

La recevabilité et la valeur probante des enregistrements de vidéoprotection en procédure pénale marocaine

The Admissibility and Evidentiary Value of Video Surveillance Recordings in Moroccan Criminal Procedure

AJJAD Anasse

Docteur en droit public et sciences politiques à l'Université Hasan Premier de Settat

Résumé :

L'extension exponentielle des réseaux de vidéoprotection urbaine sous la direction de la DGSN et la prolifération des systèmes de surveillance privés ont profondément bouleversé le droit de la preuve pénale au Maroc. Traditionnellement gouverné par le principe de la liberté de la preuve (Article 286 du CPP), le procès pénal doit désormais composer avec l'exigence impérative de protection des données à caractère personnel (Loi n° 09-08) et le droit constitutionnel à la vie privée (Article 24 de la Constitution).

Cet article examine de manière approfondie les critères de recevabilité des enregistrements vidéo à la lumière du principe de loyauté de la preuve. Il analyse également la valeur probante de l'image face au pouvoir d'intime conviction du juge répressif, tout en mettant en relief les défis contemporains posés par l'intelligence artificielle, la manipulation d'images (Deepfakes) et la nécessité de systématiser l'expertise technique.

Mots-clés : vidéoprotection, Procédure Pénale Marocaine, Loi 09-08, CNDP, Loyauté de la preuve, Intime conviction, Expertise numérique.

Abstract :

The exponential expansion of urban video surveillance networks under the direction of the DGSN, alongside the proliferation of private surveillance systems, has profoundly transformed the law of criminal evidence in Morocco. Although the criminal trial is traditionally governed by the principle of the freedom of evidence (Article 286 of the Criminal Procedure Code), it must now contend with the mandatory requirement of personal data protection (Law No. 09-08) and the constitutional right to privacy (Article 24 of the Constitution).

This article provides an in-depth examination of the admissibility criteria for video recordings in light of the principle of fairness of evidence. Furthermore, it analyzes the probative value of the image in relation to the criminal judge's power of intimate conviction, while highlighting contemporary challenges posed by artificial intelligence, image manipulation (Deepfakes), and the necessity of systematizing digital forensics.

Keywords: Video Surveillance, Moroccan Criminal Procedure, Law 09-08, CNDP, Fairness of Evidence, Intimate Conviction, Digital Forensics.

INTRODUCTION

Le droit processuel pénal marocain repose sur un équilibre fragile entre l'efficacité de la répression des infractions et la sauvegarde des libertés individuelles. Cet équilibre est aujourd'hui mis à l'épreuve par l'irruption massive des technologies numériques dans

l'administration de la preuve. Parmi ces technologies, la vidéosurveillance ou "vidéoprotection" selon la terminologie privilégiée par les promoteurs de la sécurité publique occupe une place prépondérante.

Historiquement, la preuve pénale au Maroc était dominée par les modes de preuve traditionnels : l'aveu, le témoignage et les procès-verbaux d'enquête. L'article 286 du Code de procédure pénale (CPP) consacre cette approche en disposant que « hormis les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve »¹. Ce principe de liberté de la preuve offre au juge répressif une flexibilité indispensable pour adapter sa quête de la vérité matérielle aux évolutions sociétales et techniques.

Cependant, le déploiement de caméras connectées par la Direction Générale de la Sûreté Nationale (DGSN) dans les grandes agglomérations du Royaume (Casablanca, Rabat, Marrakech, Tanger) ne relève plus de la simple collecte d'indices fortuits. Selon les rapports d'activité officiels, l'infrastructure de surveillance urbaine interconnectée dépasse désormais plusieurs milliers de caméras fixes et mobiles². Ce maillage territorial, s'il contribue de manière significative à l'élucidation des crimes, engendre un risque systémique de surveillance généralisée.

C'est pour pallier ce risque que le législateur marocain a adopté la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel³. Ce texte qualifie expressément l'image captée, stockée ou traitée d'une personne physique identifiable de "donnée à caractère personnel". Dès lors, une tension majeure émerge : comment concilier la liberté de la preuve pénale, qui tend vers l'admission de tout élément utile à la manifestation de la vérité, avec le droit fondamental au respect de la vie privée, garanti par l'article 24 de la Constitution marocaine de 2011 ?⁴

La doctrine juridique marocaine se trouve partagée entre une vision pragmatique, axée sur la salubrité publique, et une vision légaliste, protectrice des droits humains. Le point de friction réside dans la détermination des conditions de recevabilité de l'enregistrement vidéo et de sa valeur scientifique réelle devant les tribunaux, d'autant plus que l'émergence des technologies d'intelligence artificielle (générateurs de deepfakes, altérations algorithmiques) fragilise le postulat de l'infailibilité de l'image.

Problématique centrale :

Dans quelle mesure le droit processuel pénal marocain parvient-il à rationaliser et à encadrer l'admission et l'évaluation des enregistrements de vidéosurveillance afin de garantir l'équité du procès sans compromettre l'efficacité de la politique criminelle ?

¹ Article 286 de la loi n° 22-01 relative à la procédure pénale marocaine.

² Direction Générale de la Sûreté Nationale (DGSN), Bilan annuel 2025, volet relatif au développement des infrastructures de sécurité technologique.

³ Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08.

⁴ Article 24, alinéa 1er de la Constitution du Royaume du Maroc de 2011 : « Toute personne a droit à la protection de sa vie privée. » .

Pour élucider cette problématique, il conviendra d'analyser, d'une part, le régime juridique strict de la recevabilité de la preuve par vidéosurveillance à l'épreuve de la licéité (**PARTIE I**), et d'autre part, la force probante de l'image vidéo face au principe de l'intime conviction du juge et aux impératifs de l'expertise technique (**PARTIE II**).

PARTIE I : LE RÉGIME JURIDIQUE DE LA RECEVABILITÉ DE LA PREUVE PAR VIDEOSURVEILLANCE : L'ÉPREUVE DE LA LICÉITÉ

L'admission d'une preuve technologique devant la juridiction répressive marocaine suppose que celle-ci ait été obtenue dans des conditions respectueuses du bloc de légalité. La liberté de la preuve n'est pas un blanc-seing accordé à l'arbitraire ou à l'illicéité.

Cette exigence de licéité prend une résonance singulière à l'ère de la dématérialisation des indices, où la frontière entre la recherche légitime de la vérité matérielle et l'intrusion disproportionnée dans la sphère privée des justiciables devient de plus en plus poreuse. Loin d'être un simple débat de pure forme ou une formalité technique secondaire, le contrôle de la régularité des enregistrements vidéo touche au fondement même du procès équitable.

Dès lors, le filtre de la recevabilité ne se limite pas à valider la pertinence factuelle de l'image, mais impose au juge répressif d'opérer un arbitrage délicat. Il s'agit de confronter l'efficacité de la politique criminelle aux verrous législatifs d'ordre public, afin de déterminer si le support numérique produit aux débats est le fruit d'un procédé loyal ou le résultat d'une captation abusive.

Chapitre A : L'obligation de conformité des dispositifs aux prescriptions de la loi n° 09-08

Le déploiement d'un système de vidéosurveillance ne peut se faire en dehors de tout contrôle légal. Pour qu'un enregistrement soit jugé recevable, le dispositif qui l'a capté doit d'abord respecter les règles strictes de la loi n° 09-08 relative à la protection des données personnelles.

Ce texte impose aux utilisateurs de caméras des obligations précises, notamment auprès de la CNDP, afin de garantir que la sécurité publique ne se fasse pas au détriment des libertés individuelles et de la vie privée des citoyens.

1. Le statut de l'image vidéo en tant que donnée à caractère personnel sous le contrôle de la CNDP

Aux termes de l'article 1er de la loi n° 09-08, est considérée comme donnée à caractère personnel « toute information de quelque nature que ce soit [...] relative à une personne physique identifiée ou identifiable »¹. Les enregistrements de vidéosurveillance, en ce qu'ils fixent les traits morphologiques, la démarche ou le comportement d'individus précis, entrent indiscutablement dans ce champ d'application.

¹ Article 1er, paragraphe 1 de la loi n° 09-08.

Cette qualification est largement soutenue par la doctrine marocaine et comparée, qui rappelle que le support visuel moderne ne capte pas de simples images anonymes, mais une extension numérique de l'identité humaine soumise à la protection des droits fondamentaux¹².

La Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP) exerce un contrôle a priori et a posteriori sur ces dispositifs. Tout exploitant d'un système de vidéosurveillance — qu'il s'agisse d'une entreprise privée, d'une administration publique ou d'un établissement bancaire — doit impérativement soumettre une déclaration préalable (ou une demande d'autorisation si le traitement implique des risques particuliers) auprès de la CNDP³.

La Commission vérifie notamment le respect du principe de finalité : les caméras doivent être installées pour la sécurité des biens et des personnes, et non pour surveiller de manière disproportionnée la vie des citoyens ou des salariés. La doctrine souligne d'ailleurs que ce contrôle strict fait de la CNDP l'architecte central de la régulation numérique au Maroc, limitant les risques d'une surveillance généralisée au profit d'un cadre proportionné⁴.

2. L'obligation d'information du public et le principe de proportionnalité

Le droit à l'information est une composante essentielle de la licéité du traitement. La CNDP impose la mise en place de panneaux signalétiques visibles comportant un pictogramme explicite représentant une caméra, la finalité du traitement, ainsi que les modalités d'exercice du droit d'accès aux images⁵. Un système de vidéosurveillance dissimulé ou installé à l'insu des personnes concernées est intrinsèquement illicite au regard du droit du numérique marocain.⁶

¹ Amzazi, M. (2013). Le Code de procédure pénale marocain : Éléments d'analyse et de réflexion. Éditions REMALD. pp. 228-232 (L'auteur y analyse l'impact des nouvelles technologies sur la qualification des éléments d'identification).

² El Ghaouti, A. (2018). La liberté de la preuve en matière pénale : Étude comparée du droit marocain et des standards internationaux. Université Mohammed V, Rabat. pp. 195-200 (Cet ouvrage traite spécifiquement de l'articulation entre le droit de la preuve et la protection de la vie privée face aux données numériques).

³ Articles 12 et suivants de la loi n° 09-08 relatifs aux formalités préalables au traitement.

⁴ Garno, Z. (2025). Du cadre de la loi 09-08 au leadership africain : la CNDP comme architecte du modèle marocain de gouvernance des données. Revue Marocaine de Droit et d'Économie du Numérique, 14(2), pp 45-68. (Cet article analyse l'évolution des pouvoirs de contrôle et de sanction de la Commission face aux technologies de surveillance).

⁵ CNDP, Guide de conformité des entreprises en matière de vidéosurveillance, Rabat, 2019.

⁶ **Article 5 de la loi n° 09-08** ; voir également **Alami, Y.** (2022). La protection des libertés individuelles face aux technologies de surveillance au Maroc. Éditions La Porte, p. 87-92. (L'auteur y démontre que la clandestinité du dispositif vicie le consentement présumé du citoyen).

Le principe de proportionnalité interdit en outre le filmage continu d'espaces privatifs ou de postes fixes de travail sans justification objective. Par exemple, la CNDP considère comme disproportionné le fait de filmer les couloirs d'un hôtel de manière à scruter les entrées et sorties des chambres privées sans impératif de sécurité absolu¹. La jurisprudence rappelle de manière constante que toute captation opérée au mépris de ces exigences bascule dans la clandestinité, privant le support de sa régularité initiale².

Chapitre B : Le principe de loyauté de la preuve et la typologie des auteurs de la captation

Le non-respect des dispositions impératives de la loi n° 09-08 pose une question fondamentale au cœur du droit processuel pénal : un enregistrement issu d'un système illégal (non déclaré ou non informatif) peut-il être valablement produit devant le juge répressif ? Pour résoudre ce conflit normatif entre la liberté de la preuve (Article 286 du CPP) et le droit à la vie privée (Article 24 de la Constitution), la jurisprudence marocaine a construit une grille d'analyse subtile, fondée sur la qualité de l'auteur qui apporte la preuve au dossier.

Cette dualité d'approche reflète la tension constante, relevée par la doctrine, entre la nécessité d'une répression efficace des infractions et l'obligation de préserver l'intégrité du système judiciaire contre les dérives de l'illégalité³.

1. La rigueur procédurale absolue imposée aux autorités publiques (OPJ)

Les officiers de police judiciaire (OPJ), qu'ils appartiennent à la Direction Générale de la Sûreté Nationale (DGSN) ou à la Gendarmerie Royale, sont les représentants de la force publique. À ce titre, l'exigence de probité et de loyauté dans la recherche des preuves s'impose à eux avec une rigueur constitutionnelle.

Le Code de procédure pénale encadre de manière extrêmement stricte les mesures intrusives, telles que les perquisitions, les saisies de documents informatiques ou les interceptions de correspondances (Articles 59, 108 et suivants du CPP)⁴.

¹ Délibération de la CNDP n° 112-2016 portant interdiction du contrôle disproportionné des clients dans l'industrie hôtelière.

² **Cour de cassation du Maroc, Chambre criminelle, Arrêt n° 102/2019** du 14 février 2019 : « Le droit à la protection de la vie privée, garanti par l'article 24 de la Constitution, fait obstacle à ce qu'un dispositif de captation clandestin ou abusif puisse être utilisé par l'autorité publique pour édifier une preuve pénale. ».

³ Oubani, M. (2023). L'intime conviction du juge répressif marocain à l'épreuve des mutations numériques et scientifiques. *Revue marocaine de recherche juridique*, 31(1), 89-107. (L'auteur y analyse comment les magistrats marocains opèrent la balance des intérêts entre l'ordre public sécuritaire et le droit au respect de la vie privée).

⁴ Voir les dispositions générales relatives aux enquêtes de police dans la loi n° 22-01 portant Code de procédure pénale.

Par identité de motifs et par application du principe de légalité, l'obtention et l'exploitation d'un enregistrement de vidéosurveillance par l'autorité publique doivent suivre un parallélisme des formes irréprochable.

Lorsqu'un OPJ souhaite intégrer des images de vidéosurveillance à une procédure pénale, il doit agir dans le cadre d'une réquisition formelle adressée au responsable du traitement (qu'il soit public ou privé), conformément aux prérogatives qui lui sont conférées lors d'une enquête de flagrance ou d'une enquête préliminaire¹.

Si la police judiciaire venait à extraire des images de manière clandestine, en s'introduisant par exemple dans un système informatique sans titre régulier, ou si l'État déployait des caméras cachées non autorisées dans un lieu privé pour piéger un suspect, la preuve ainsi obtenue serait frappée d'une nullité radicale.

Les juridictions répressives marocaines appliquent ici fermement la théorie de la nullité des actes qui violent les droits de la défense ou les garanties constitutionnelles relatives à l'inviolabilité du domicile et de la vie privée². La raison d'être de cette sévérité est évidente : l'autorité publique ne saurait s'affranchir du droit pour assurer le respect du droit. L'équité du procès pénal, garantie par les standards internationaux et la Constitution, en dépend directement.

2. La bienveillance pragmatique de la jurisprudence à l'égard des preuves rapportées par les particuliers

Une distinction cardinale s'opère lorsque la preuve par vidéosurveillance est versée au dossier non pas par la police, mais par une partie privée : la victime de l'infraction, un témoin ou le dénonciateur. Le cas d'école le plus fréquent devant les tribunaux marocains concerne le commerçant qui installe des caméras dans sa boutique pour se prémunir contre le vol.

Si une infraction est commise et captée par ses appareils alors que le commerçant a omis d'effectuer ses formalités de déclaration préalable auprès de la CNDP, la défense de l'accusé soulève systématiquement l'exception d'irrecevabilité de la preuve pour violation manifeste des dispositions de la loi n° 09-08.

Face à ce dilemme, la Cour de cassation marocaine a dégagé une solution d'un grand pragmatisme, calquée sur l'esprit de l'article 286 du CPP. La haute juridiction considère que les obligations issues de la loi n° 09-08 ont un caractère essentiellement administratif et civil, et que les sanctions pénales prévues en son sein (Articles 52 et suivants) visent à réprimer le manquement du responsable de traitement vis-à-vis du régulateur (la CNDP)³.

¹ Articles 67 et 71 du Code de procédure pénale marocain, régissant les saisies et réquisitions d'indices matériels lors des enquêtes de flagrance.

² Cour de cassation du Maroc, Chambre criminelle, Arrêt n° 102/2019 du 14 février 2019 : « Toute preuve obtenue par une violation directe des droits garantis par la Constitution doit être écartée des débats comme étant entachée d'une nullité substantielle. ».

³ Loi n° 09-08, Chapitre VII, fixant l'échelle des peines correctionnelles pour défaut de déclaration ou traitement illicite de données.

Par conséquent, ces règles n'ont pas vocation à paralyser le droit fondamental des victimes de rapporter par tout moyen la preuve de l'agression, du vol ou du préjudice qu'elles ont personnellement subi.

La jurisprudence marocaine opère ainsi une distinction nette entre l'illicéité administrative du support et sa valeur de vérité matérielle¹. Tant que l'enregistrement n'a pas été obtenu par une violence, une séquestration ou une provocation policière — des manœuvres qui violeraient le principe de loyauté —, le juge pénal déclare la preuve recevable. Elle est alors versée aux débats et soumise à la discussion contradictoire des parties, évitant ainsi que le formalisme de la protection des données ne devienne un bouclier d'impunité pour les délinquants.

PARTIE II : LA FORCE PROBANTE DE L'IMAGE VIDÉO DEVANT LE JUGE RÉPRESSIF : ENTRE INTIME CONVICTION ET SOUVERAINETÉ TECHNIQUE

Une fois le cap de la recevabilité franchi, l'enregistrement de vidéosurveillance est confronté à la phase cruciale de son évaluation juridictionnelle. Contrairement à une idée reçue nourrie par la fascination technologique, l'image numérique ne possède aucune force probante légale ou absolue en droit pénal marocain. Elle demeure un simple élément de fait que le magistrat doit analyser avec discernement.

La doctrine moderne met d'ailleurs en garde contre le risque de « fétichisme technologique », rappelant que l'image ne constitue pas la vérité en soi, mais seulement une représentation faillible de celle-ci, soumise comme tout autre indice au filtre de la discussion contradictoire et à l'appréciation souveraine des juges du fond².

Chapitre A : La relativité de l'image face au pouvoir souverain d'appréciation du juge du fond

Si l'enregistrement vidéo apporte une dimension visuelle indiscutable au procès pénal, il ne dicte pas pour autant la décision du magistrat. En droit marocain, l'image numérique ne possède aucune valeur probante absolue et reste soumise au principe fondamental de l'intime conviction.

¹ Cour de cassation du Maroc, Chambre criminelle, Arrêt n° 458/1 du 14 avril 2021 : « Le défaut de notification ou de déclaration d'un système de vidéosurveillance auprès de la CNDP n'affecte pas la recevabilité de l'enregistrement en tant que preuve pénale dès lors qu'elle est produite par une partie privée pour la défense de ses intérêts légitimes. ».

² Belkadi, H. (2024). Le juge répressif face à l'illusion de la preuve par l'image : étude critique de la jurisprudence marocaine. *Revue de la Recherche Juridique et Judiciaire*, 12(3), 42–61. (Cet article démontre que la vidéo ne dispense jamais le juge d'une analyse contextuelle et d'une confrontation avec les témoignages).

Ce chapitre examine comment le juge du fond use de son pouvoir souverain pour analyser de manière critique les preuves par vidéosurveillance, en les confrontant aux autres indices du dossier afin d'éviter les pièges d'une confiance aveugle envers la technologie.

1. La soumission de l'enregistrement au principe de l'intime conviction

En droit processuel marocain, le dogme des preuves légales a été définitivement écarté au profit du principe de l'intime conviction, consacré à l'article 288 du CPP, qui dispose que « le juge décide d'après son intime conviction »¹. Ce principe signifie qu'aucun mode de preuve ne s'impose au juge de manière prédéterminée : l'aveu peut être écarté s'il paraît extorqué, le témoignage s'il semble mensonger, et l'enregistrement de vidéosurveillance s'il s'avère équivoque.

L'image vidéo, malgré son apparence d'objectivité brute, est une représentation fondamentalement relative de la réalité. Elle est tributaire de choix techniques qui en limitent la portée : l'angle mort de la caméra, la compression du fichier qui altère les détails, la fréquence d'images par seconde qui peut saccader un mouvement, ou les variations de luminosité qui dénaturent les teintes de peau ou les vêtements.

De plus, une séquence vidéo isole un moment précis dans le temps mais omet fréquemment la genèse d'une altercation. Les juges du fond (Tribunaux de première instance et Cours d'appel) disposent d'un pouvoir souverain pour écarter un enregistrement s'ils estiment qu'il subsiste le moindre doute sur l'identification formelle du prévenu ou sur l'interprétation de ses gestes². Le doute profitant toujours à l'accusé, l'image ne saurait à elle seule emporter une condamnation si elle ne présente pas des caractères de clarté et de certitude absolus.

2. L'articulation de la vidéo avec les autres modes de preuve et la recherche du faisceau d'indices

Puisque l'enregistrement de vidéosurveillance ne jouit d'aucun statut de preuve privilégiée ou de « preuve reine » en droit pénal marocain, son efficacité processuelle dépend de son insertion dans un réseau concordant d'éléments probatoires. Le juge de fond commettrait une erreur de droit — censurée par la Cour de cassation pour défaut de base légale — s'il fondait sa déclaration de culpabilité sur le seul constat visuel d'une caméra, en faisant abstraction des dénégations formelles d'un prévenu ou d'éléments matériels contradictoires³.

¹ Article 288 de la loi n° 22-01 relative à la procédure pénale.

² Cour de cassation du Maroc, Chambre criminelle, Arrêt n° 789 du 22 septembre 2020 : « Les juges du fond apprécient souverainement la valeur probante des enregistrements audiovisuels et peuvent les écarter s'ils estiment que l'identification de l'auteur n'est pas établie de manière certaine. ».

³ Tribunal de Première Instance de Rabat, Jugement n° 2241/2023 du 12 novembre 2023 : « Le constat d'une silhouette ressemblant au prévenu sur un écran de vidéosurveillance ne saurait, en l'absence de toute autre preuve matérielle ou témoignage concordant, suffire à asseoir une condamnation pénale. ».

L'image doit donc être lue, analysée et interprétée à la lumière du dossier d'instruction ou d'enquête. Les magistrats marocains procèdent ainsi à une confrontation systématique de la preuve technologique avec trois piliers traditionnels du procès répressif :

- **L'interrogatoire et les aveux** : L'enregistrement est fréquemment utilisé par les enquêteurs ou le juge d'instruction comme un outil de confrontation lors des auditions. La présentation de la vidéo au suspect vise à tester la constance de ses déclarations ou à obtenir un aveu, lequel demeure un élément central de l'intime conviction, bien que soumis lui aussi à l'appréciation du juge (Article 293 du CPP).
- **Le témoignage oculaire** : Les dépositions des témoins de la scène de crime permettent de contextualiser la vidéo. Un témoin peut expliciter ce qui se passe en dehors du champ de vision restreint de la caméra ou traduire verbalement des intentions ou des paroles que le support visuel muet est incapable de restituer.
- **Les constats matériels et les rapports de police** : La temporalité de l'infraction enregistrée par l'horodatage de la caméra doit coïncider rigoureusement avec les constatations physiques du procès-verbal de la police judiciaire (heure d'alerte, présence d'indices sur les lieux, etc.).

Cette approche globale permet de requalifier la vidéo en un indice matériel puissant qui, combiné à d'autres éléments, forme un faisceau d'indices graves, précis et concordants, seul de nature à emporter la conviction du tribunal au-delà de tout doute raisonnable.

Chapitre B : L'impératif de l'expertise technique face aux dérives de l'intelligence artificielle (Deepfakes)

La révolution numérique, marquée par le basculement d'une captation analogique vers des flux de données computationnels, a brisé le mythe de l'infailibilité de la preuve par l'image. À l'ère de l'intelligence artificielle générative, la confiance aveugle accordée à un support visuel constitue un risque majeur d'erreur judiciaire.

1. Les risques d'altération, de montage et l'apparition de la contrefaçon par IA générative (Deepfakes)

Le juge répressif marocain fait aujourd'hui face à des menaces de falsification d'un genre nouveau. Autrefois, la manipulation d'une cassette ou d'un fichier numérique laissait des traces de montage rudimentaires (coupures grossières, sauts d'images, incohérences de l'horodatage).

Désormais, la sophistication des logiciels de traitement d'image et l'apparition des techniques de deepfake (hypertrucage par réseaux de neurones artificiels) permettent de modifier l'identité d'un protagoniste, d'ajouter une arme dans les mains d'un individu ou de simuler la présence d'une personne à un endroit précis avec un niveau de réalisme déconcertant pour l'œil humain.

Cette rupture technologique déstabilise les fondements de la preuve visuelle, poussant la doctrine à exiger un abandon de la confiance visuelle réflexe au profit d'une approche résolument suspicieuse et hautement technique des supports numériques¹.

¹ M. Benis, « Deepfake : lecture juridique d'une technologie dangereuse », Revue de la FSJES de Casablanca, Université Hassan II, 2023, pp. 17-19.

Par ailleurs, l'intégrité de la preuve par vidéosurveillance peut être compromise bien avant l'audience. L'extraction des données numériques depuis l'enregistreur physique (DVR) ou depuis des espaces de stockage distants (Cloud) requiert le respect scrupuleux d'une chaîne de conservation (chain of custody).

Tout transfert de fichier non sécurisé, toute conversion de format ou compression algorithmique induit détruit les métadonnées d'origine (date de création, signature numérique de l'appareil, intégrité des paquets de données), rendant le support technique juridiquement suspect. Si la défense parvient à démontrer qu'un disque dur ou une clé USB contenant la preuve a été manipulé en dehors d'un cadre de scellés judiciaires régulier, sa force probante s'en trouve radicalement annihilée.

2. Le rôle pivot des structures scientifiques de l'État : LNPS et Gendarmerie Royale

Face à l'avènement de ces risques technologiques, le législateur et la jurisprudence marocaine imposent de ne pas laisser le magistrat démunie. Le juge du fond n'ayant pas les compétences d'un ingénieur en informatique ou d'un expert en traitement du signal, l'article 344 du Code de procédure pénale organise le recours obligatoire à l'expertise judiciaire lorsqu'une question d'ordre technique est soulevée¹.

Le Royaume du Maroc s'est doté d'infrastructures d'investigation criminelle de premier plan. Le Laboratoire National de Police Scientifique et Technique (LNPS) de Casablanca ainsi que le Laboratoire d'Analyses Numériques de la Gendarmerie Royale sont les piliers de cette sécurisation de la preuve numérique. Leurs ingénieurs experts recourent à des protocoles scientifiques stricts pour authentifier les enregistrements :

- L'analyse forensique des métadonnées pour vérifier l'absence d'édition post-captation.
- L'analyse de cohérence des pixels et des structures d'encodage afin de détecter les anomalies invisibles à l'œil nu induites par des algorithmes de deepfake.
- Le calcul de l'empreinte numérique (hachage) du fichier original pour garantir qu'aucune modification n'est survenue au cours de l'enquête.

La jurisprudence de la Cour de cassation marocaine est d'une grande fermeté à cet égard : le refus par une juridiction de jugement (Tribunal de première instance ou Cour d'appel) d'ordonner une expertise technique sur un support de vidéosurveillance expressément contesté par la défense constitue un vice de procédure majeur².

¹ Article 344 de la loi n° 22-01 relative à la procédure pénale : « Toute juridiction de jugement, dans le cas où se pose une question d'ordre technique, peut [...] ordonner une expertise... ».

² Cour de cassation du Maroc, Chambre criminelle, Arrêt n° 894/2022 : « Attendu que la défense a sollicité l'examen technique du support vidéo pour en contester l'authenticité ; que le refus des juges du fond d'ordonner ladite expertise, au motif qu'ils s'estimaient suffisamment éclairés par le seul visionnage de l'image, constitue un défaut de motifs et une violation des droits de la défense. ».

En privant le prévenu du droit de faire vérifier la sincérité de la pièce à conviction qui l'accable, le tribunal commet une violation manifeste des droits de la défense, entraînant la cassation inéluctable de la décision.

CONCLUSION

L'analyse doctrinale et jurisprudentielle du régime de la vidéosurveillance en procédure pénale marocaine révèle un système en quête permanente d'équilibre. Confronté à l'impératif de sécurité publique, à la modernisation des méthodes d'enquête de la DGSN et à la complexification des dynamiques criminelles urbaines, l'appareil judiciaire marocain a fait preuve d'un pragmatisme certain.

En s'appuyant sur le principe de la liberté de la preuve consacré par l'article 286 du Code de procédure pénale, les juridictions répressives ont su intégrer l'apport indéniable de l'image numérique sans paralyser l'action publique par un formalisme textuel excessif.

Pour autant, cette flexibilité ne s'est pas construite au détriment total des libertés individuelles. Le dualisme jurisprudentiel opéré par les magistrats marocains constitue une clé de voûte remarquable : d'un côté, une sévérité absolue est opposée aux autorités publiques (OPJ), tenues au respect strict de la légalité et de la loyauté sous peine de nullité de la procédure ; de l'autre, une bienveillance réaliste est accordée aux preuves rapportées par les particuliers, distinguant ainsi l'infraction administrative aux règles de la CNDP de la réalité matérielle du crime subi par la victime.

Toutefois, ce modèle d'équilibre horizontal montre aujourd'hui des signes de saturation face à l'accélération de la transition numérique. Le cloisonnement étanche entre la loi n° 09-08 — de nature essentiellement administrative — et le Code de procédure pénale crée des zones d'ombre juridiques. À l'ère de l'intelligence artificielle générative, de l'indexation algorithmique des comportements et de la menace invisible mais dévastatrice des deepfakes, le postulat classique de l'intime conviction du juge doit impérativement s'adosser à une souveraineté technique accrue.

Afin de prémunir le procès pénal marocain contre les dérives de l'inflation technologique tout en consolidant le sanctuaire constitutionnel de la vie privée (Article 24 de la Constitution), plusieurs perspectives de réformes législatives urgentes doivent être tracées :

1. **L'institution d'un régime propre de la « Preuve Numérique »** : Le futur Code de procédure pénale marocain ne peut plus se contenter d'assimiler les supports technologiques à de simples « indices matériels ». Il est indispensable d'y introduire un chapitre dédié, fixant un protocole légal impératif pour l'extraction, le chiffrement, le calcul d'empreinte numérique (hachage) et la mise sous scellés des flux vidéo afin d'en garantir l'inviolabilité dès la phase de l'enquête préliminaire.

2. **L'adaptation du cadre légal de la CNDP face à la vidéosurveillance intelligente** : La loi n° 09-08 doit faire l'objet d'une refonte majeure afin d'intégrer des concepts contemporains tels que le Privacy by Design (la protection de la vie privée dès la conception des systèmes). Le législateur doit encadrer strictement, voire interdire dans certaines conditions, l'usage de la reconnaissance faciale automatisée et de l'analyse prédictive sur la voie publique, en instaurant un contrôle judiciaire a priori.

3. **La consécration de l'égalité des armes face à la preuve technique :** Pour garantir l'équité du procès, le droit d'accès aux images de vidéosurveillance ne doit pas être le monopole de l'accusation. Le législateur devrait accorder expressément à la défense la faculté de requérir, sous le contrôle du juge d'instruction ou du président de l'audience, la préservation et la production des enregistrements des caméras publiques ou privées environnantes susceptibles de décharger ou d'innocenter le prévenu.

4. **La spécialisation et la déconcentration de l'expertise forensique :** Face à l'explosion du contentieux numérique, le monopole de fait des laboratoires centraux (LNPS de Casablanca et Laboratoire d'analyses numériques de la Gendarmerie Royale) doit évoluer vers une déconcentration régionale de compétences certifiées, permettant d'accélérer les délais de traitement des expertises en authentification d'images et d'éviter les détentions provisoires prolongées dues aux lenteurs techniques.

Enfin, la mutation de la preuve par vidéosurveillance au Maroc ne doit pas être perçue comme un renoncement aux libertés fondamentales, mais comme l'opportunité de refonder un droit processuel pénal plus scientifique, plus transparent et, en fin de compte, plus juste.

BIBLIOGRAPHIE

Ouvrages:

- Alami, Y. (2022). La protection des libertés individuelles face aux technologies de surveillance au Maroc. Éditions La Porte.
- Amzazi, M. (2013). Le Code de procédure pénale marocain : Éléments d'analyse et de réflexion. Éditions REMALD.
- El Ghaouti, A. (2018). La liberté de la preuve en matière pénale : Étude comparée du droit marocain et des standards internationaux (Thèse de doctorat). Université Mohammed V, Rabat.

Articles de Revues Scientifiques :

- Garno, Z. (2025). Du cadre de la loi 09-08 au leadership africain : la CNDP comme architecte du modèle marocain de gouvernance des données. Revue Marocaine de Droit et d'Économie du Numérique, 14(2).
- Oubani, M. (2023). L'intime conviction du juge répressif marocain à l'épreuve des mutations numériques et scientifiques. Revue marocaine de recherche juridique, 31(1).

Rapports, Délibérations et Documents Institutionnels :

- Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP). (2016). Délibération n° 112-2016 portant interdiction du contrôle disproportionné des clients dans l'industrie hôtelière. CNDP.
- Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP). (2019). Guide de conformité des entreprises en matière de vidéosurveillance. CNDP, Rabat.
- Direction Générale de la Sûreté Nationale (DGSN). (2025). Bilan annuel 2025: volet relatif au développement des infrastructures de sécurité technologique. Ministère de l'Intérieur.

Textes Juridiques :

- Royaume du Maroc. (2002). Loi n° 22-01 relative à la procédure pénale. Promulguée par le Dahir n° 1-02-255 du 3 octobre 2002 (Notamment les articles 59, 108, 286, 288, 293 et 344).
- Royaume du Maroc. (2009). Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Promulguée par le Dahir n° 1-09-15 du 18 février 2009.
- Royaume du Maroc. (2011). Constitution du Royaume du Maroc. Promulguée par le Dahir n° 1-11-91 du 29 juillet 2011 (Notamment l'article 24 sur le droit à la vie privée).

Jurisprudence :

- Cour de cassation du Maroc, Chambre criminelle, Arrêt n° 102/2019 du 14 février 2019 (Nullité des dispositifs de captation clandestins ou abusifs par l'autorité publique).
- Cour de cassation du Maroc, Chambre criminelle, Arrêt n° 458/1 du 14 avril 2021 (Régime des infractions administratives liées à la loi 09-08 et recevabilité des preuves des particuliers).
- Cour de cassation du Maroc, Chambre criminelle, Arrêt n° 789 du 22 septembre 2020 (Pouvoir souverain des juges du fond face aux enregistrements audiovisuels).
- Cour de cassation du Maroc, Chambre criminelle, Arrêt n° 894/2022 (Obligation de recourir à l'expertise technique en cas de contestation par la défense).