

La preuve électronique : reconnaissance juridique et difficultés probatoires en droit marocain

Electronic Evidence: Legal Recognition and Evidentiary Difficulties in Moroccan Law

Dr. Asseya ABLI

Docteur en droit

Résumé

Le passage au numérique des échanges quotidiens a ébranlé les catégories sur lesquelles reposait, depuis plus d'un siècle, le droit marocain de la preuve. En adoptant la loi n° 53-05 relative à l'échange électronique de données juridiques, puis la loi n° 43-20 relative aux services de confiance pour les transactions électroniques, le législateur a posé le principe d'une équivalence entre le document électronique et le document papier, et mis en place une échelle de signatures électroniques aux effets gradués. Cette consécration, difficilement contestable à la lecture des textes, ne se retrouve pourtant qu'imparfaitement dans les salles d'audience : le support numérique demeure fragile et fugace, l'auteur d'un message et l'intégrité de son contenu restent difficiles à établir, l'expertise technique fait défaut, les données situées à l'étranger échappent largement aux juridictions nationales, et la jurisprudence, encore jeune, avance avec précaution. La présente étude s'attache à comprendre ce fossé entre la lettre de la loi et le vécu judiciaire de la preuve électronique au Maroc, puis à esquisser les moyens de le combler, en s'appuyant notamment sur les enseignements du droit français et du droit de l'Union européenne.

Mots-clés : preuve électronique — écrit électronique — signature électronique — loi n° 53-05 — loi n° 43-20 — force probante — intégrité — expertise judiciaire — cybercriminalité — droit marocain.

Abstract

The shift of everyday exchanges to digital form has unsettled the categories on which Moroccan evidence law had rested for over a century. With Law No. 53-05 on the electronic exchange of legal data, and later Law No. 43-20 on trust services for electronic transactions, the legislature established the principle that an electronic document is equivalent to a paper one and introduced a scale of electronic signatures carrying graduated legal effects. This recognition, hard to dispute on a reading of the texts, is only imperfectly reflected in the courtroom. Digital media remain fragile and short-lived; the author of a message and the integrity of its content are difficult to establish; technical expertise is in short supply; data stored abroad largely escapes the reach of national courts; and case law, still young, proceeds with caution. This article seeks to explain the gap between the letter of the law and the judicial reality of electronic evidence in Morocco, and to outline ways of closing it, drawing in particular on the lessons of French and European Union law.

Keywords: electronic evidence — electronic writing — electronic signature — Law No. 53-05 — Law No. 43-20 — probative value — integrity — judicial expertise — cybercrime — Moroccan law.

Introduction

Pendant plus d'un siècle, prouver, c'était montrer du papier. Une lettre écrite à la main, une signature tracée par son auteur, un original rangé dans un coffre ou consigné sur un registre : l'ensemble du système probatoire issu du dahir formant code des obligations et des contrats du 12 août 1913⁵⁰⁴⁷ tenait à la matérialité du support et au geste de celui qui s'oblige. Ce monde-là s'est effacé en l'espace d'une génération. On conclut aujourd'hui ses affaires par courriel, on règle ses achats depuis un téléphone, on négocie sur une messagerie instantanée — et l'on s'investit, à l'occasion, sur les réseaux sociaux. Le contentieux a suivi ce déplacement : chaque jour, des courriels imprimés, des captures d'écran, des enregistrements, des relevés de connexion ou des fils de discussion WhatsApp atterrissent sur le bureau du juge marocain, qui doit décider de leur valeur avec les outils d'un droit de la preuve façonné pour le papier.

Le phénomène est mondial, mais il prend au Maroc un relief singulier. Le Royaume a érigé le numérique en priorité stratégique : stratégie « Maroc Digital », essor des téléservices administratifs qu'encourage la loi n° 55-19 relative à la simplification des procédures administratives⁵⁰⁴⁸, montée en puissance de la plateforme des juridictions numériques ou, plus récemment encore, accueil de procédés électroniques dans le nouveau code de procédure civile. Dans le même temps, la pratique des tribunaux trahit une réception encore mal assurée de la preuve numérique. Les parties versent aux débats des impressions de courriels dont l'authenticité est aussitôt discutée; les magistrats, privés d'expertise, peinent à jauger la fiabilité technique des pièces qui leur sont soumises; et lorsque les données décisives dorment sur des serveurs installés à l'étranger, le sentiment d'impuissance n'est jamais très loin.

Encore faut-il s'entendre sur les mots. La preuve électronique déborde largement la seule notion d'écrit électronique. Elle englobe, d'un côté, la preuve préparée à l'avance sous forme numérique — l'acte juridique établi, signé et archivé électroniquement dans la perspective d'un litige éventuel — et, de l'autre, la preuve après coup de faits juridiques : journaux de connexion, métadonnées, fichiers de logs, messages, photographies, enregistrements sonores ou vidéo, données extraites d'un appareil ou d'un serveur. La première catégorie ressortit pour l'essentiel au droit civil et commercial de la preuve, que la loi n° 53-05 a profondément renouvelé⁵⁰⁴⁹; la seconde nourrit les contentieux pénal, social, commercial ou familial, où prévalent d'autres logiques — la liberté de la preuve et l'intime conviction du juge⁵⁰⁵⁰.

La reconnaissance juridique de cette preuve d'un genre nouveau s'est faite en deux étapes. En 2007, la loi n° 53-05 — qui doit beaucoup à la loi type de la CNUDCI sur le commerce électronique ainsi qu'à la réforme française du 13 mars 2000⁵⁰⁵¹ — a inséré dans le code des obligations et des contrats les articles 417-1 à 417-3 : l'écrit électronique y est reçu en preuve

5047 Royaume du Maroc. (1913). Dahir du 9 ramadan 1331 (12 août 1913) formant code des obligations et des contrats, tel que modifié et complété. *Bulletin officiel*, 12 septembre 1913.

5048 Royaume du Maroc. (2020). Loi n° 55-19 relative à la simplification des mesures et des procédures administratives, promulguée par le dahir n° 1-20-06 du 6 mars 2020. *Bulletin officiel*, 6866, 19 mars 2020.

5049 Royaume du Maroc. (2007). Loi n° 53-05 relative à l'échange électronique de données juridiques, promulguée par le dahir n° 1-07-129 du 30 novembre 2007. *Bulletin officiel*, 5584, 6 décembre 2007.

5050 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, art. 286.

5051 Commission des Nations Unies pour le droit commercial international. (1996). *Loi type de la CNUDCI sur le commerce électronique*. Nations Unies; République française. (2000). Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique. *Journal officiel de la République française*, 14 mars 2000.

« au même titre que l'écrit sur support papier » et se voit reconnaître une force probante identique, à condition toutefois que son auteur puisse être identifié et que son intégrité soit garantie. Il a fallu attendre treize ans pour que la loi n° 43-20 relative aux services de confiance pour les transactions électroniques⁵⁰⁵² vienne rajeunir le versant technique du dispositif : elle distingue désormais trois niveaux de signature électronique — simple, avancée, qualifiée —, consacre le cachet électronique, l'horodatage et l'envoi recommandé électronique, et remet l'agrément comme la surveillance des prestataires de services de confiance entre les mains d'une autorité nationale. La parenté avec le règlement européen « eIDAS » est revendiquée sans détour⁵⁰⁵³.

Du côté répressif, la reconnaissance a suivi d'autres chemins : la loi n° 07-03, qui sanctionne les atteintes aux systèmes de traitement automatisé des données⁵⁰⁵⁴; la loi n° 03-03 relative à la lutte contre le terrorisme, qui a élargi les possibilités d'intercepter des communications; la loi n° 09-08 sur la protection des données à caractère personnel⁵⁰⁵⁵; la loi n° 05-20 relative à la cybersécurité⁵⁰⁵⁶; et, sur la scène internationale, l'adhésion du Royaume à la Convention de Budapest sur la cybercriminalité, applicable à son égard depuis 2018⁵⁰⁵⁷. L'appareil normatif existe donc bel et bien, et il n'a rien de dérisoire.

D'où vient, alors, que l'on parle encore de difficultés probatoires? De ce qu'un mode de preuve consacré par la loi n'est pas pour autant efficace devant le juge. Entre l'admissibilité de principe et la conviction du magistrat s'interposent une série d'obstacles que la preuve électronique franchit mal : établir qui a réellement écrit un message parti d'un compte susceptible d'être piraté; démontrer qu'un fichier est demeuré intact entre sa création et sa production en justice; obtenir l'expertise d'une pièce technique quand les spécialistes compétents se comptent sur les doigts d'une main; arracher à un hébergeur étranger des données de connexion; concilier, enfin, la manifestation de la vérité avec la vie privée et les données personnelles, que la Constitution de 2011 range parmi les droits fondamentaux⁵⁰⁵⁸. Sur toutes ces questions, les textes ne donnent que des réponses partielles, et une jurisprudence encore rare, parfois divisée, n'a pas achevé de dire le droit.

L'intérêt du sujet se mesure sur deux plans. Sur le plan théorique, la preuve électronique soumet à rude épreuve les notions cardinales du droit probatoire — l'écrit, l'original, la signature, la copie — et impose de reconstruire la hiérarchie des preuves autour d'un critère inédit : la fiabilité technique. Sur le plan pratique, la solidité du régime probatoire conditionne

5052 Royaume du Maroc. (2020). Loi n° 43-20 relative aux services de confiance pour les transactions électroniques, promulguée par le dahir n° 1-20-100 du 31 décembre 2020. *Bulletin officiel*, 6951, 14 janvier 2021. Ce texte abroge et remplace notamment les dispositions de la loi n° 53-05 relatives à la signature électronique.

5053 Parlement européen et Conseil de l'Union européenne. (2014). Règlement (UE) n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS). *Journal officiel de l'Union européenne*, L 257, 28 août 2014.

5054 Royaume du Maroc. (2003). Loi n° 07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données, promulguée par le dahir n° 1-03-197 du 11 novembre 2003. *Bulletin officiel*, 5171, 22 décembre 2003 (art. 607-3 à 607-11 du code pénal).

5055 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. *Bulletin officiel*, 5714, 5 mars 2009.

5056 Royaume du Maroc. (2020). Loi n° 05-20 relative à la cybersécurité, promulguée par le dahir n° 1-20-69 du 25 juillet 2020. *Bulletin officiel*, 6898, 30 juillet 2020.

5057 Conseil de l'Europe. (2001). *Convention sur la cybercriminalité* (STE n° 185). Budapest, 23 novembre 2001. Le Maroc y a adhéré en 2018.

5058 Royaume du Maroc. (2011). Constitution du Royaume du Maroc, promulguée par le dahir n° 1-11-91 du 29 juillet 2011, art. 24. *Bulletin officiel*, 5964 bis, 30 juillet 2011.

tout à la fois la sécurité des transactions en ligne, l'attractivité économique du pays, l'efficacité de la lutte contre la cybercriminalité et, au fond, la confiance que les citoyens placent dans leur justice à l'heure numérique. Quel commerçant accepterait de contracter en ligne sans la certitude de pouvoir, le moment venu, prouver son contrat? Quelle victime de chantage numérique déposerait plainte sans croire la justice capable d'établir les faits?

La problématique peut dès lors s'énoncer en ces termes : *dans quelle mesure le droit marocain, après avoir consacré la recevabilité et la force probante de la preuve électronique, réussit-il à lui assurer une efficacité réelle devant le juge, et par quelles réformes pourrait-on réduire l'écart entre la reconnaissance des textes et les difficultés constatées dans la pratique?*

La démarche retenue pour y répondre est avant tout analytique et critique : elle part des textes — code des obligations et des contrats, lois n° 53-05 et 43-20, code de procédure pénale, législations spéciales — pour les confronter aux orientations de la jurisprudence marocaine et aux acquis du droit comparé, français et européen au premier chef, puisque c'est là que le législateur marocain a puisé ouvertement son inspiration. L'étude se déploie en deux temps complémentaires : il s'agira d'examiner d'abord comment le droit marocain a reconnu juridiquement la preuve électronique, dans ses assises civiles comme dans ses prolongements pénaux (Première partie), puis d'analyser les difficultés probatoires qui en limitent la portée et les perspectives permettant d'y remédier (Deuxième partie).

Première partie : La reconnaissance juridique de la preuve électronique en droit marocain

Longtemps reléguée aux marges du droit positif, la preuve électronique a gagné sa place au Maroc par une double voie. Une consécration substantielle, d'abord, inscrite au cœur même du code des obligations et des contrats et achevée par la loi n° 43-20 : l'écrit électronique y est assimilé à l'écrit papier et les instruments techniques de sa fiabilité y sont organisés (Chapitre I). Une consécration contentieuse, ensuite, qui s'observe dans les différentes familles de litiges, où la preuve numérique est désormais reçue selon des régimes contrastés — préconstitution en matière civile, liberté de la preuve en matière pénale (Chapitre II).

Chapitre I : La consécration législative de l'écrit et de la signature électroniques

Le parti pris fondamental de la loi n° 53-05 tient en deux mots : équivalence fonctionnelle. Au lieu d'ériger, à côté du droit commun, un régime probatoire particulier pour les documents numériques, le législateur marocain a choisi de redéfinir l'écrit lui-même, en des termes indifférents au support. Aux termes de l'article 417-1 du code des obligations et des contrats, l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous la double condition que la personne dont il émane puisse être dûment identifiée et qu'il soit établi et conservé dans des conditions garantissant son intégrité⁵⁰⁵⁹. L'article 417-2 en déduit la suite logique : l'écrit sur support électronique possède la même force probante que son homologue papier⁵⁰⁶⁰. La portée de la formule est considérable : le juge ne peut plus écarter un document pour la seule raison qu'il est numérique, et l'acte électronique régulier accède au rang de preuve littérale parfaite, qui lie en principe le juge dans le système de preuve légale applicable aux actes juridiques civils.

Cette assimilation n'a pourtant rien d'automatique ni d'inconditionnel. Le papier porte en lui une apparence de stabilité; le fichier numérique, lui, doit faire la preuve de la sienne. Les deux exigences de l'article 417-1 — identification de l'auteur, garantie d'intégrité — fonctionnent comme un filtre de qualité : elles transcrivent, en termes juridiques, les fonctions que le papier et la signature manuscrite assuraient d'elles-mêmes. Identifier l'auteur, c'est restaurer l'imputabilité; garantir

⁵⁰⁵⁹ Code des obligations et des contrats, art. 417-1, tel qu'introduit par la loi n° 53-05 (2007).

⁵⁰⁶⁰ Code des obligations et des contrats, art. 417-2.

l'intégrité, c'est restaurer la permanence du contenu. On saisit ici la finesse de la méthode : le texte ne prescrit aucun procédé technique — il demeure technologiquement neutre — mais il fait de ces exigences les clés d'entrée dans le statut d'écrit probatoire. Un banal courriel non sécurisé peut, en théorie, valoir écrit au sens de l'article 417-1; encore faudra-t-il, en cas de contestation, persuader le juge que l'expéditeur est bien celui qu'il prétend être et que le contenu n'a pas bougé. À défaut, la pièce glissera vers un rôle probatoire de second rang — commencement de preuve par écrit, ou simple indice.

Le dispositif s'accompagne d'une série d'ajustements. L'article 417-3 institue — on y reviendra — une présomption de fiabilité au bénéfice des procédés sécurisés. Les articles 65-3 à 65-7 du même code règlent la formation du contrat par voie électronique, de l'offre à l'acceptation, en encadrant la mise à disposition des stipulations contractuelles et le mécanisme dit du « double clic »⁵⁰⁶¹. L'acte sous seing privé peut désormais être dressé électroniquement, et le régime des copies a été retouché pour accueillir les reproductions numériques fiables et durables⁵⁰⁶². L'ensemble compose un authentique statut civil de l'écrit électronique, couvrant aussi bien la conclusion du contrat que sa preuve — statut que la loi n° 31-08 édictant des mesures de protection du consommateur est venue prolonger pour les contrats conclus à distance⁵⁰⁶³.

L'équivalence fonctionnelle connaît par ailleurs des limites expressément posées. Le législateur de 2007 a soustrait au domaine de l'écrit électronique certains actes jugés trop sensibles pour quitter le formalisme du papier : les actes sous seing privé relatifs à l'application du code de la famille, et ceux relatifs aux sûretés personnelles ou réelles, civiles ou commerciales, sauf lorsqu'ils sont passés par une personne pour les besoins de sa profession⁵⁰⁶⁴. La prudence se conçoit : on n'a pas voulu qu'un cautionnement s'échange sur une messagerie, ni qu'un acte touchant au statut personnel se dématérialise sans garde-fou. Mais ce périmètre d'exclusions, arrêté en 2007, prête aujourd'hui à discussion, à une époque où le mariage se célèbre parfois à distance et où la pratique bancaire réclame la dématérialisation des garanties. Le droit français, qui a peu à peu ouvert l'écrit électronique à la plupart des actes sous signature privée, y compris certaines sûretés, plaide pour un réexamen de ces enclaves de papier⁵⁰⁶⁵.

La date n'est pas un problème moindre. La date certaine, qui rend l'acte opposable aux tiers, s'obtient classiquement par l'enregistrement ou par les événements que le code énumère; dans l'ordre numérique, ce rôle échoit à l'horodatage, et la loi n° 43-20 a eu le mérite d'en faire un service de confiance à part entière, dont la version qualifiée jouit d'une présomption d'exactitude. Mais tant que l'horodatage qualifié restera l'exception, la datation des documents électroniques ordinaires — un courriel, un fichier bureautique — dépendra de métadonnées manipulables, que l'expertise peut analyser sans toujours pouvoir les certifier. Là encore se creuse un fossé entre une élite documentaire sécurisée et le tout-venant numérique des relations juridiques courantes — et c'est dans ce fossé que le contentieux prospère.

Un écrit ne vaut que par la signature qui l'assume. Dès 2007, la loi n° 53-05 avait donc défini la signature électronique et bâti un régime de signature « sécurisée », appuyé sur des certificats émanant de prestataires agréés. Ce premier édifice, techniquement vieilli et peu pratiqué, a été entièrement refondu par la loi n° 43-20 relative aux services de confiance pour

5061 Code des obligations et des contrats, art. 65-3 à 65-7, introduits par la loi n° 53-05 (2007), relatifs à l'échange d'informations et à la conclusion du contrat par voie électronique.

5062 Code des obligations et des contrats, art. 426 et 440, tels que modifiés par la loi n° 53-05 (2007).

5063 Royaume du Maroc. (2011). Loi n° 31-08 édictant des mesures de protection du consommateur, promulguée par le dahir n° 1-11-03 du 18 février 2011, art. 25 et s. *Bulletin officiel*, 5932, 7 avril 2011.

5064 Loi n° 53-05 (2007), art. 2.

5065 République française. (2016). Code civil, art. 1174 et s., dans leur rédaction issue de l'ordonnance n° 2016-131 du 10 février 2016.

les transactions électroniques, devenue le droit commun technique de la matière. Empruntant sans détour son architecture au règlement européen eIDAS, le texte marocain retient une gradation à trois degrés : la signature électronique simple; la signature électronique avancée, liée au signataire de manière univoque, permettant de l'identifier, créée par des moyens demeurant sous son contrôle exclusif et rendant détectable toute modification ultérieure de l'acte; et la signature électronique qualifiée, produite au moyen d'un dispositif qualifié et adossée à un certificat qualifié délivré par un prestataire agréé⁵⁰⁶⁶.

À cette échelle de signatures répond une échelle d'effets. Seule la signature qualifiée est, de plein droit, assimilée à la signature manuscrite; elle seule bénéficie de la présomption de fiabilité qui inverse la charge de la contestation : c'est au contestataire d'établir la défaillance du procédé, non au porteur de l'acte d'en démontrer la solidité⁵⁰⁶⁷. Les signatures simple et avancée ne sont pas pour autant sans valeur : le juge ne saurait les repousser au seul motif de leur forme électronique ou de leur absence de qualification, mais leur fiabilité relève de sa libre appréciation, au vu des éléments versés. Le système joue ainsi sur deux tableaux : une admissibilité générale, qui ouvre le prétoire à toutes les signatures électroniques, et une hiérarchie des forces probantes, qui récompense l'investissement dans la sécurité. La loi n° 43-20 prolonge du reste la logique des services de confiance au-delà de la signature : cachet électronique des personnes morales, horodatage donnant date opposable à un fichier, envoi recommandé électronique, authentification de sites — autant d'outils de préconstitution d'une preuve numérique solide.

La clé de voûte institutionnelle du système est l'Autorité nationale des services de confiance, dont les attributions sont exercées par la Direction générale de la sécurité des systèmes d'information, rattachée à l'Administration de la défense nationale : agrément des prestataires qualifiés, contrôle de leur activité, tenue des listes de confiance, qualification des dispositifs⁵⁰⁶⁸. Confier la certification électronique à l'autorité chargée de la cybersécurité relève d'une logique cohérente : en dernière analyse, la valeur juridique de la signature repose sur la robustesse cryptographique et organisationnelle des prestataires. En pratique toutefois, l'offre de certification qualifiée reste concentrée entre les mains d'un petit nombre d'opérateurs — historiquement dominée par le service de certification de Barid Al-Maghrib —, ce qui bride la diffusion de la signature qualifiée dans le tissu économique, au premier chef auprès des petites entreprises et des particuliers.

Chapitre II : L'admissibilité de la preuve électronique dans les différents contentieux

En matière civile, régie par le système de la preuve légale, la preuve électronique se distribue selon la distinction classique des actes et des faits juridiques. Pour les actes dépassant le seuil au-delà duquel le témoignage est irrecevable, l'écrit demeure requis — mais cet écrit peut désormais être électronique, pourvu qu'il réponde aux conditions de l'article 417-1. L'acte sous seing privé électronique régulièrement signé fait foi de son contenu entre les parties, et celui qui porte une signature qualifiée jouit de la présomption de fiabilité. Quant à l'écrit électronique qui ne remplit pas les conditions légales — courriel ordinaire, message non signé —, il n'est pas pour autant chassé du débat : doctrine et jurisprudence inclinent à y voir un commencement de preuve par écrit, susceptible d'être complété par témoignages et présomptions, ou à tout le

5066 Loi n° 43-20 (2020), art. 2 et s., définissant les niveaux de signature électronique et les services de confiance.

5067 Code des obligations et des contrats, art. 417-3, combiné avec les dispositions de la loi n° 43-20 (2020) relatives aux effets juridiques de la signature électronique qualifiée.

5068 Loi n° 43-20 (2020), dispositions relatives à l'Autorité nationale des services de confiance pour les transactions électroniques, dont les attributions sont confiées à la Direction générale de la sécurité des systèmes d'information (DGSSI).

moins un indice abandonné à l'appréciation du juge. Cette souplesse est heureuse; elle entretient cependant une zone grise où la valeur d'une même pièce varie sensiblement d'un tribunal à l'autre.

La question de l'acte authentique électronique dessine, quant à elle, la prochaine frontière du droit civil de la preuve. Le notariat moderne et les professions de l'authenticité — adoul, notaires, huissiers — reposent sur l'intervention d'un officier public qui confère à l'acte une force probante renforcée et la force exécutoire; rien n'interdit, conceptuellement, que cette intervention se dématérialise — l'officier instrumentant sur support électronique, signant au moyen d'un dispositif qualifié, conservant l'acte dans un minutier central numérique. Le droit français a sauté le pas depuis longtemps, jusqu'à admettre l'acte notarié à distance par comparution vidéo; le Maroc, où la numérisation des études notariales et de leurs échanges avec la conservation foncière et l'administration fiscale avance à bon rythme, possède les briques techniques d'une évolution comparable. L'enjeu probatoire est de taille : l'acte authentique électronique apporterait au monde numérique ce qui s'approche le plus d'une preuve absolue, et son minutier dématérialisé, adossé aux services de confiance qualifiés, formerait l'archive de référence des transactions importantes. La réforme exigera de retoucher les textes professionnels et le régime de l'authenticité; elle mérite de figurer sans attendre à l'agenda législatif.

Le contentieux commercial réserve à la preuve électronique un accueil plus favorable encore. L'article 334 du code de commerce pose en effet la liberté de la preuve en matière commerciale, sous réserve des exceptions légales⁵⁰⁶⁹ : factures électroniques, courriels échangés entre commerçants, bons de commande dématérialisés, relevés tirés des systèmes d'information — tout peut librement concourir à la démonstration des obligations. La pratique bancaire en donne l'illustration la plus quotidienne : la jurisprudence reconnaît de longue date la force probante des relevés et enregistrements informatiques des établissements de crédit dans leurs rapports avec leurs clients commerçants, sous les conditions de régularité fixées par la législation bancaire⁵⁰⁷⁰. De même, l'essor du paiement mobile et du commerce en ligne repose tout entier sur la traçabilité électronique des opérations, dont les journaux informatiques forment la mémoire probatoire.

La vie des affaires fournit du reste au juge commercial un repère que le droit civil ignore : l'usage. Entre partenaires accoutumés à traiter par courriel, l'échange demeuré incontesté au fil des années vaut convention tacite sur le mode de communication, et la partie qui découvre au premier litige que les courriels « ne prouvent rien » se heurte à l'exigence de bonne foi. Les conventions de preuve — clauses sur la valeur des journaux informatiques, sur les procédés de validation, sur l'archivage — se multiplient dans les contrats d'affaires et les conditions générales des services en ligne. Licites lorsqu'elles portent sur des droits disponibles, elles restent sous le regard du juge quand, dans un rapport déséquilibré, elles priveraient une partie de toute possibilité effective de preuve contraire.

Les matières sociale et familiale révèlent, pour leur part, les tensions que la preuve numérique fait naître. Devant les juridictions sociales, l'employeur brandit volontiers courriels professionnels, fichiers de pointage ou traces de connexion pour établir la faute du salarié, tandis que ce dernier produit des messages pour prouver des heures supplémentaires ou un harcèlement; au juge, alors, d'arbitrer entre le pouvoir de contrôle patronal et la vie privée du salarié, y compris sur les outils professionnels. Dans le contentieux familial, captures d'écran de conversations et publications sur les réseaux sociaux envahissent les procédures de divorce; leur recevabilité bute à la fois sur les exclusions de l'article 2 de la loi n° 53-05 pour

⁵⁰⁶⁹ Royaume du Maroc. (1996). Loi n° 15-95 formant code de commerce, promulguée par le dahir n° 1-96-83 du 1er août 1996, art. 334. *Bulletin officiel*, 4418, 3 octobre 1996.

⁵⁰⁷⁰ Royaume du Maroc. (2014). Loi n° 103-12 relative aux établissements de crédit et organismes assimilés, promulguée par le dahir n° 1-14-193 du 24 décembre 2014, art. 156. *Bulletin officiel*, 6328, 22 janvier 2015.

les actes relevant du code de la famille et sur les exigences de loyauté et de respect de l'intimité. La preuve électronique s'infiltré ainsi dans tous les prétoires, mais avec des fortunes inégales, au gré des régimes probatoires propres à chaque contentieux.

Le procès pénal reçoit la preuve électronique sous la bannière d'un principe cardinal : la liberté de la preuve. L'article 286 du code de procédure pénale permet d'établir les infractions par tout mode de preuve, hors les cas où la loi en dispose autrement, le juge statuant selon son intime conviction, qu'il doit motiver⁵⁰⁷¹. Rien ne s'oppose donc, dans le principe, à ce qu'une condamnation s'appuie sur des courriels, des messages, des données de connexion, des enregistrements ou des fichiers extraits d'un support informatique. La preuve numérique s'est même imposée comme la reine des preuves dans des pans entiers du contentieux répressif : escroqueries en ligne, chantage à la webcam, usurpation d'identité numérique, diffusion d'images portant atteinte à la vie privée, atteintes aux systèmes de traitement automatisé des données que répriment les articles 607-3 et suivants du code pénal issus de la loi n° 07-035072. Dans ces affaires, l'infraction elle-même est numérique; sa preuve ne saurait l'être moins.

La liberté de la preuve n'est pas, pour autant, licence de prouver n'importe comment. La preuve pénale électronique demeure tenue par le principe de légalité dans la recherche des preuves et par les garanties constitutionnelles du procès équitable. L'article 24 de la Constitution protège la vie privée et le secret des communications privées, auxquels il ne peut être porté atteinte que dans les conditions prévues par la loi. Le code de procédure pénale encadre ainsi strictement l'interception des communications à distance : interdite par principe, elle n'est possible que sur autorisation judiciaire, pour des infractions limitativement énumérées — atteintes à la sûreté de l'État, terrorisme, stupéfiants, armes, enlèvement, fausse monnaie, notamment —, pour une durée bornée et sous le contrôle du magistrat⁵⁰⁷³. Les perquisitions et saisies s'étendent, en pratique, aux supports et données informatiques, et l'officier de police judiciaire peut s'adjoindre toute personne qualifiée pour procéder aux constatations techniques.

L'adhésion du Maroc à la Convention de Budapest a par ailleurs élargi la panoplie conceptuelle : conservation rapide des données stockées, injonctions de produire, perquisition et saisie de données informatiques, entraide internationale renforcée. La loi n° 05-20 sur la cybersécurité, en soumettant les opérateurs d'importance vitale à des obligations de sécurité et de notification des incidents, contribue indirectement à la formation de traces exploitables. Il n'en reste pas moins que le code de procédure pénale marocain ne comporte toujours pas de régime général et cohérent de la preuve numérique : les textes avancent par retouches successives, greffées sur des institutions conçues pour le monde physique — perquisition, saisie, expertise — et laissent en suspens des questions aussi essentielles que la chaîne de conservation des supports saisis, la copie forensique, l'accès aux données chiffrées ou la captation à distance. Cette incomplétude, supportable tant que la preuve numérique restait marginale, devient problématique à mesure qu'elle envahit le contentieux; elle est l'une des sources majeures des difficultés qu'il faudra examiner.

Deux gisements de preuve dominent la pratique répressive contemporaine. Le premier est celui des données de connexion conservées par les opérateurs de télécommunications : identification des abonnés, journaux d'appels, données de

⁵⁰⁷¹ Loi n° 22-01 (2002), art. 286.

⁵⁰⁷² Code pénal, art. 607-3 à 607-11, issus de la loi n° 07-03 (2003).

⁵⁰⁷³ Loi n° 22-01 (2002), art. 108 et s., tels que modifiés notamment par : Royaume du Maroc. (2003). Loi n° 03-03 relative à la lutte contre le terrorisme, promulguée par le dahir n° 1-03-140 du 28 mai 2003. *Bulletin officiel*, 5112, 29 mai 2003.

localisation des terminaux, qui permettent de reconstituer déplacements et contacts d'un suspect avec une précision redoutable. Leur obtention par réquisition judiciaire est devenue un réflexe d'enquête; leur exploitation pose, en retour, la question de la durée de conservation imposée aux opérateurs et de la proportionnalité de l'accès — que les juridictions européennes ont profondément rediscutée et que le droit marocain gagnerait à encadrer plus finement. Le second gisement est celui des contenus publiés sur les réseaux sociaux, théâtre d'une part croissante des infractions d'expression — diffamation, injure, incitation à la haine, atteintes à la vie privée par diffusion d'images — comme des escroqueries et manipulations. Le caractère public de la publication simplifie la preuve du contenu; demeurent entières les difficultés d'imputation du compte à une personne et de coopération avec des plateformes étrangères pour démasquer les auteurs retranchés derrière des pseudonymes.

On ajoutera que la preuve électronique pénale n'est pas seulement une arme de l'accusation : elle est aussi, et de plus en plus, une preuve de la défense. L'horodatage d'une connexion, la géolocalisation d'un téléphone, l'historique d'une messagerie peuvent asseoir un alibi, révéler une manipulation, démentir un témoignage. L'égalité des armes commande alors que la défense accède, dans des conditions praticables, aux données saisies et aux rapports techniques, et qu'elle puisse en solliciter la contre-expertise. L'accès du prévenu à la copie des données extraites de ses propres supports, comme le financement de la contre-expertise pour les justiciables sans ressources, participe du procès équitable numérique que l'article 120 de la Constitution appelle de ses vœux⁵⁰⁷⁴.

Deuxième partie : Les difficultés probatoires de la preuve électronique et les voies de leur dépassement

Consacrée par les textes, la preuve électronique reste laborieuse dans les faits. Sa nature même — immatérielle, fugace, reproductible à l'infini, modifiable sans trace apparente — la rend suspecte aux yeux d'un juge élevé dans le culte de l'original papier, tandis que son administration réclame des compétences, des institutions et des coopérations qui manquent encore en partie (Chapitre I). Ces difficultés, que les insuffisances du cadre normatif et la retenue de la jurisprudence viennent aggraver, appellent des réponses dont le dessin se précise déjà, entre consolidation prétorienne, modernisation institutionnelle et réforme législative (Chapitre II).

Chapitre I : Les difficultés d'administration de la preuve électronique

Une première série de difficultés tient à la nature même de la preuve numérique. Un document papier falsifié laisse presque toujours des stigmates — grattage, surcharge, différence d'encre — que l'expertise graphologique sait débusquer. Un fichier numérique, lui, peut être retouché sans autre trace que des métadonnées, elles-mêmes altérables. La capture d'écran, pièce vedette des dossiers d'aujourd'hui, résume le paradoxe : rien n'est plus simple à produire, rien n'est plus simple à fabriquer. Quelques minutes suffisent, avec des outils grand public, pour composer une fausse conversation WhatsApp ou un faux courriel d'une vraisemblance parfaite. Le juge est ainsi placé devant une alternative inconfortable : accueillir avec crédulité des pièces éminemment falsifiables, ou les écarter avec une rigueur qui priverait de preuve des plaideurs de bonne foi. Les juridictions marocaines oscillent entre ces deux pôles : certaines décisions reçoivent les captures d'écran comme éléments de preuve ou indices, surtout lorsqu'elles sont corroborées, quand d'autres les rejettent, dès qu'elles sont contestées, comme dénuées de toute garantie d'authenticité.

⁵⁰⁷⁴ Constitution du Royaume du Maroc (2011), art. 119 et 120, consacrant la présomption d'innocence et le droit à un procès équitable.

Le courriel, doyen des écrits électroniques, illustre bien la gradation des vérifications possibles. L'impression papier d'un message, telle qu'elle est ordinairement versée aux débats, n'établit par elle-même ni l'envoi, ni la réception, ni l'intégrité du texte : elle se fabrique en quelques instants dans n'importe quel logiciel de messagerie. Un premier degré de contrôle consiste à examiner le message sous sa forme native, avec ses en-têtes complets, qui retracent le cheminement du courriel de serveur en serveur et consignent les résultats des mécanismes d'authentification du courrier électronique — signatures des domaines expéditeurs, contrôles d'origine — dont la vérification permet souvent de confirmer ou d'exclure la provenance alléguée. Un deuxième degré fait intervenir le tiers : l'opérateur de messagerie ou l'hébergeur, requis d'attester l'existence du message dans les boîtes concernées et dans les journaux de transport. Le troisième degré est l'expertise du support lui-même. Rien de tout cela n'excède les moyens d'une justice organisée; mais tout cela suppose que la pièce soit demandée et produite sous forme native, et non en simple copie d'écran — réflexe procédural élémentaire qui, à lui seul, désamorceraient une part notable des contestations, et que les juridictions gagneraient à ériger en exigence de principe.

Une difficulté plus sourde, d'ordre culturel, s'y ajoute : la formation initiale des magistrats, des avocats et des greffiers demeure essentiellement juridique, et la culture technique qu'exige l'appréciation critique d'une preuve numérique — savoir ce qu'est un en-tête de courriel, une valeur de hachage, une métadonnée EXIF, un journal de serveur — reste inégalement partagée. Il en résulte tantôt une défiance excessive, qui stérilise des preuves exploitables, tantôt une confiance excessive, qui accueille sans recul des pièces manipulées. Les efforts de formation continue de l'Institut supérieur de la magistrature et la spécialisation progressive de certains parquets et services d'enquête en matière de cybercriminalité vont dans la bonne direction; mais la montée en compétence de toute la chaîne judiciaire prendra du temps.

Un défi d'une ampleur inédite se profile enfin avec l'intelligence artificielle générative. Des outils à la portée de tous produisent désormais en quelques instants des images photoréalistes, des voix clonées et des vidéos truquées dont la détection dépasse l'œil et, parfois, l'expert. La conséquence probatoire est double : des contenus fabriqués pourront être présentés comme preuves de faits qui n'ont jamais eu lieu, et les auteurs de faits réellement enregistrés invoqueront systématiquement le trucage — ce que la doctrine étrangère appelle déjà le « dividende du menteur ». La riposte passe par l'authentification à la source — signature des contenus, ancrage cryptographique, métadonnées certifiées — et par l'organisation du débat contradictoire sur l'authenticité, volet que le législateur marocain, s'il entend encadrer l'intelligence artificielle, ne pourra laisser de côté.

L'expertise judiciaire forme le premier goulot d'étranglement. Apprécier l'intégrité d'un fichier, analyser un support saisi, restaurer des données effacées ou examiner un système d'information suppose des experts en informatique légale — la « forensique numérique » — dont le vivier reste étroit au regard du contentieux. Les tableaux des experts judiciaires près les cours d'appel comptent peu de spécialistes du numérique, leur répartition sur le territoire est inégale, et la technicité des missions contraste parfois avec les conditions matérielles de leur exercice⁵⁰⁷⁵. Le coût des expertises, avancé par les parties en matière civile, dissuade en outre les plaideurs modestes de provoquer la vérification technique qui emporterait pourtant la décision; la preuve électronique risque ainsi de devenir une preuve de riches. Du côté répressif, les laboratoires spécialisés de la police judiciaire et de la gendarmerie ont indéniablement gagné en capacité, mais l'engorgement des services devant

5075 Royaume du Maroc. (2001). Loi n° 45-00 relative aux experts judiciaires, promulguée par le dahir n° 1-01-126 du 22 juin 2001. *Bulletin officiel*, 4918, 19 juillet 2001.

la massification des supports saisis — chaque affaire livre désormais téléphones, disques et comptes par dizaines — allonge les délais et fragilise les procédures.

La chaîne de conservation illustre, quant à elle, le déficit d'encadrement procédural. De la saisie d'un support à la production de son contenu à l'audience se déroule une chaîne d'opérations — copie, scellés, analyse, extraction, restitution — dont chaque maillon peut altérer la donnée ou en compromettre la traçabilité. Les standards internationaux de la forensique imposent la copie bit à bit, le calcul d'empreintes de hachage, la documentation de chaque accès; or le code de procédure pénale marocain, pensé pour les scellés physiques, n'impose pas expressément ces protocoles, abandonnés aux bonnes pratiques des services. Il en résulte un risque contentieux à double tranchant : pour la défense, l'impossibilité de vérifier que la donnée produite est bien celle qui a été saisie; pour l'accusation, le risque de voir contester des éléments recueillis sans méthodologie certifiée. Consacrer légalement un protocole de préservation de la preuve numérique — copie forensique, empreinte, journal des accès — remédierait à une lacune que la seule jurisprudence peine à combler.

Le facteur temps constitue une difficulté transversale que la procédure civile domestique encadre mal. La preuve numérique est périssable : les plateformes purgent leurs journaux à brève échéance, les contenus litigieux s'effacent d'un geste, les comptes se ferment, les téléphones se réinitialisent. Le procès civil, lui, s'étire dans la durée. Entre l'assignation et le jugement ordonnant, le cas échéant, une expertise ou une production de pièces, les données pertinentes ont souvent disparu. La parade existe dans les principes : mesures d'instruction préventives, constats ordonnés sur requête avant tout procès, injonctions de conservation adressées aux détenteurs de données sous astreinte. Mais leur usage en matière numérique demeure timide, faute de réflexes et de références : le plaideur marocain n'a pas encore à sa disposition l'équivalent rodé des procédures d'urgence probatoire que d'autres systèmes ont acclimatées au numérique. Le développement d'un véritable « référé probatoire numérique » — saisine rapide du juge aux fins de constat, de conservation ou de communication de données menacées de disparition — représenterait l'un des progrès procéduraux les plus rentables qui soient, car il intervient au moment où la preuve peut encore être sauvée.

Les obstacles atteignent leur comble lorsque la preuve se trouve à l'étranger — et c'est presque toujours le cas. Les messageries, réseaux sociaux et services d'hébergement utilisés au Maroc sont, pour l'essentiel, exploités par des opérateurs établis hors du territoire, soumis à des droits étrangers et peu empressés de répondre aux réquisitions directes des autorités marocaines. L'obtention des données de contenu passe alors par l'entraide judiciaire internationale, dont la lenteur — plusieurs mois, parfois davantage — s'accorde mal avec la volatilité de données souvent effacées avant l'aboutissement de la demande. L'adhésion à la Convention de Budapest a ouvert des canaux plus rapides — conservation rapide des données, réseau de points de contact permanents — et les mécanismes de coopération directe avec certains fournisseurs se développent pour les données qui ne relèvent pas du contenu; il n'en demeure pas moins que le juge marocain dépend, pour une part croissante de la preuve, du bon vouloir d'acteurs privés étrangers et d'ordres juridiques tiers. Le chiffrement de bout en bout des messageries ajoute une couche d'opacité supplémentaire, qui déplace l'enquête vers l'exploitation des terminaux eux-mêmes.

La preuve électronique nourrit enfin un contentieux propre de licéité. Recueillie au mépris des formes légales — interception non autorisée, accès frauduleux à un compte, enregistrement clandestin —, elle expose son auteur à des poursuites et sa production à la nullité ou au rejet. La ligne de partage n'est pourtant pas toujours nette : que vaut, au pénal, la preuve rapportée par un particulier qui a fouillé le téléphone de son conjoint? La liberté de la preuve couvre-t-elle la

preuve déloyalement obtenue par une partie privée, comme l'admet, dans certaines limites, la jurisprudence française au nom du droit à la preuve⁵⁰⁷⁶? Le droit marocain n'offre pas de réponse d'ensemble, et les solutions varient d'un contentieux à l'autre, entre exigence de loyauté civile, protection pénale de la vie privée renforcée par les articles 447-1 et suivants du code pénal⁵⁰⁷⁷ et régime des nullités de procédure. Cette incertitude entretient une insécurité juridique que seule une doctrine jurisprudentielle ferme, ou une intervention du législateur, pourrait dissiper.

L'ensemble de ces obstacles dessine, en filigrane, un risque d'inégalité devant la preuve. La partie institutionnelle ou fortunée — banque, opérateur, grande entreprise, ministère public appuyé sur des services spécialisés — dispose des systèmes d'information, des journaux, des certificats et des experts qui fabriquent les preuves solides; le particulier, lui, n'a le plus souvent que son téléphone, ses captures d'écran et sa bonne foi. Le déséquilibre n'est pas propre au numérique, mais le numérique l'accentue, car la qualité de la preuve y dépend directement de l'équipement technique de celui qui la constitue. Y remédier suppose des instruments de rééquilibrage : accès facilité aux constats et aux expertises, obligations de production de données à la charge des détenteurs professionnels sous astreinte du juge, présomptions protectrices dans les rapports asymétriques — sur le modèle de celles que connaît déjà le droit de la consommation — et, en amont, diffusion d'outils de préconstitution simples et peu coûteux à destination du grand public.

Chapitre II : Les limites du cadre normatif et les perspectives d'amélioration

Le premier grief que l'on peut adresser au dispositif marocain est son éparpillement. Le régime de la preuve électronique se reconstitue aujourd'hui par la juxtaposition de textes d'époques et d'inspirations diverses : le D.O.C. pour la force probante, la loi n° 53-05 résiduelle pour le domaine de l'écrit électronique et ses exclusions, la loi n° 43-20 pour les services de confiance, le code de commerce pour la liberté commerciale, le code de procédure pénale pour l'enquête, les lois n° 07-03, 09-08, 05-20 et 103-13 pour leurs objets respectifs. Cette sédimentation nuit à la lisibilité : le praticien doit se frayer un chemin entre des définitions qui ne coïncident pas toujours, des renvois implicites et des abrogations partielles dont le périmètre exact prête à débat. La coexistence de la loi n° 53-05, partiellement abrogée, et de la loi n° 43-20 en est le symbole : réunir le droit de la preuve électronique dans un corpus cohérent — au sein d'un D.O.C. rénové ou d'un texte consolidé — servirait la sécurité juridique.

La deuxième insuffisance tient au mutisme des textes sur la preuve numérique en procédure pénale. On l'a dit : ni la copie forensique, ni l'empreinte numérique, ni la conservation des données saisies, ni l'accès aux données chiffrées, ni la captation de données à distance ne font l'objet d'un régime légal d'ensemble, alors même que la matière touche au cœur des libertés. Le contraste avec les droits voisins est frappant : le code de procédure pénale français consacre des dispositions détaillées aux perquisitions informatiques, aux réquisitions numériques, à la mise au clair des données chiffrées et aux techniques spéciales d'enquête⁵⁰⁷⁸. Le chantier, ouvert de longue date, de la réforme du code de procédure pénale marocain offre l'occasion d'y introduire un titre dédié à la preuve numérique, qui codifierait les garanties — autorisation, proportionnalité, contrôle du juge, droits de la défense sur la donnée — en même temps que les pouvoirs.

5076 Cour de cassation, Assemblée plénière. (2023, 22 décembre). *Arrêt n° 20-20.648*. Cet arrêt admet, sous conditions, la recevabilité d'une preuve obtenue de manière déloyale lorsqu'elle est indispensable et proportionnée.
5077 Royaume du Maroc. (2018). Loi n° 103-13 relative à la lutte contre les violences faites aux femmes, promulguée par le dahir n° 1-18-19 du 22 février 2018. *Bulletin officiel*, 6655, 12 mars 2018 (art. 447-1 à 447-3 du code pénal, réprimant notamment la diffusion d'enregistrements et d'images sans consentement).
5078 République française. Code de procédure pénale, art. 57-1, 60-1 et s., 230-1 et s., 706-102-1 et s.

La troisième zone d'ombre est jurisprudentielle. Faute d'un contentieux massif porté jusqu'à la Cour de cassation, la matière manque de ces arrêts de principe qui fixent le droit : quelle valeur exacte pour un courriel simple contesté? Une capture d'écran non corroborée peut-elle fonder une condamnation? Le refus de communiquer un code de déverrouillage peut-il être sanctionné, et la donnée tirée d'un téléphone consulté sans base légale doit-elle être écartée? À ces questions, les juridictions du fond apportent des réponses dispersées, rarement publiées, parfois contradictoires; l'unification prétorienne demeure embryonnaire. Cette discrétion jurisprudentielle a un coût systémique : elle prive les plaideurs de prévisibilité et les juges du fond de repères, et elle entretient chez les justiciables le sentiment que la valeur d'une preuve numérique tient moins à sa qualité qu'au tribunal devant lequel elle échoit. La publication systématique des décisions — que la numérisation de la justice rend techniquement possible — et une politique de pourvois dans l'intérêt de la loi contribueraient à l'édification d'une doctrine cohérente.

La doctrine du juge face à la pièce numérique contestée reste elle aussi à écrire. Trois offices sont concevables, que la pratique mélange sans les distinguer : un office passif, où le juge retient ou écarte la pièce sur une impression d'ensemble; un office arbitral, où il répartit les charges entre celui qui produit et celui qui conteste, puis tire les conséquences des carences — ce qui suppose des règles claires de charge de la preuve de la fiabilité, aujourd'hui incertaines pour les procédés non qualifiés; un office actif, enfin, où il ordonne d'office les vérifications qu'appelle la pièce douteuse, au besoin par expertise. Le choix ne devrait pas dépendre du tempérament de chaque magistrat : la Cour de cassation ou le législateur gagnerait à poser que la contestation sérieuse d'une pièce numérique déterminante ne peut être tranchée sans vérification technique.

Reste la tension, encore mal arbitrée, entre l'efficacité probatoire et la protection des données personnelles. Toute preuve électronique est, peu ou prou, un traitement de données à caractère personnel; sa collecte, sa conservation et sa production en justice croisent donc la loi n° 09-08 et les principes de finalité, de proportionnalité et de licéité qu'elle édicte sous le contrôle de la Commission nationale de contrôle de la protection des données à caractère personnel. Le justiciable qui produit les messages de son adversaire, l'employeur qui exploite les journaux de connexion de ses salariés, l'enquêteur qui aspire le contenu d'un téléphone manipulent des données protégées. Droit à la preuve et droit à la protection des données doivent être conciliés, non hiérarchisés dans l'abstrait; la réforme annoncée du cadre marocain de protection des données, appelée à le rapprocher des standards du RGPD européen, devra impérativement traiter cette interface probatoire, aujourd'hui abandonnée à l'intuition des juges⁵⁰⁷⁹.

Les voies d'amélioration se laissent ordonner en trois cercles. Le premier est institutionnel et ne réclame aucune loi nouvelle : étoffer le corps des experts judiciaires en informatique légale, en révisant les conditions d'inscription, la rémunération et la formation continue; doter les juridictions de référents numériques; généraliser, dans les services d'enquête, des protocoles certifiés de copie et de scellement numériques; intégrer, enfin, la preuve électronique dans la formation initiale et continue des magistrats et des avocats. L'expérience comparée le montre : la qualité de la justice numérique tient moins aux textes qu'aux hommes et aux procédures internes — un protocole de chaîne de conservation rigoureusement appliqué vaut mieux qu'un article de loi ignoré.

5079 Parlement européen et Conseil de l'Union européenne. (2016). Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD). *Journal officiel de l'Union européenne*, L 119, 4 mai 2016. Voir aussi la jurisprudence de la Cour de justice de l'Union européenne sur la conciliation entre protection des données et administration de la preuve en justice.

Le deuxième cercle est technologique. L'État peut jouer un rôle d'entraînement en généralisant la signature qualifiée et l'horodatage dans ses propres relations avec les usagers — marchés publics, téléservices, actes de l'administration — et créer ainsi l'écosystème de confiance dont le secteur privé a besoin pour basculer. L'identité numérique nationale, adossée à la carte nationale d'identité électronique, offre un socle prometteur pour une authentification forte accessible à tous, qui réglerait en amont une large part des litiges d'imputabilité. Les technologies d'ancrage cryptographique — empreintes de hachage, registres distribués — méritent par ailleurs l'attention du législateur probatoire : plusieurs droits étrangers attachent déjà des effets juridiques à l'enregistrement d'une empreinte sur une chaîne de blocs, qui procure une datation et une garantie d'intégrité pratiquement inviolables. Sans sacrifier à la mode, le droit marocain gagnerait à ménager, par une disposition technologiquement neutre, la recevabilité de ces procédés d'ancrage comme mode de préconstitution de la preuve.

Le troisième cercle est législatif et jurisprudentiel. Législatif : unifier le corpus de la preuve électronique, réviser les exclusions héritées de 2007, introduire dans le code de procédure pénale un régime complet de la preuve numérique, encadrer la production en justice des données personnelles et clarifier le sort de la preuve illicite ou déloyale selon une grille de proportionnalité. Jurisprudentiel : il revient à la Cour de cassation, au fil des pourvois, de fixer une doctrine de la preuve numérique — degrés de force probante, conditions de corroboration, sanctions des irrégularités — qui donne aux juges du fond la grammaire commune qui leur fait défaut. La dynamique est lancée : la dématérialisation des procédures elles-mêmes, portée par les juridictions numériques et consacrée par la réforme de la procédure civile, familiarise chaque jour davantage l'institution judiciaire avec l'écrit électronique — et il serait paradoxal qu'une justice qui se numérise continue de se méfier de la preuve numérique.

La consolidation du régime probatoire numérique est aussi l'affaire de la communauté juridique tout entière. La doctrine marocaine, dont les travaux sur la preuve électronique se multiplient dans les revues spécialisées et les universités, a un rôle décisif à tenir : recenser et commenter les décisions éparpillées des juridictions du fond, construire les typologies et les grilles d'analyse dont les praticiens ont besoin, dialoguer avec les ingénieurs pour traduire en catégories juridiques les réalités techniques. Les barreaux et les instances professionnelles peuvent, de leur côté, diffuser les bonnes pratiques de constitution et de production de la preuve numérique — bien des preuves se perdent moins devant le juge que dans la manière dont elles ont été recueillies. Un droit vivant de la preuve électronique ne naîtra pas du seul législateur : il se construira, comme tous les grands corps de règles probatoires, par l'échange continu entre le texte, le prétoire et l'école.

Le droit comparé, enfin, fournit des repères sans imposer de modèle. Le règlement eIDAS, révisé en 2024 pour instituer le portefeuille européen d'identité numérique⁵⁰⁸⁰, montre la voie d'une identité et d'une signature électroniques de masse; la jurisprudence française sur le droit à la preuve enseigne l'art de la proportionnalité entre vérité et vie privée; les standards de la Convention de Budapest et de son deuxième protocole additionnel dessinent l'avenir de la coopération probatoire transfrontière. Le Maroc, qui a toujours su emprunter sans se renier, dispose là d'un matériau abondant pour écrire la prochaine étape de son droit de la preuve.

5080 Parlement européen et Conseil de l'Union européenne. (2024). Règlement (UE) 2024/1183 du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique. *Journal officiel de l'Union européenne*, L, 30 avril 2024.

Resterait à évoquer, dans une perspective plus lointaine, l'irruption de l'intelligence artificielle dans l'appréciation même de la preuve : outils d'analyse massive des données saisies, détection automatisée des contenus falsifiés, aide à la cotation de la fiabilité des pièces. Ces instruments promettent d'assister un juge submergé par le volume numérique; ils portent aussi le risque d'une délégation insidieuse de l'intime conviction à des systèmes opaques. Le principe doit être posé dès maintenant : l'outil éclaire, le juge apprécie. La conviction judiciaire, garantie par la motivation et le contradictoire, ne se sous-traite pas — et c'est précisément parce que la preuve électronique est technique que son appréciation doit demeurer profondément humaine.

Conclusion

Au terme de cette étude, le diagnostic tient en une formule : le droit marocain de la preuve électronique souffre moins d'un déficit de reconnaissance que d'un déficit d'effectivité. La reconnaissance est acquise, et elle est solide : l'équivalence fonctionnelle de l'écrit électronique, la gradation des signatures issue de la loi n° 43-20, la liberté de la preuve pénale et l'arsenal des législations spéciales composent un cadre que bien des systèmes juridiques comparables pourraient envier. Mais entre ce cadre et la salle d'audience, la preuve numérique s'égare trop souvent en chemin : contestée sans pouvoir être vérifiée, produite sans pouvoir être imputée, demandée sans pouvoir être obtenue, elle déçoit les attentes que les textes avaient fait naître. Ce décalage n'a rien d'une fatalité; il est le lot des droits en transition, et l'expérience des systèmes voisins montre qu'il se résorbe par la conjonction d'une jurisprudence directrice, d'institutions outillées et de retouches législatives ciblées.

Encore faut-il ne pas se tromper de méthode. La tentation existe, devant la falsifiabilité du numérique, de durcir les conditions d'admissibilité et de réserver la force probante aux seuls procédés qualifiés; ce serait ignorer une réalité sociale qui contracte et communique massivement hors des circuits sécurisés, et transformer le droit de la preuve en privilège des acteurs équipés. La voie inverse — l'accueil indiscriminé de toute pièce numérique — sacrifierait la fiabilité à la facilité. La ligne juste est celle d'une admissibilité largement ouverte, assortie d'une appréciation exigeante et outillée de la fiabilité : que toute preuve électronique puisse franchir la porte du prétoire, mais qu'aucune n'y pèse au-delà de ce que sa qualité technique autorise, dûment vérifiée lorsqu'elle est contestée. C'est à cette pesée que juges, experts et législateur doivent, ensemble, donner les moyens d'être rendue.

Le regard comparatif conforte ce diagnostic autant qu'il rassure. Les difficultés décrites — falsifiabilité des pièces, imputabilité incertaine, expertise rare, données extraterritoriales — n'ont rien de singulièrement marocain : les juridictions françaises, européennes ou nord-américaines les affrontent chaque jour, et aucun système n'a trouvé de solution miracle. Ce que les expériences les plus abouties enseignent, c'est une méthode : traiter la preuve numérique comme une politique publique de bout en bout, qui commence par l'équipement technique de la société — identité numérique, services de confiance accessibles —, se poursuit par l'organisation de la collecte — protocoles, urgence probatoire, coopération avec les détenteurs de données — et s'achève par l'outillage du jugement — expertise, formation, doctrine jurisprudentielle. Le Maroc a déjà posé, souvent avec pertinence, les fondations normatives de chacun de ces étages; c'est leur mise en cohérence et leur mise en œuvre effective qui feront la différence dans la décennie qui s'ouvre.

La preuve, disait-on, est la rançon des droits. À l'ère numérique, elle en est devenue la condition d'existence : un droit que l'on ne peut prouver dans le monde où il est né — celui des réseaux — est un droit mort-né. En donnant à sa justice les moyens de lire, de vérifier et de peser la trace numérique, le Maroc ne fera pas seulement œuvre de modernisation

technique; il honorera la promesse constitutionnelle d'un procès équitable et d'une sécurité juridique à la hauteur de son ambition numérique.

Bibliographie

I. Textes juridiques

Code civil français, art. 1366 et s., dans leur rédaction issue de l'ordonnance n° 2016-131 du 10 février 2016; loi française n° 2000-230 du 13 mars 2000.

Constitution du Royaume du Maroc, promulguée par le dahir n° 1-11-91 du 29 juillet 2011, B.O. n° 5964 bis du 30 juillet 2011.

Convention du Conseil de l'Europe sur la cybercriminalité, Budapest, 23 novembre 2001, et son deuxième protocole additionnel relatif au renforcement de la coopération et de la divulgation des preuves électroniques (2022).

Dahir du 9 ramadan 1331 (12 août 1913) formant code des obligations et des contrats, tel que modifié et complété, notamment par la loi n° 53-05.

Loi n° 53-05 relative à l'échange électronique de données juridiques, dahir n° 1-07-129 du 30 novembre 2007, B.O. n° 5584 du 6 décembre 2007.

Loi n° 43-20 relative aux services de confiance pour les transactions électroniques, dahir n° 1-20-100 du 31 décembre 2020, B.O. n° 6951 du 14 janvier 2021.

Loi n° 22-01 relative à la procédure pénale, dahir n° 1-02-255 du 3 octobre 2002, telle que modifiée et complétée.

Loi n° 07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données, dahir n° 1-03-197 du 11 novembre 2003, B.O. n° 5171 du 22 décembre 2003.

Loi n° 03-03 relative à la lutte contre le terrorisme, dahir n° 1-03-140 du 28 mai 2003, B.O. n° 5112 du 29 mai 2003.

Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, dahir n° 1-09-15 du 18 février 2009, B.O. n° 5714 du 5 mars 2009.

Loi n° 05-20 relative à la cybersécurité, dahir n° 1-20-69 du 25 juillet 2020, B.O. n° 6898 du 30 juillet 2020.

Loi n° 31-08 édictant des mesures de protection du consommateur, dahir n° 1-11-03 du 18 février 2011, B.O. n° 5932 du 7 avril 2011.

Loi n° 15-95 formant code de commerce, dahir n° 1-96-83 du 1er août 1996, B.O. n° 4418 du 3 octobre 1996.

Loi n° 103-12 relative aux établissements de crédit et organismes assimilés, dahir n° 1-14-193 du 24 décembre 2014, B.O. n° 6328 du 22 janvier 2015.

Loi n° 55-19 relative à la simplification des mesures et des procédures administratives, dahir n° 1-20-06 du 6 mars 2020, B.O. n° 6866 du 19 mars 2020.

Loi type de la CNUDCI sur le commerce électronique (1996) et loi type de la CNUDCI sur les signatures électroniques (2001).

Règlement (UE) n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance (« eIDAS »), modifié par le règlement (UE) 2024/1183 du 11 avril 2024.

Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD).

II. Ouvrages

مجلة علمية معتمدة دوليا و محكمة تصدر عن مختبر البحث قانون الأعمال - جامعة الحسن الأول - سطات - المغرب

الإميل الرسمي : MForKi22@Gmail.com الموقع الرسمي : WWW.Droitentreprise.com

CAPRIOLI (É. A.), Signature électronique et dématérialisation, LexisNexis, Paris, 2014.

FÉRAL-SCHUHL (C.), Cyberdroit. Le droit à l'épreuve de l'internet, Dalloz, Paris, éd. la plus récente.

TERRÉ (F.), Introduction générale au droit, Dalloz, coll. « Précis », Paris, éd. la plus récente.

Travaux et publications de la Revue marocaine d'administration locale et de développement (REMALD), séries « Textes et documents » et « Thèmes actuels », relatifs au commerce électronique et à la modernisation du droit de la preuve.

III. Ressources institutionnelles et électroniques

Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), délibérations et guides, www.cndp.ma.

Conseil de l'Europe, Comité de la Convention sur la cybercriminalité (T-CY), rapports et lignes directrices sur la preuve électronique, www.coe.int.

Direction générale de la sécurité des systèmes d'information (DGSSI), publications relatives aux services de confiance et à la cybersécurité, www.dgssi.gov.ma.

Portail juridique et judiciaire du ministère de la Justice du Royaume du Maroc, www.mahakim.ma.

Secrétariat général du gouvernement du Royaume du Maroc, Bulletin officiel, www.sgg.gov.ma.