de preuve pertinents pour l'enquête, y compris les fichiers effacés ou dissimulés. Son module complémentaire, FTK Imager, permet de créer des images forensiques exactes des disques et autres supports numériques, ce qui garantit la préservation de l'intégrité des données et la fiabilité de la preuve originale[38].

2. L'appréciation de la preuve numérique par le juge

Au niveau de cette partie, nous allons traiter, dans un premier temps, la question relative aux critères d'appréciation de la preuve numérique (2.1.), alors que dans un second temps, nous allons mettre en relief certaines recommandations dans le but de renforcer le cadre juridique et technique relatif à la preuve numérique (2.2).

2.1.Les critères d'appréciation de la preuve numérique

L'admissibilité de la preuve numérique constitue une étape préalable et déterminante dans le processus juridictionnel. En effet, avant d'examiner la valeur probante de la preuve numérique et son lien avec les faits incriminés, le juge s'assure de son admissibilité juridique, et par conséquent, elle ne pourrait produire des effets juridiques tant qu'elle n'a pas été régulièrement obtenue et introduite dans le débat judiciaire.

Ainsi, la preuve numérique doit, d'une part, permettre de prouver la commission de l'infraction et, d'autre part, présenter une valeur juridique probante qui est conditionnée par le respect des règles encadrant sa collecte, son traitement et sa conservation. À cet égard, on peut dire que l'admissibilité de la preuve numérique par le juge est conditionnée par la légalité des opérations entamées dans le cadre de l'enquête judiciaire, le respect des droits et libertés fondamentaux et l'observation des garanties procédurales.

De surcroît, lorsque la preuve est admise, son appréciation ne se limite pas à une lecture purement juridique, mais impose également une analyse technique approfondie qui doit porter

[37] https://www.magnetforensics.com/fr/resources/outils-modernes-de-criminalistique-numerique-decouvrez-comment-de-nouveaux-outils-eliminent-le-bruit-pour-trouver-des-preuves/ (consulté le 28/12/2025)
[38] https://en.wikipedia.org/wiki/Forensic_Toolkit (consulté le 28/12/2025)

notamment sur son intégrité, son authenticité, sa fiabilité et sa traçabilité. On doit souligner à ce stade que la conservation des données numériques doit être effectuée dans des conditions garantissant l'absence de toute altération ou suppression.

Dans ce cadre, nous allons traiter, en premier lieu, la question relative aux critères juridiques et procéduraux qui visent à garantir la légalité et l'admissibilité de la preuve numérique (2.1.1.) et, dans un second lieu, celle relative au recours à l'expertise technique pour l'évaluation de la valeur probante de cette dernière (2.1.2).

2.1.1. Les critères juridiques et procéduraux d'appréciation de la preuve numérique

En matière pénale, l'appréciation de la preuve repose sur le principe de l'intime conviction du juge ; un principe selon lequel le juge forme sa conviction à partir des éléments de preuve figurant au dossier. Ainsi, la preuve est libre en la matière, et par conséquent, les parties peuvent prouver leurs prétentions par tout moyen de preuve. Dans ce cadre, l'art. 280 du CPP prévoit que les infractions peuvent être établies par tout moyen de preuve, à moins que la loi n'en dispose autrement. Cet article prévoit également que le juge statue selon son intime conviction. Or, la décision rendue doit être dûment motivée.

On peut donner à titre d'exemple les dispositions de l'art. 106 du CPP qui prévoit que le juge d'instruction peut, en l'absence de toute contestation sérieuse ou lorsque les moyens de preuve disponible sont insuffisants, ordonner la restitution des objets, instruments, moyens de transport ou production saisis au cours de l'enquête à la personne qui y a droit. En effet, les dispositions de cet article s'inscrivent dans le cadre du principe de l'intime conviction du juge et lui confèrent la faculté d'évaluer dans quelle mesure les éléments de preuve figurant au dossier sont suffisants pour établir la commission de l'infraction. De même, le juge d'instruction peut décider la non poursuite lorsqu'il constate que les faits ne sont pas punissables par la loi en vigueur, qu'ils ne sont plus constitutifs d'infraction pénale, ou que les moyens de preuve recueillis demeurent insuffisants pour fonder des poursuites[39].

Ainsi, le juge est appelé à examiner la régularité de la constitution de la preuve, notamment la preuve numérique. En effet, il doit s'assurer du respect du principe de légalité des diligences procédurales et du respect des droits des parties, conformément aux modalités prévues par le CPP[40].

À ce stade, on peut donner l'exemple de l'opération d'infiltration. Le CPP prévoit que cette opération est subordonnée à l'obtention de l'accord du ministère public. Cet accord doit

[39] Art. 216 du CPP.
[40] Art.3 du CPP.

être établi par écrit et doit préciser l'infraction justifiant le recours à l'opération d'infiltration, ainsi que l'identité de l'officier de police judiciaire sous la responsabilité duquel ladite opération serait menée. Ainsi, l'accord doit préciser la durée pendant laquelle l'opération serait exécutée. Il convient de souligner que l'opération d'infiltration doit être exécutée dans un délai de quatre mois, susceptible d'être prolongé une seule fois. Tout accord verbal, non motivé, ou encore ne comportant pas les informations précitées est de nature à entraîner la nullité de l'opération[41].

De surcroît, ladite opération ne peut être menée que par un officier ou agent de police judiciaire dûment habilité à cet effet et doit faire l'objet d'un PV ou d'un rapport rédigé par l'officier chargé de la coordination de l'opération. En effet, le non-respect de ces exigences entraîne également la nullité de l'opération et des actes qui en découlent, lesquels ne peuvent alors produire aucun effet juridique[42]. Il convient de souligner à ce stade que lorsque le juge constate que l'opération d'infiltration a été réalisée en violation des dispositions en vigueur, il peut écarter tout document y relatif du dossier.

Outre l'opération d'infiltration, le législateur marocain soumet également l'opération d'interception des appels téléphoniques, des communications effectuées au moyen des dispositifs de communication à distance, ainsi que celles électroniques à un ensemble d'exigences légales.

En principe, l'interception des communications nécessite une ordonnance rendue par le premier président de la Cour d'Appel sur demande du procureur général du roi. Toutefois, en cas d'extrême urgence, ce dernier peut ordonner par écrit la mise en œuvre de cette opération. Dans cette perspective, il serait tenu d'informer le premier président de l'ordonnance qu'il a émise. Si ce dernier décide l'annulation de l'ordonnance, l'opération d'interception doit être immédiatement interrompue et l'ensemble des diligences y relatives est annulé. Il est à noter que si le procureur général du roi n'informe pas le premier président de l'ordonnance qu'il a émise, ou si l'opération d'interception est exécutée par des personnes non-habilitées par la loi, ladite opération serait frappée de nullité[43].

On doit mettre en relief à ce niveau que tout document frappé de nullité doit être retiré du dossier et conservé au secrétariat-greffe de la cour d'appel, et ne peut plus servir de moyen de preuve[44].

[41] Art. 82-3-3 du CPP.
[42] Art. 82-3-1 du CPP.
[43] Art. 108 du CPP.
[44] Art. 213 du CPP.

D'après ce qui a été a été précédemment souligné, on peut dire que le juge doit s'assurer, en premier lieu, de la régularité et de la légalité des modalités d'obtention des éléments de preuve, et ce n'est qu'après la vérification du respect des exigences prévues par la loi qu'il peut procéder à l'examen de la valeur probante des éléments figurant au dossier et apprécier dans quelle mesure ceux-ci sont suffisants pour établir la commission de l'infraction et l'implication de la personne concernée.

De surcroît, le principe du contradictoire constitue à son tour une garantie fondamentale dans l'appréciation de la preuve numérique. Il implique que toutes les parties aient connaissance des moyens de preuve présentées et puissent y répondre de manière effective et ce afin de préserver l'équilibre procédural et protéger les droits de la défense. Dans ce cadre, l'art. 287 du CPP prévoit que le tribunal ne peut fonder ses décisions que sur des preuves présentées au cours de l'audience et débattues oralement et contradictoirement devant lui. Par conséquent, tout élément de preuve obtenu irrégulièrement ou présenté hors du cadre contradictoire doit être exclu du dossier.

2.1.2. Le recours à l'expertise technique pour l'évaluation de la valeur probante de la preuve numérique

La preuve numérique, en raison de sa nature immatérielle, volatile et techniquement complexe, échappe souvent à l'appréciation directe du juge. Selon David BENICHOU, « *les premières attentes du juge dans le cadre de la constitution d'une preuve numérique sont relativement dépendantes des missions des experts* »[45].

En effet, l'appréciation de la preuve numérique requiert, dans la majorité des cas, des compétences techniques spécialisées dépassant les compétences juridiques classiques. Dans ce cadre, le recours à l'expertise technique s'impose comme un outil permettant au juge d'apprécier la valeur probante de la preuve. L'art. 194 du CPP prévoit que le juge d'instruction, ainsi que le juge de fond peuvent ordonner une expertise à chaque fois qu'ils se trouvent face à une question d'ordre technique ou scientifique.

L'expertise technique permet d'éclairer le juge sur les conditions de collecte, de conservation, d'extraction et d'analyse des données numériques qui constituent des éléments de preuve numérique. Elle permet de vérifier l'intégrité des données, l'absence de toute altération ou modification, ainsi que la fiabilité des procédés techniques utilisés. A titre d'exemple, la saisie d'un support de stockage numérique, tel qu'un disque dur, ne saurait à elle

[45] KAI (F.) ; La preuve numérique à l'épreuve de la cybercriminalité, mémoire en vue de l'obtention du Master 2 en droit pénal et européen, Université de Limoges, 2021, p. 49.

seule conférer une valeur probante aux données qu'il contient. La valeur de ce support est subordonnée à l'identification de l'environnement technique dans lequel il a été utilisé, ainsi qu'à l'établissement du lien entre le support saisi et la personne à laquelle il est susceptible d'appartenir. En outre, la valeur probante des données numériques repose de manière déterminante sur la garantie de leur intégrité qui implique la mise en place des mesures techniques assurant la protection du support contre toute altération ou modification ultérieure depuis le moment de sa saisie jusqu'à celui de son analyse par un expert qualifié[46].

En effet, en matière de preuve numérique, la mission de l'expert consiste de rendre intelligible les données numériques stockées dans un disque dur par exemple. Cela permettrait au juge de saisir concrètement la réalité de l'infraction commise[47]. À ce stade, on peut donner l'exemple d'une intrusion frauduleuse dans un système informatique, réalisée au moyen d'un programme malveillant. Dans ce cas, l'appréciation du juge va se baser largement sur la capacité de l'expert à exposer, de manière claire et concrète, le mode de fonctionnement du virus en cause et ses effets sur le système visé[48]. Ainsi, afin de s'assurer que l'expert désigné n'a rien omis dans son travail, le juge dispose de la possibilité d'ordonner une contre-expertise qui va lui permettre de vérifier l'absence de toute contradiction technique et de consolider la fiabilité des conclusions rendues.

Finalement, on peut dire que si l'expertise joue un rôle déterminant dans l'appréciation de la preuve numérique, elle ne lie pas le juge. Celui-ci conserve son pouvoir souverain d'appréciation des preuves, dans la mesure où l'expertise ne constitue qu'un élément parmi d'autres soumis à son appréciation. On peut noter également que le juge confronte les conclusions de l'expert aux autres éléments du dossier, tout en prenant en considération le respect des garanties procédurales, notamment le respect du principe du contradictoire et des droits de la défense.

2.2.Recommandations visant le renforcement du cadre relatif à la preuve numérique

Il convient à ce stade de traiter, d'une part, le point relatif au renforcement des capacités techniques et humaines (2.2.1) et, d'autre part, celui relatif au renforcement du cadre juridique en vigueur (2.2.2.).

[46] FREYSSINET (E.) ; La preuve numérique : un défi pour l'enquête criminelle du 21e siècle, La preuve numérique : un défi pour l'enquête criminelle du 21e siècle, JLE éditions, Vol. 3, 2003, p. 206. Disponible sur : https://www.researchgate.net/publication/313611223_La_preuve_numerique_Un_defi_pour_l'enquete_criminelle_du_21e_siecle

[47] KAI (F.) ; La preuve numérique à l'épreuve de la cybercriminalité, *op. cit.*, p. 49.

[48] Ibid.

2.2.1. Le renforcement des capacités techniques et humaines

L'un des principaux obstacles faisant face à une administration efficace de la preuve numérique réside dans l'insuffisance de formations spécialisées au sein de l'ensemble de la chaîne pénale. En effet, la maîtrise des enjeux techniques ne peut être réservée aux seules unités spécialisées. Elle doit concerner tous les intervenants depuis les brigades territoriales jusqu'au service d'enquêtes hautement spécialisés.

En pratique, la majorité des suspects ont recours à des outils informatiques largement répandus et à des logiciels couramment utilisés[49], allant des plateformes de communication chiffrée et des navigateurs anonymisant, aux logiciels d'intrusion et de ransomware. Or, même en l'existence d'une diversité de logiciels et de protocoles de communication qui sont susceptibles de générer des traces d'utilisation, celles-ci ne sont intelligibles que si l'enquêteur possède une connaissance approfondie du fonctionnement des systèmes d'exploitation, des applications, ainsi que des protocoles de communication sur Internet, d'où l'importance de la formation continue au profit de l'ensemble des intervenants de la chaîne pénale.

De même, la complexité atteint son niveau le plus élevé en matière de piratage informatique. L'auteur d'une infraction cherche généralement à supprimer ou dissimuler les traces numériques. Dans ce cadre, l'enquête reposerait sur une reconstitution technique fondée sur la corrélation d'indices numériques. Dans ce cadre, une fois le suspect est identifié, il conviendrait d'établir une concordance rigoureuse entre les traces relevées sur le système de la victime et celles découvertes sur le matériel du suspect. A ce niveau, le recours à des plateformes de simulation constituerait un outil pertinent pour tester les hypothèses techniques et consolider l'analyse probatoire[50].

Au-delà des enquêteurs et des experts, l'ensemble des professionnels de la justice, et en particulier les magistrats, doivent s'adapter à la transformation numérique de l'environnement judiciaire, et ce vu que l'évolution des technologies modifie non seulement la nature des infractions mais aussi les modalités d'établissement et d'appréciation de la preuve.

En effet, la formation initiale des magistrats doit intégrer une véritable culture numérique. Il ne s'agit pas de transformer le juge en technicien, mais plutôt de lui permettre de comprendre les logiques fondamentales des environnements numériques, d'identifier les enjeux techniques soulevés par un dossier et d'exercer un contrôle éclairé sur les opérations d'expertise. Il convient de souligner que le développement d'une pensée numérique implique

[49] FREYSSINET (E.) ; La preuve numérique : un défi pour l'enquête criminelle du 21e siècle, *op.cit.*, p. 215.
[50] Ibid.

la capacité à appréhender les interactions entre technique et le droit et d'intégrer ces évolutions dans le raisonnement juridictionnel[51].

Par ailleurs, la formation continue apparaît indispensable. Les innovations technologiques évoluent à un rythme soutenu, tandis que la défense peut s'appuyer sur des compétences techniques particulièrement pointues. Par conséquent, les magistrats doivent acquérir une autonomie intellectuelle suffisante pour dialoguer avec les experts, apprécier la fiabilité des méthodes utilisées et évaluer la solidité scientifique des conclusions présentées[52]. Ainsi, la désignation, au sein des juridictions, de magistrats spécialisés en matière numérique pourrait constituer une réponse institutionnelle adaptée, permettant de centraliser l'expertise et d'assurer une meilleure cohérence dans le traitement des dossiers techniques.

Finalement, s'agissant des données collectées lors des enquêtes, on doit souligner qu'elles doivent être stockées sur des supports sécurisés qui permettent la non détérioration et la protection des éléments de preuve numérique. Ainsi, afin de préserver leur intégrité, l'analyse desdits éléments ne doit jamais se réaliser sur les supports originaux mais doit plutôt porter sur des copies des fichiers afin de préserver la valeur probante des éléments de preuve et de prévenir toute contestation ultérieure quant à une éventuelle altération[53].

2.2.2. Le renforcement du cadre juridique en vigueur

Le renforcement du cadre juridique relatif à la preuve numérique constitue aujourd'hui une exigence incontournable vu, d'une part, la diversité des modes de commission des infractions et, d'autre part, la transformation technologique des techniques d'enquête.

Il convient, en premier lieu, de donner une définition claire et précise de la preuve numérique, ainsi que de préciser les différents éléments susceptibles de la constituer. Une telle définition permettrait d'établir un cadre juridique stable et harmonisé, réduisant les incertitudes lors de l'admission et de l'évaluation des preuves devant les juridictions pénales.

En effet, la preuve numérique peut prendre diverses formes, notamment emails, fichiers informatiques, logs de serveurs, données de géolocalisation, ou encore transactions électroniques. La définition de ces éléments permettrait, d'une part, de faciliter la qualification juridique de chaque type de preuve et, d'autre part, d'adopter des procédures harmonisées de leur collecte, conservation et transmission, ce qui garantirait leur intégrité et leur authenticité.

[51] CASSUTO (T.), « Objectiver la preuve grâce au numérique », Revue justice actualités, N. 1, 2019, p. 135. Disponible sur : https://droit.cairn.info/revue-justice-actualites-2019-1-page-134?lang=fr

[52] QUEMENER (M.) ; La preuve à l'ère du numérique un défi pour la justice, Justice actualités n° 21, p25.

[53] GAZAGNE (D.) ; Enquête numérique : les systèmes d'information ont de la mémoire, sécurité et stratégie, rev. des directeurs sécurité d'entreprise, n°21, 2016, p.42.

Ainsi, il convient d'harmoniser le cadre juridique national avec les standards internationaux, notamment la Convention de Butapest sur la cybercriminalité, ratifiée par l'Etat marocain en 2018[54]. Cela permettrait, en effet, de renforcer la cohérence des règles applicables à la preuve numérique et faciliterait la coopération judiciaire entre les États. De surcroît, cette harmonisation permettrait d'établir des procédures communes pour la collecte, la transmission et la protection des preuves électroniques, tout en assurant leur reconnaissance dans différents systèmes juridiques. De même, l'harmonisation contribuerait à améliorer l'efficacité des enquêtes transfrontalières et à lutter contre les formes sophistiquées de cybercriminalité.

Il convient de souligner également que le caractère transfrontalier de la preuve numérique rend sa collecte et son exploitation particulièrement complexes. En effet, les données électroniques peuvent être stockées sur des serveurs situés dans différents pays, chacun ayant sa propre législation. Cette dispersion géographique des données rend difficile l'accès direct aux preuves et peut retarder les enquêtes judiciaires, d'où vient l'importance de renforcer la coopération internationale entre les États, ainsi qu'entre les autorités judiciaires. De même, le partage d'expertise technique et de bonnes pratiques entre les pays renforce l'efficacité des enquêtes et la capacité à lutter contre des formes complexes de criminalité.

Conclusion

A l'ère du numérique, où les auteurs d'infractions ont de plus en plus recours aux technologies de l'information et de la communication pour commettre leurs actes délictueux, la preuve numérique occupe désormais une place centrale dans la recherche et l'établissement de la vérité. En effet, les traces numériques laissées par l'utilisation des systèmes informatiques et des réseaux constituent des éléments précieux permettant non seulement l'identification des auteurs des infractions mais également la reconstitution des faits et la détermination des éléments constitutifs de l'infraction.

Toutefois, la spécificité technique de ces éléments de preuve impose le recours à des méthodes rigoureuses lors de leur collecte, de leur conservation et de leur analyse et ce afin de garantir l'intégrité, la fiabilité et la valeur probante des données recueillies, tout en assurant le respect des droits et libertés fondamentaux.

[54] https://fr.le360.ma/politique/la-question-de-la-cybercriminalite-et-de-la-cybersecurite-au-maroc_JSTNHE6OJ5CUJBPPTPMU3HJHQM/ (consulté le 08/01/2026)

Bibliographie :

- ABOU EL JAOUAD (A.) ; La preuve numérique à l'épreuve de la cybercriminalité en droit marocain, rev. Droit et société, n°11, pp. 7-18, 2023.
- BENTELHI (H.) ; L'enquête pénale à l'épreuve de la cybercriminalité, Mémoire pour l'obtention d'un Master de Droit pénal et sciences criminelles, Panthéon-Assas Université Paris, 2024.
- BOOS (R.) ; La lutte contre la cybercriminalité au regard de l'action des Etats, thèse de doctorat en droit privé et sciences criminelles, Université de LORRAINE, France, 2017.
- CASSUTO (T.), « Objectiver la preuve grâce au numérique », Revue justice actualités, N. 1, 2019, pp. 134-137. Disponible sur : https://droit.cairn.info/revue-justice-actualites-2019-1-page-134?lang=fr
- DIK (A.) ; « Règles pénales procédurales relatives aux délits informatiques », Revue du droit marocain. N. 27, 2015, pp. 43-53.
- DIRAND (C.) ; Les réquisitions de données de connexion : un régime européen en construction, Mémoire pour l'obtention d'un Master droit parcours métiers du droit, Avignon Université, 2024.
- ENYEGUE (C.) ; « L'enquête pénale à l'épreuve de l'internet », Revue Internationale du chercheur, Volume 5 : Numéro 1, 2024, pp : 925-948
- FRANSSEN (V.), BERRENDORF (A.), et CORHAY (M.) ; « La collecte transfrontière de preuves numériques en matière pénale. Enjeux et perspectives européennes », RIDP, 2019. Disponible sur : https://www.penal.org/sites/default/files/Franssen%20collecte%20transfrontiere_0.pdf
- FREYSSINET (E.) ; La preuve numérique : un défi pour l'enquête criminelle du 21e siècle, JLE éditions, Vol. 3, 2003, pp. 205-217. Disponible sur : https://www.researchgate.net/publication/313611223_La_preuve_numerique_Un_defi_pour_l'enquete_criminelle_du_21e_siecle
- GAZAGNE (D.) ; Enquête numérique : les systèmes d'information ont de la mémoire, sécurité et stratégie, rev. des directeurs sécurité d'entreprise, n°21, 2016.
- Guinchard (S.) et Buisson (J.), Procédure Pénale, édition LexisNexis, 8ème édition, 2012.
- JELDA (H.) et ECHCHARYF (H.) ; « Les conditions de recevabilité de la preuve numérique », Revue Marocaine des Eudes Juridiques et Economiques, Numéro 14, Mars, 2025.

- KAI (F.) ; La preuve numérique à l'épreuve de la cybercriminalité, mémoire en vue de l'obtention du Master 2 en droit pénal et européen, Université de Limoges, 2021.
- QUEMENER (M.) ; La preuve à l'ère du numérique un défi pour la justice, Justice actualités n° 21, pp. 23-25.
- QUEMENER (M.), DALLE (F.) et WIERRE (C.) ; Quels droits face aux innovations numériques ? Gualino, Paris, 2020.
- UNODC, Étude détaillée sur la cybercriminalité, New York, 2013.
- طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، مجلة الحقوق، المجلد 12، العدد 1، ص. 40-73.
- عبد الرزاق رفيق، جرائم النصب والاحتيال عبر الانترنيت. دراسة مقارنة، الطبعة الأولى، مكتبة الرشاد سطات، 2019، المغرب.
- خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، دار الفكر الجامعي، 2020 ، مصر.

Webographie :

- https://www.netapp.com/fr/data-storage/what-is-data-storage/ (consulté le 17/12/2025)
- https://www.dropbox.com/fr_CA/resources/storage-devices (consulté le 17/12/2025)
- https://www.ibm.com/fr-fr/think/topics/network-attached-storage (consulté le 17/12/2025)
- https://www.dovit.com/blog/systeme-domotique-qu-est-ce-que-c-est-et-comment-ca-fonctionne/ (consulté le 18/12/2025)
- https://www.kaspersky.fr/resource-center/threats/deep-web (consulté le 19/12/2025)
- https://www.magnetforensics.com/fr/resources/outils-modernes-de-criminalistique-numerique-decouvrez-comment-de-nouveaux-outils-eliminent-le-bruit-pour-trouver-des-preuves/ (consulté le 28/12/2025)
- https://en.wikipedia.org/wiki/Forensic_Toolkit (consulté le 28/12/2025)
- https://fr.le360.ma/politique/la-question-de-la-cybercriminalite-et-de-la-cybersecurite-au-maroc_JSTNHE6OJ5CUJBPPTPMU3HJHQM/ (consulté le 08/01/2026)