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

DOI : 10.5281/zenodo.11518517– Vol.4, N° 12- 1ère trimistre 2023

L'ADMINISTRATION DE LA PREUVE NUMERIQUE EN MATIERE DE LUTTE CONTRE LA CYBERCRIMINALITE.

THE ADMINISTRATION OF DIGITAL EVIDENCE IN THE FIGHT AGAINST CYBERCRIME.

Abdellatif MARDDI

Conseiller à l'Ambassade du Maroc à Tunis

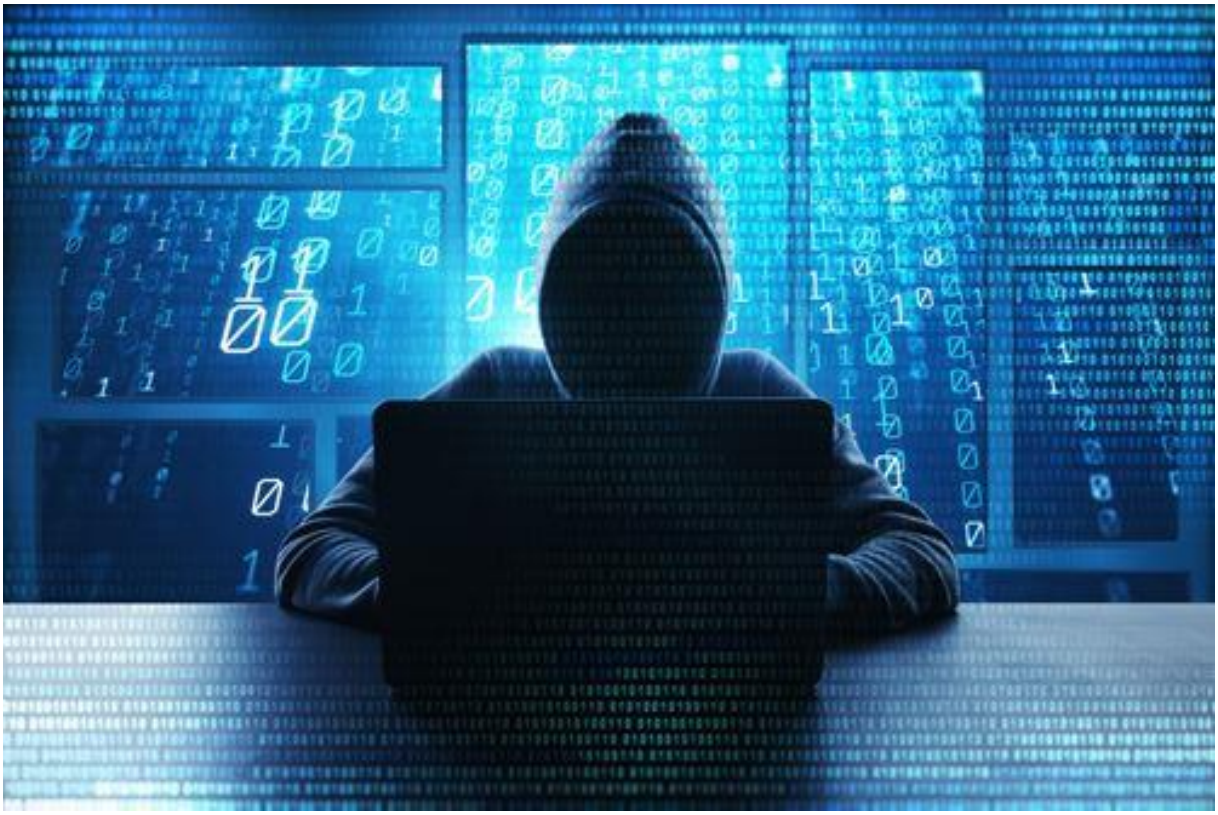
Doctorant en sciences juridiques

Université Mohamed V, Rabat, Maroc

Rights

Citation:
MARDDI, A. (2024). L'ADMINISTRATION DE LA PREUVE NUMERIQUE EN MATIERE DE LUTTE CONTRE LA CYBERCRIMINALITE. REVUE DROIT ET SOCIETE, 5(12), 55-74. https://doi.org/10.5281/zenodo.11518517

L'ADMINISTRATION DE LA PREUVE NUMERIQUE EN MATIERE DE LUTTE CONTRE LA CYBERCRIMINALITE



REVUE DROIT & SOCIETE
N° 12 JANVIER / MARS 2023

Abdellatif MARDDI

Doctorant en sciences juridiques

Université Mohamed V, Rabat, Maroc

RESUME

Dans la conjoncture actuelle, marquée par une évolution fulgurante des nouvelles technologies d'information de communication, la criminalité informatique se trouve de plus en plus confrontée à la justice pénale.

Cette évolution, qui a marqué la vie économique du fait de la mondialisation n'a pas manqué de provoquer des changements tous azimuts, surtout au niveau du droit applicable. En effet, le passage de l'analogique au numérique, annonce en réalité l'avènement d'un nouveau mode de preuve en l'occurrence la preuve numérique.

Nous essayerons dans cette étude de jeter la lumière d'abord sur la notion de la preuve numérique, pour s'attarder ensuite sur la recevabilité et l'évaluation de celle-ci par la juridiction pénale.

Mots clés : Preuve numérique, criminalité informatique, recevabilité, loyauté, pouvoir discrétionnaire.

THE ADMINISTRATION OF DIGITAL EVIDENCE IN THE FIGHT AGAINST CYBERCRIME

Abdellatif MARDDI

PhD student in Private Law

Mohamed V University -Rabat, Morocco

ABSTRACT

In the current situation, marked by a dazzling evolution of new information and communication technologies, computer crime is increasingly confronted with criminal justice.

This development, which has marked economic life due to globalization, has not failed to cause major upheavals, both in terms of communication on a global scale and in terms of applicable law. Indeed, the transition from analog to digital actually announces the advent of a new mode of proof, in this case digital proof.

In this study, we will try to shed light first on the notion of digital evidence, then focus on its admissibility and its evaluation by the criminal jurisdiction.

Keywords: Digital evidence, computer crime, admissibility, loyalty, discretionary power.

INTRODUCTION

La notion de preuve qui implique la démonstration de la réalité d'un fait ou d'un droit, occupe une place essentielle dans l'ensemble des domaines de droit, y compris le droit pénal, dont le rôle est de déterminer la commission d'une infraction et d'identifier son auteur.

Cependant, l'évolution de la technologie a radicalement transformé le paysage de la preuve, notamment en introduisant des éléments de preuves sous forme de documents numériques ou de données stockées. Cette mutation de l'analogique au numérique a donné naissance, en droit pénal, à la notion de la preuve numérique.

La preuve numérique, qui de plus en plus invoquée devant les juridictions, a soulevé, eu égard de sa nature volatile et immatérielle, des problèmes quant à sa recevabilité et à son évaluation par le juge pénal.

A travers cette contribution, notre objectif sera de jeter la lumière sur la question de la preuve numérique en matière de lutte contre la criminalité informatique. Un premier axe sera consacré à la recevabilité de la preuve numérique, et un deuxième traitera la question de l'évaluation de la preuve numérique par le juge pénal.

I- La recevabilité de la preuve numérique.

Pour qu'elle soit recevable en matière pénale, la preuve numérique doit remplir un certain nombre de conditions ayant trait à sa loyauté, son authenticité et son intégrité. Mais il y a d'abord de clarifier cette notion de preuve numérique.

A- Notion de preuve numérique.

La révolution technologique, marquée par la montée en puissance des nouvelles technologies d'informations et de communications, a favorisé le passage de l'analogique au numérique. Ce progrès dans le secteur de l'informatique n'a pas conduit seulement à l'apparition de nouvelles formes de comportement criminel, mais a généré également l'émergence d'un nouveau type de preuves connues sous l'appellation de preuves numériques.

L'expression « preuve numérique » n'a pas explicitement été utilisée par le législateur marocain, en tout cas pas dans les Codes pénal et de procédure pénale. Le constat en est que, en évoquant les éléments de preuves, le législateur utilise souvent l'expression « données informatiques ».

La notion de la preuve numérique a fait l'objet d'une controverse doctrinale, puisque chaque auteur ou chaque système juridique, a une définition propre de la preuve numérique, c'est ce qui explique l'existence d'une pluralité de définitions.

Portant, la preuve numérique peut être définie comme « une démonstration qui associe un ou plusieurs éléments de nature numérique et un raisonnement »[1]. Il s'agit de « tout élément ou information numérique pouvant être utilisée dans une affaire de type judiciaire »[2]. Elle est définie également comme « une modalité particulière de l'établissement de la vérité qui consiste à avoir recours à des moyens numériques variés qui vont de l'étude des contenus dans la mémoire d'un disque dur, aux messages électroniques en passant par l'enregistrement numérique »[3].

Il s'agit aussi « d'une preuve extraite d'ordinateurs, qui se présente sous forme de champs ou impulsions magnétiques ou électriques, qui peuvent être collectées et analysées à l'aide de programmes et d'applications technologiques et qui seront ensuite présentées sous forme de preuve devant la justice »[4].

Selon une autre définition, la preuve électronique « n'est rien d'autre qu'une information acceptée par la raison et la logique et approuvée par la science. Elle est obtenue grâce à des procédures scientifiques et juridiques en traduisant les informations et données stockées dans l'ordinateur, ses périphériques et les réseaux de communication. Elle peut être utilisée à chaque stade du

[1] Marylou Garcias et Max Chouzier, « la preuve informatique –quelles nouveautés techniques pour quelles évolutions juridiques ? », Lexbase, Revues n° 280 du 18 janvier 2012.

[2] Article intitulé « La preuve numérique : Approche juridique », disponible sur l'adresse suivante : https://www.advisecurity.com/la-preuve-numerique-approche-juridique/ .

[3] Contribution de madame Mélanie CLEMENT-FONTAINE, in colloque sous thème «La preuve numérique à l'épreuve du litige », organisé le 13 avril 2010 à la première chambre de la cour d'appel de Paris. Disponible à : https://search.app.goo.gl/mZKfPAV

[4] ممدوح عبد الحميد عبد المطلب : البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والأنترنت، دار الكتب القانونية، مصر، 2006، ص 88.

procès pour prouver la véracité d'un acte ou d'une chose liée au crime »[5].

On constate que les définitions précédentes se limitaient pour la plupart, à la notion de preuve numérique extraite principalement d'ordinateur, sans prendre en considération les autres sources telles que les Smartphones, les tablettes, les disquettes, les cartes mémoires et toute autre appareil numérique, qui pourrait être la source de cette preuve. Cependant, ces définitions convergent, pour la plupart, vers un élément unique et commun, à savoir l'utilisation de l'informatique, laquelle permet de faire la distinction entre la preuve numérique et la preuve traditionnelle.

De ce qui précède, la preuve électronique peut être définie comme la trace numérique laissée par une infraction informatique ou tout autre crime, qu'elle soit obtenue d'un ordinateur, d'un Smartphone ou de tout autre appareil électronique, et qui permet de prouver la commission d'un délit électronique et l'identification de son auteur[6].

La preuve électronique peut prendre de nombreuses formes, tels les courriels, les SMS, les fichiers multimédia (photos, enregistrements audio et les vidéos), des documents électroniques, des données de transaction...etc. Elle est de plus en plus courante dans les procédures judiciaires.

Par rapport à la preuve physique, la preuve numérique a des caractéristiques très distinctes[7]. Ainsi, outre l'intangibilité et la virtualité, la preuve numérique est :

- **Prolifique** : les preuves électroniques peuvent être réduites facilement, et la copie ou la duplication peut présenter exactement le même contenu que l'original. Donc, la preuve électronique est relativement facile à présenter par les parties devant une juridiction et à être conservée par celle-ci.
- **Persistante** : contrairement au papier, la preuve électronique ne va ni s'abîmer, ni se décomposer, ni moisir avec le temps. Finalement elle a plus d'avantage du point de vue de la conservation.
- **Omniprésente** : surtout dans le commerce électronique, la preuve électronique est la preuve principale, et on peut la retrouver presque dans toutes les étapes du commerce électronique. Donc, la reconnaissance et l'admission de la preuve électronique va conditionner la prospérité du commerce électronique.

Bien que le document informatique contraste par son mode d'établissement avec l'écrit, tel que le préconise le droit positif, il n'en faudrait pas moins assumer ce choix d'informatisation, et réserver aux supports informatiques la place qu'ils méritent parmi les moyens de preuve.

Il reste, à cet égard, de déterminer les critères de la recevabilité de la preuve électronique en matière pénale.

[5] محمد أمين البشري : التحقيق في الجرائم المستحدثة، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004، ص 234.

[6] ياسين زوباير : قصور الدليل الالكتروني الجنائي في إثبات الجريمة الالكترونية، رسالة لنيل دبلوم الماستر المتخصص، كلية العلوم القانونية والاقتصادية والاجتماعية سلا، 2013-2014.

[7] Peihao Yuan, « l'admission de la preuve électronique dans le droit français et le droit chinois ». Voir : http://blogs.u-paris10.fr/content

REVUE DROIT & SOCIETE
N° 12 JANVIER / MARS 2023

B- Les conditions de recevabilité de la preuve numérique.

A la différence du droit civil qui inscrit la constitution de la preuve dans un ensemble d'obligations légales et contractuelles[8], le droit pénal consacre une liberté relative de la production de la preuve. Ainsi, l'article 286 du C.P.P dispose que « *les infractions peuvent être établies par tout mode de preuves, hors le cas où la loi en dispose autrement...* ». C'est à dire que la preuve d'un fait ou d'un droit, en matière pénale, « peut être apportée par tout moyen, sans qu'une preuve ne prévale sur l'autre ou que le juge ne soit lié à l'une plutôt qu'à l'autre »[9].

On peut avancer que le principe de la liberté de preuve reste le plus approprié en matière d'infractions informatiques, en raison de l'incapacité des moyens classiques de preuve à en faire face.

Par ailleurs, l'entrée en vigueur de la loi n° 53-05 relative à l'échange électronique de données juridiques, a constitué une reconnaissance par le législateur civil de la valeur probante de l'écrit sur support électronique, en l'assimilant à l'écrit sur support papier, sous réserve de l'identification de la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité[10]. Reste à savoir si la liberté de la preuve en matière pénale permet aux juges de prendre en considération les preuves électroniques.

Au regard du principe de la liberté de la preuve en matière pénale posé par l'article 286 du C.P.P, la preuve numérique est parfaitement admise par les juges marocains qui l'incluent même dans la motivation de leurs décisions, comme en témoignent plusieurs arrêts et jugements judiciaires. Ainsi, il a été précisé dans un jugement rendu par le Tribunal de Première Instance de Marrakech[11] qu' « attendu que la dénégation de l'accusé devant le tribunal du fait qui lui a été reproché, est réfutée par ses déclarations préliminaires devant la police judiciaire et par les différentes photos et vidéos extraites de son compte Facebook ».

Une autre décision de la Cour d'appel de Rabat[12] précise que : « la dénégation de l'accusé est réfutée par le matériel électronique saisi en sa possession (quatre disques durs et sept CD), chose qui confirme son implication dans le crime qui lui est reproché ». De même, un jugement du tribunal de première instance de Kelaâ Sraghna[13] précise que : « attendu qu'il a été prouvé au tribunal, à travers les éléments du dossier, en particulier le CD faisant objet de la plainte, qu'il contient des séquences vidéo de la plaignante. Attendu que le tribunal est convaincu, sur la base de ce qui précède, qu'il existait plusieurs preuves solides confirmant le délit de participation à l'exploitation des CD vidéo,

[8] Article 9 du code de procédure civile.

[9] S. Grunvald et J. Danet, « la preuve pénale », cours archivé, Université de Nantes. Disponible à l'adresse : https://cours.unjf.fr/

[10] Article 417-1 du D.O.C marocain.

[11] حكم ابتدائي عدد 4، الصادر عن المحكمة الابتدائية بمراكش بتاريخ 2012/01/02، ملف جنحي تلبسي عدد 11/2103/38323، حكم غير منشور.

[12] القرار عدد 364، صادر عن محكمة الإستئناف بالرباط ملحقة حي السلام بسلا، بتاريخ 2006/04/17، في الملف عدد 22/05/740، ص 12 غير منشور، مشار إليه عند إيمان الريشي، إثبات الجرائم الإلكترونية وإشكالاته العلمية، بحث نهاية تكوين المعهد العالي للقضاء، 2015، ص47.

[13] حكم ابتدائي غير مشار إلى عدده، صادر عن المحكمة الإبتدائية بقلعة السراغنة بتاريخ 2011/12/09، في ملف جنحي عادي عدد 2010/400، حكم غير منشور.

comprenant des scènes contraires aux bonnes mœurs, à des fins commerciales, sans autorisation du Centre Cinématographique Marocain». Cette approche a été confirmée par la décision de la Cour suprême (actuelle Cour de cassation) numéro 204 en date du 3 mars 2011, dossier n° 416/6/8/2011.

Il reste à savoir les différentes règles qui encadrent la conviction du juge pénal en termes de recevabilité de la preuve électronique. Dans ce sens, le juge pénal, et avant de procéder à l'évaluation des preuves, doit d'abord s'assurer que celles-ci respectent les principes de loyauté, d'authenticité et d'intégrité.

1- La loyauté de la preuve numérique.

La notion de loyauté constitue une importante limitation à la libre recherche des preuves. Il s'agit par ce biais, d'assurer la correction des poursuites judiciaires et de tempérer l'action des organes répressifs. L'infraction peut être démontrée par tout moyen, fait ou objet, dans la mesure où les droits de la défense et de l'accusé sont respectés[14]. La doctrine la conçoit comme « une manière d'être de la recherche de la preuve conforme au respect des droits de l'individu et à la dignité de la justice »[15].

La condamnation de tout délit requiert donc qu'elle soit fondée sur des preuves légitimes, recueillies dans le respect de la loi. Par conséquent, le principe de la loyauté pour les délits informatiques exige que la preuve soit obtenue conformément aux prescriptions légales. Autrement dit, toute preuve obtenue en violation d'un droit fondamental de l'accusé est réputée nulle et ne peut être invoquée en aucun stade du procès pénal.

En effet, l'OPJ ne peut utiliser, dans le cadre d'une enquête judiciaire, ni provocations, ni ruses ni stratagèmes, sauf si ces derniers sont prévus par la loi, car ces manœuvres portent atteinte à la présomption d'innocence. Or, dans certaines infractions pour lesquelles la preuve numérique s'avère difficile à constituer, des enquêteurs s'adonnent à toute sorte de pratique pouvant parfois être qualifiées de détournements de procédure.

Une preuve numérique est donc recevable devant une juridiction pénale lorsqu'elle a été recueillie dans les conditions de légalité, c'est-à-dire lorsque le principe de loyauté et de dignité[16] ont été rigoureusement observées par les enquêteurs. Il nécessaire donc d'opérer un équilibre entre la légitimité de constituer une preuve et le respect des libertés individuelles et collectives des personnes.

Quant au juge pénal, il est tenu de s'assurer que la procédure, ayant abouti à la collecte des éléments de preuve, respecte les exigences de loyauté. En

[14] P. VERGUCHT, « La répression des délits informatiques dans une perspective internationale », thèse en droit, Montpellier, 1996, p.432.
Il faut noter toutefois que la liste des moyens de preuves recevables qui existent parfois, comme en Allemagne et aux Pays-Bas, sont en fait très largement interprétés par les juges.

[15] P. Bouzat, « La loyauté dans la recherche des preuves », Mélanges Hugueney, 1964, p. 155

[16] Le principe de dignité renvoie à l'absence d'emploi de la violence par les agents enquêteurs au moment de la collecte des éléments de preuve.

effet, seul les preuves régulièrement obtenues peuvent être utilisées par le juge pénal comme fondement de sa décision, car si la preuve est libre, son administration ne l'est pas. Autrement dit « les preuves obtenues directement ou indirectement en violation des droits fondamentaux n'ont pas d'effet juridique »[17]. C'est ainsi que la jurisprudence, à son tour, précise que « les preuves obtenues en violation des droits fondamentaux ne doivent pas être appréciées par la Cour»[18].

Ce principe de loyauté de la preuve est donc valable tant pour les enquêteurs que pour les magistrats[19]. A défaut du respect de ce principe, les éléments de preuves recueillis seront frappés de nullité[20].

2- Authenticité et intégrité de la preuve numérique.

Le but des services de police étant de prouver l'infraction. Les officiers de police seront souvent amenés à remonter la chaîne des opérations informatiques dans le sens inverse pour découvrir la démarche logique du délit informatique. Cependant, les preuves électroniques peuvent être porteuses de risque car elles peuvent être plus ou moins facilement altérées, supprimées ou falsifiées.

Pour avoir une valeur probante, l'information numérique doit présenter des garanties spécifiques telles que l'intégrité et l'authenticité. On entend par authenticité, le phénomène où pourra être remis en cause, l'origine du document informatique. L'intégrité quant à elle renferme l'hypothèse où le contenu de l'information n'a pas été modifié.

Afin de préserver l'authenticité des données récupérées, les autorités chargées de l'enquête doivent doubler de vigilance entre le moment où les données ont été captées et celui où elles seront utilisées à l'audience. Par conséquent, il est nécessaire, avant de manipuler le support informatique, de calculer « l'empreinte numérique » sur l'intégralité des données qui s'y trouvent à l'aide d'un algorithme mathématique de «hash », notamment « l'algorithme MD5 », qui permet d'attribuer à un fichier une chaîne de caractères unique. Quand le fichier est modifié, même très légèrement, son empreinte numérique change complètement. D'effectuer ensuite une copie intégrale, bit par bit, dudit support, y compris les données supprimées[21].

A ce stade, se pose la question de la fiabilité de la copie, sachant que les preuves sont souvent présentées devant la justice sous forme de documents imprimés ou affichés sur un écran d'ordinateur. Autrement dit, la preuve électronique conserve-t-elle son caractère dématérialisé même si elle est copiée et transformée sous forme d'une preuve ordinaire, c'est-à-dire imprimée sous forme de papier tangible?

[17] Article 11.1 de la loi judiciaire espagnole de 1985.
[18] Arrêt la cour espagnole n° 3943/1990 du 24 mai 1990.
[19] Cass. crim., 12 juin 1952, Bull. n° 153
[20] L'article 751 du C.P.P. stipule que «Toute formalité édictée par le présent Code dont l'accomplissement n'a pas été régulièrement constaté, est présumée n'avoir pas été accomplie».
[21] Jean-François TYRODE, « Eléments de procédure pénale dans le cadre de l'atteinte aux personnes par la cybercriminalité endroit européen », MASTER Droit de l'Internet Public - Administration - Entreprises, Année Universitaire 2006 - 2007.

Une partie de la doctrine[22] considère que la preuve électronique n'est pas une preuve tangible, mais de nature virtuelle, qui nécessite un environnement compatible à sa nature technique. Selon cette doctrine, il n'y a pas de preuve numérique en dehors de son environnement technique ou numérique.

Les données sont considérées, dans la plupart des juridictions, comme une forme particulière de preuve écrite. Les documents classiques (papiers) se présentent traditionnellement sous trois dimensions, un support matériel (généralement en papier), un contenu sémantique (généralement un texte) et une signature (généralement manuscrite). Les liaisons entre le support, le texte et la signature sont évidentes. Les signes d'authenticité des documents papier proviennent normalement d'une signature écrite : le destinataire fait confiance à l'identité de l'expéditeur et au caractère original du texte.

Par contre, les documents informatiques ne présentent pas une telle liaison entre le support, le contenu et la signature. Les données électroniques ne sont pas fixées de façon permanente (verrouillées) sur le support de stockage, les informations qu'elles véhiculent sont facilement modifiables sans attaque matérielle décelable. Sans que leur forme antérieure soit toujours récupérable (mais elle l'est parfois), les signatures sont difficiles à attacher à un contenu ou à une personne et témoignent encore moins facilement d'une absence de modification[23].

L'altération d'un document papier doit adopter la forme d'une agression matérielle discernable sur l'objet physique, alors que l'altération de données n'est cependant pas détectable à l'œil nu, elle consiste souvent en des modifications, à peine impossible à reconstituer, d'un arrangement de bits qui peut avoir lieu, par exemple, pendant une transmission sur réseau[24].

Les juges seront confrontés à l'appréciation de l'authenticité des preuves électroniques surtout avec l'évolution permanente des NTIC. L'attestation du fait qu'un document informatique provient bien de l'individu qu'on qualifie comme son auteur et du fait que son contenu est bien celui qu'existait à l'origine, peut être compliquée.

Certes, les tribunaux, dans la recherche de la vérité ne peuvent fonder leurs décisions que sur des informations sûres et dûment vérifiées, surtout lorsqu'il y a risque de sanction pénale et privative de liberté. A titre d'exemple, une impression d'écran est une preuve admissible par un juge, mais insuffisante pour donner lieu à une condamnation, surtout lorsqu'il est contesté par la partie adverse. Il arrive parfois que le tribunal se trouve contraint d'écarter des pièces produites sous forme d'impression d'écran, dès lors que l'adresse URL qui figurait en bas de page était incomplète, que l'impression d'écran ne mentionnait pas

[22] خالد ممدوح إبراهيم : الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية، الطبعة الأولى، السنة 2009، ص 180 وما بعدها.

[23] P. VERGUCHT, op. cit note (14), p. 441.

[24] Conseil de l'Europe: «Problèmes de procédure pénale liés à la technologie de l'information», Recommandation nº R(95) 13, septembre 1995, p. 64, n° 154.

la date de sa réalisation, etc. La raison de cette exclusion des preuves réside dans la possibilité technique de modifier la page offline, voire d'imprimer une copie de la page litigieuse qui était présente dans la mémoire cache de l'ordinateur[25].

Il est très important que la preuve soit hors de doute, pour que le juge puisse en servir pour statuer, car il n'y a pas lieu d'écarter le principe de la présomption d'innocence et supposer le contraire, sauf si la conviction du juge atteint la certitude.

Dans ce sens, la Cour de cassation a souligné dans plusieurs arrêts la nécessité que la preuve soit fondée sur le principe de certitude, précisant que « les jugements doivent être fondés sur la certitude et non sur le doute et la conjecture, et à cette fin, toute décision de condamnation sera cassée, alors que le tribunal a déclaré qu'il ne disposait d'aucune preuve matérielle certaine pour prouver le crime »[26]. La Cour de cassation indique également que « les décisions pénales de condamnation doivent être certaines et fondées sur des faits présentés devant le tribunal et étayés par des moyens de preuve certains », précisant que « si le juge pénal est libre de fonder sa conviction sur les différents moyens de preuve dont il dispose, ces preuves doivent être solides, exemptes d'ambiguïté et déduites de faits établis et d'informations certaines,… »[27].

À côté de l'authenticité, **l'intégrité** des preuves numériques pourra être mise en cause, et une attention particulière devra alors être portée à l'état matériel du support de données lors de son acquisition, de son examen et de sa conservation par les autorités judiciaires. Il est donc indispensable d'assurer l'intégrité des preuves électroniques en vue de leur production devant la justice. Sinon, la moindre anomalie détectée par la défense causera le rejet de cet élément de preuve, voire tous les actes subséquents.

Ainsi, il est souvent nécessaire de remonter **la chaîne de la preuve** afin de connaitre l'environnement initial, les conditions de saisie ainsi que les conditions de conservation de la preuve, car « un disque dur saisi dans une affaire judiciaire n'a réellement de sens que si l'on sait quelle était la configuration de l'ordinateur dans lequel il a été saisi, la personne à qui il pouvait appartenir, et on ne pourra garantir l'intégrité de son contenu que s'il a été convenablement protégé de toute modification extérieure entre le moment de sa saisie et le moment de l'analyse par un spécialiste. Sans cela, l'avocat de la défense pourra très

[25] Sur la question de la preuve par capture d'écran, voir J .-M. Léger, « Les captures d'écran : moyens de preuve des utilisations illicites de créations sur Internet », Village de la Justice, 20 mars 2023, https://www.village-justice.com/articles/les-captures-ecran-moyens-preuve-des-utilisations-illicites-creations-sur,40233.html

[26] القرار الجنائي عدد 49 الصادر في 19 نونبر 1970، منشور بمجلة قضاء المجلس الأعلى، عدد 20-1970، ص 32-33.

[27] قرار المجلس الأعلى عدد 8/474 المؤرخ في 2001/01/25، ملف جنحي عدد 00/7908، منشور بمجلة قضاء المجلس الأعلى، العدد المزدوج 57 و 58، السنة 23 يوليوز 2001، ص 419 مشار إليه في الناجم كوبان، الإثبات الجنائي في الجرائم المعلوماتية، بحث لنيل دبلوم الماستر في القانون الخاصة، جامعة محمد الخامس أكدال، 2010-2011، ص 140.

raisonnablement rejeter les conclusions tirées à partir de cet objet »[28].

La traçabilité de la preuve électronique met en exergue le fait que le procédé technique de la collecte des données doit permettre d'établir les différentes opérations techniques qui ont pu être réalisées jusqu'à la conservation des éléments de preuves. Le but est de permettre la validité des éléments de preuve numérique et aussi d'éviter à la partie qui les a produits d'être confrontée à une contestation du camp adverse.

Afin de garantir l'intégrité des preuves électroniques, on peut recourir à des techniques spéciales telles que l'utilisation de scellements électroniques, d'empreintes numériques, de l'expertise ou de la signature électronique. Cette dernière est un dispositif juridique fiable, mais malheureusement, dans la pratique, l'information numérique signée électroniquement reste très minoritaire.

Au-delà du droit, il est aussi pertinent de s'intéresser aux technologies qui seraient à même d'offrir des améliorations quant à l'intégrité et la fiabilité de la preuve numérique. Tel est le cas de la « blockchain »[29] qui semblerait ouvrir des perspectives pouvant permettre de démocratiser le concept de preuve numérique[30]. La blockchain présente de nombreux avantages en matière de preuve comme la transparence, la sécurité, la rapidité, la dimension internationale, la confidentialité. La preuve, étant simultanément inscrite sur les différents nœuds du réseau, peut, en effet, être vérifiée à tout moment. Finalement, ces conditions de loyauté, d'authenticité et d'intégrité ont un double but : D'une part, permettre à la preuve numérique d'affirmer sa validité en résistant à la contestation, et d'autre part, à une partie de disposer de moyens valables de la contester.

Par ailleurs, lorsque les enquêteurs ont pu collecter les traces numériques et que les poursuites ont été actionnées, il s'observera une pratique juridictionnelle qui consistera pour le juge d'apprécier à la lumière de la loi et de son intime conviction les différents éléments de la procédure qui lui ont été communiquées : c'est la phase dite de l'appréciation du juge.

II- L'appréciation de la preuve électronique par le juge pénal.

La phase du jugement est considérée comme l'étape fondamentale du procès pénal, car c'est au cours de celle-ci que le juge pénal évalue les preuves pour décider soit de la culpabilité ou de l'acquittement de l'accusé. Il ne fait aucun doute que la préoccupation majeure de la justice pénale dans son rapport avec la preuve pénale, qu'elle soit physique ou électronique, reste la manifestation de la vérité, mais la question d'acceptation des données issues d'un environnement électronique comme moyen de preuve, est la situation qui inquiète encore le pouvoir judiciaire, en raison de la possibilité que ces preuves, en raison de leur

[28] Eric OK, « La preuve numérique : Un défi pour l'enquête criminelle du 21e siècle », in les Cahiers du numérique 2003/3 (Vol. 4), p 209.

[29] Selon la définition de Blockchain France, il s'agit d'une « technologie de stockage et de transmission d'informations, transparente, sécurisée et fonctionnant sans organe de contrôle ».

[30] S. Canas, « Blockchain et preuve : le point de vue du magistrat », Dalloz IP/IT, févr. 2019, p. 82.

nature virtuelle, soient altérées ou falsifiées[31].

Dès lors, la question qui se pose à cet égard est la suivante : quelles sont les limites du pouvoir du juge pénal dans l'évaluation des preuves électroniques ? La nature de la preuve électronique, en tant que preuve scientifique ayant une valeur probante susceptible d'être irréfutable, a-t-elle un impact sur le pouvoir discrétionnaire du juge pénal ?

Pour répondre à ces questions, nous avons décidé de diviser ce paragraphe comme suit :

A- Le pouvoir discrétionnaire du juge pénal.

Le pouvoir discrétionnaire du juge pénal est l'un des principes de base sur lesquels repose le système de preuve pénale. Il octroi au juge un large pouvoir d'évaluation de la valeur probante de l'ensemble des preuves qui lui sont soumises[32], afin de prononcer par la suite, soit l'acquittement ou la condamnation de l'accusé.

Si le pouvoir discrétionnaire du juge ne pose pas de problèmes en ce qui concerne l'appréciation de la preuve traditionnelle, ce n'est pas le cas pour la preuve électronique, qui évoque, en tant que preuve scientifique, la question de l'étendue du pouvoir du juge pénal.

Afin de parvenir à la vérité, le juge pénal jeue un rôle important par son action positive à la lumière du principe de l'intime conviction, qui repose sur le fait que le juge est libre d'évaluer les preuves qui lui ont été présentées sans aucune restriction autre que celle de tenir compte de son devoir judiciaire[33].

En droit pénal marocain, basé sur le système de preuve morale, les éléments de preuve, recueillis par l'information, sont librement et souverainement appréciés par le juge qui, selon l'article 286 du C.P.P., « décide d'après son intime conviction ». S'il subsiste un doute dans son esprit sur la culpabilité de la personne poursuivie, ce doute doit, aux termes de l'article 1er du C.P.P, être « Interprété en faveur de l'accusé ». C'est la maxime in dubio pro reo, corollaire de la présomption d'innocence[34].

Pour dire le droit, le juge ne peut se fonder uniquement sur les procès-verbaux des officiers de police judiciaire pour condamner l'intéressé, mais également sur les preuves rapportées par les parties au procès pénal, conformément au principe du contradictoire, qui impose au juge de ne prendre en considération dans sa décision que des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui[35]. Ainsi, toute preuve, qu'elle soit électronique ou physique, doit être soumise à la discussion et présentée au juge afin que sa conviction soit absolue et dépourvue de tout doute.

[31] رشيدة بوكر : الدليل الالكتروني و مدى حجيته في الإثبات الجنائي في القانون الجزائري ، مجلة جامعة دمشق للعلوم الاقتصادية و القانونية، المجلد 29، العدد الثاني، 2011، ص 31.

[32] Arrêt de la Cour de Cassation n° 1280 en date du 30/12/2015, dossier n° 5808/6/5/2015.

[33] احمد فتحي سرور : الوسيط في قانون الإجراءات الجنائية ، الطبعة السابعة ، دار النهضة العربية ، 1996، ص 747.

[34] Mohammed Jalal ESSAID, « le procès équitable dans le code de la procédure pénale de 2002 », 1èr édition, 2008, p145-157.

[35] Koulika Arnaud NIKIEMA, « La preuve dans le contentieux du cyberespace », mémoire Master, Université Gaston Berger de Saint Louis (Sénégal), 2010-2011.

Le principe du contradictoire est édicté par l'article 287 du C.P.P qui dispose que « La juridiction ne peut fonder sa décision que sur des preuves versées aux débats et discutées oralement et contradictoirement devant elle ». C'est au terme de la discussion qu'intervient donc le pouvoir discrétionnaire du juge pénal, qui apprécie souverainement les preuves de chaque partie[36].

Ce principe est confirmé également par la Cour de cassation, qui précise qu'« en vertu de l'article 287 du C.P.P, le juge ne peut fonder sa décision que sur des preuves versées aux débats publiques et discutées devant lui oralement et contradictoirement. Sinon, sera cassée toute décision fondée sur des connaissances personnelles du juge, inspirées d'une affaire qu'il a instruit auparavant »[37].

Si le juge est libre d'apprécier une preuve électronique, il ne peut pas la rejeter au seul motif qu'elle est numérique, selon le principe de neutralité et de non-discrimination. Mais il peut, s'il n'est pas convaincu, la rejeter à condition de motiver sa décision[38]. C'est là que l'expert intervient pour montrer au juge le degré de fragilité des preuves numériques, et lui laisse la décision de déterminer leur valeur probante. A titre d'exemple, pour une intrusion frauduleuse dans un système informatique, commise au moyen d'un programme malveillant, l'appréciation du juge va dépendre de la possibilité que lui offre l'expert de voir concrètement le fonctionnement du virus.

Toutefois, les juges ne sont pas obligés de prendre en considération les rapports des experts qui peuvent parfois se révéler erronés. Ils peuvent dans ce cas ordonner ou autoriser une contre-expertise pour s'assurer de l'absence de contradiction technique.

Par ailleurs, la nature scientifique des preuves électroniques **stockées**, tels les fichiers LOG[39] et les fichiers journaux[40], pose la question de savoir dans quelle mesure le juge est tenu de les prendre en compte, sachant que leur valeur est déjà tranchée scientifiquement. On peut avancer que malgré la force probante décisive dont jouit la preuve scientifique, le juge pénal a le droit de l'apprécier à la lumière des conditions et circonstances dans lesquelles elle a été collectée. Le juge doit donc tenir compte, lors de son évaluation de la preuve électronique en tant que preuve scientifique, de deux choses, à savoir sa valeur scientifique irréfutable et les conditions et les circonstances dans lesquelles elle a été collectée.

Or, nous pensons que la même preuve, compte tenu de sa nature électronique, reste également incertaine en raison de la possibilité d'être falsifiée ou

[36] عبد الحكيم الحكماوي : الإثبات في الجريمة الالكترونية ، سلسلة ندوات محكمة الاستئناف بالرباط ،تأثير الجريمة الالكترونية على الائتمان المالي، العدد السابع، مطبعة الأمنية ، الرباط، 2014، ص 158.

[37] القرار الجنائي عدد 49 الصادر في 19 نونبر 1970، منشور بمجلة قضاء المجلس الأعلى، عدد 20-1970، ص 32-33. في نفس الإطار ذهب القرار الجنائي عدد 582 الصادر عن محكمة النقض بتاريخ 2016/05/18، ملف عدد 2014/1/6/10512.

[38] Arrêt de la Cour suprême n° 117 en date du 03/02/2011, dossier 6581/6/9/2010.

[39] En informatique, le fichier LOG est un format de fichier texte. Il s'agit d'un document créé par un programme ou un système d'exploitation qui constitue un historique des activités liées à l'utilisation de ce programme ou ce système.

[40] Les « **fichiers journaux** » sont des **enregistrements des activités des utilisateurs**, des **anomalies** et des **événements liés à la sécurité** d'un environnement informatique (logiciel, système d'exploitation, application, site internet etc.).

modifiée. Par conséquent, le juge pénal dispose d'un pouvoir discrétionnaire qui lui permet d'évaluer cette preuve, de déterminer ses forces et ses faiblesses, afin de rendre la vérité scientifique une vérité judiciaire. Le juge ne doit pas également fonder son évaluation sur des informations personnelles ou des déclarations faites, mais plutôt sur sa conviction ou le cas échéant sur une expertise, dont le résultat peut être décisif pour la manifestation de la vérité dans les infractions informatiques[41].

Ainsi, la spécificité de la preuve en matière de cybercriminalité exige que la preuve électronique soit évaluée par un moyen pouvant ramener le juge à un degré de certitude qui ne peut être atteint qu'avec des arguments solides et irréfutables. C'est ce que souligne la Cour de cassation dans l'un de ses arrêts : « attendu que, si le juge de fond dispose d'un pouvoir discrétionnaire lui permettant d'apprécier souverainement la force probante des éléments de preuves, il reste que l'affaire en cours ne doit pas porter sur des questions d'ordre technique sur lesquels le tribunal ne peut pas s'exprimer, ce qui impose au juge le recours à l'expertise pour trancher cet affaire »[42].

Il n'y a pas donc conflit entre la nature de la preuve électronique et le pouvoir discrétionnaire du juge, mais plutôt une complémentarité. Ainsi, le pouvoir discrétionnaire du juge ne porte pas sur la valeur scientifique décisive de la preuve électronique, mais plutôt sur les circonstances dans lesquelles la preuve a été collectée, surtout lorsqu'il estime que ladite preuve n'est pas cohérente avec les circonstances de l'affaire. La simple présence de la preuve ne signifie pas que le juge prononcera automatiquement la condamnation ou l'acquittement, mais il doit avant tout analyser et examiner les conditions et circonstances entourant sa collecte.

Cette approche a été confirmée par la Cour d'Appel de Casablanca qui précise dans un arrêt que « Le tribunal estime dans ce cas qu'il ne dispose pas d'un pouvoir discrétionnaire, du fait de la force scientifique dont jouit l'expertise, mais par contre, il a le pouvoir d'apprécier les circonstances entourant cette expertise d'un point de vue pratique et non scientifique... »[43].

Il est à conclure que, quelle que soit l'efficacité de l'expertise en matière de cybercriminalité, elle nécessite un pouvoir judiciaire discrétionnaire, surtout dans les cas où le rapport de l'expert semble incompatible avec les circonstances entourant la commission du délit électronique. Ainsi, chaque fois que le rapport d'expertise est incompatible avec la conviction du juge, celui-ci peut l'écarter sur la base d'une décision motivée.[44]

En conclusion, on peut dire que la justice pénale marocaine reconnait la preuve électronique, l'inclut dans ses décisions et la soumis, en termes

[41] قرار عدد 3400 الصادر بتاريخ 21 شتنبر 2010 عن غرفة الجنح الاستئنافية بمحكمة الاستئناف بالرباط ، ملف عند 2751/2010/19 ، حكم منشور بمجلة قضاء محكمة الاستئناف بالرباط العدد الثاني.

[42] قرار المجلس الأعلى عدد : 745 المؤرخ في 13/01/2000 ، ملف جنحي عدد 17203/6/7/99 مجلة قضاء المجلس الأعلى ، العدد المزدوج 58 و 57 السنة 23 يوليوز 2001 ، ص 402 و 403 المشار اليه في الناجم كوبان، مرجع سابق، هامش 449 ، ص 148. في نفس الاتجاه ذهب القرار عدد 23 الصادر عن المجلس الأعلى (محكمة النقض حاليا) بتاريخ 2011/01/06، ملف عدد 2010/10/6/14911.

[43] قرار جنحي صادر عن محكمة الاستئناف بالدار البيضاء، بتاريخ 27/07/1994، ملف عدد 3650/93 ، منشور بمجلة القصر ، العدد 3، ص 63

[44] ياسين زوباير، مرجع سابق، هامش 430، ص 63

d'appréciation et d'évaluation, au pouvoir discrétionnaire du juge. Ce dernier est tenu de vérifier sa loyauté, son authenticité, son intégrité et sa traçabilité et de se nourrir également des débats contradictoires afin de renforcer son appréciation des éléments de la preuve.

En tout état de cause, l'intime conviction du juge devra être le dernier recours pour apprécier les différents éléments des preuves électroniques. Toutefois, le pouvoir discrétionnaire du juge n'est pas absolu, des tempéraments et exceptions sont prévus par la loi.

B- Les limites du pouvoir discrétionnaire du juge pénal.

Il faut reconnaître que le pouvoir d'appréciation des tribunaux n'est pas absolu. Il subit un certain nombre de tempéraments, qui ont pour effet de restreindre la liberté du juge, en le soumettant au contrôle de la Cour de cassation. Dans d'autres cas, la règle de l'intime conviction et la maxime in dubio pro reo subissent de véritables exceptions, avec en particulier certains procès-verbaux ayant une force probante particulière.

S'il est incontestable que le système de preuve morale doit normalement faciliter la répression, dans le cadre d'une procédure, comme la nôtre, fondée sur le principe de la liberté des preuves, il reste que la mise en œuvre de la règle de l'intime conviction et de la maxime in dubio pro reo est soumise au contrôle de la cour de cassation[45].

La meilleure preuve est donnée par l'article 286 déjà cité qui dispose clairement que «la décision doit comporter les motifs sur lesquels se base la conviction du juge... ». Ce texte est complété par le 8ème paragraphe de l'article 365, qui énonce plus clairement que toute décision doit contenir « Les motifs de fait et de droit sur lesquels le jugement, arrêt ou ordonnance est fondé, même en cas d'acquittement ».

Ces tempéraments, qui restreignent la liberté du juge et assurent d'autant la protection de l'individu, sont renforcés par d'autres dispositions qui se trouvent au cœur de toute la procédure pénale marocaine et du procès équitable. Aux termes de l'article 287 du C.P.P. « *la juridiction ne peut fonder sa décision que sur des preuves versées au cours de l'audience et discutées oralement et contradictoirement devant elle* ».

Tant de garanties sont de nature à parer aux abus éventuels et à éviter l'arbitraire du juge.

Par ailleurs, les procès-verbaux à force probante particulière peuvent neutraliser la présomption d'innocence, la règle du doute favorable et même l'intime conviction, et ce, malgré que le législateur a subordonné leur force probante à deux conditions essentielles:

- Les P.V. et les rapports dressés par les O.P.J., les agents de police judiciaire et les fonctionnaires et agents chargés de certaines missions de police judiciaire, n'ont de force probante qu'autant qu'ils sont réguliers en la forme.
- Les auteurs de ces P.V. rapportent, dans le cadre de leur compétence, ce qu'ils ont vu ou entendu personnellement.

[45] Mohammed Jalal ESSAID, op.cit note (32), p145-157.

Ces garanties ne sont pas négligeables, mais s'avèrent insuffisantes face à la force probante des P.V ou rapports dressés par les OPJ en matières délictuelle et contraventionnelle. Dans ce sens, l'article 290 du C.P.P, dispose que « les procès-verbaux ou rapports dressés par les OPJ pour constater les délits et les contraventions font foi jusqu'à preuve contraire », sachant que la majorité des infractions informatiques relèvent du domaine délictuel.

C'est la même chose pour les P.V. et rapports, dressés par certains fonctionnaires et les agents chargés de certaines missions de police judiciaire, concernent des domaines bien limités: certaines infractions douanières, et des infractions relatives aux Eaux et Forêts et à la pêche maritime. Mais cette fois-ci les PV et rapports font foi jusqu'à inscription de faux. Le prévenu, dans ce cas, fait l'objet d'une présomption absolue de culpabilité : une présomption qui ne peut être attaquée que par la procédure aléatoire de l'inscription de faux, qui aboutit rarement.

Certains juristes, se référant à la jurisprudence de la Cour de cassation, ont critiqué cette catégorie de P.V. dont la force probante ne peut céder devant les seules dénégations et explications du prévenu[46]. La mise en œuvre des grands principes qui dominent le procès équitable, doit conduire à doter tous les procès-verbaux de la même force probante. Quelle que soit la gravité de l'infraction commise et la nature de la matière concernée, les procès-verbaux et les rapports ne doivent valoir qu'à titre de simples renseignements.

La force probante, attribuée par le législateur aux P.V. et rapports dressés par les O.P.J., en matière délictuelle, n'est pas conforme à la présomption d'innocence et limite le pouvoir d'appréciation du juge[47].

Dans la pratique le juge s'appuie principalement sur les PV de la police judiciaire, qui peuvent contenir des preuves électroniques en lien avec l'auteur du crime. Dans ce sens, un jugement rendu par le tribunal de première instance de Casablanca précise : « ... attendu que le PV établit dans le respect des prescriptions légales, est considéré comme une preuve irréfutable jusqu'à preuve du contraire »[48].

Par conséquent, la justice pénale s'appuie sur les PV de la police judiciaire comme principal moyen de preuve. C'est ce que confirme le même jugement susmentionné, qui précise : « Attendu que le tribunal, avec le pouvoir dont il dispose, peut fonder sa conviction sur tous les moyens de preuve qui lui sont présentés, y compris le PV de la police judiciaire... ».

Le recours automatique aux PV de la police judiciaire, conduit le juge pénal à traiter les moyens de preuve de manière négative. Le but recherché par le juge, selon cette doctrine, est la facilité de motivation[49].

[46] M. Jaouhar, art. cit. in Mélanges M-J Essaid, op. cit. note (249), p 231

[47] C.C.D.H., rapport annuel sur la situation des droits de l'homme au Maroc en 2003.

[48] حكم جنحي صادر عن المحكمة الابتدائية بالدار البيضاء بتاريخ 28/08/2012 في ملف رقم 6845/101/2012، حكم غير منشور.

[49] يوسف وهابي، وسائل الإثبات وسائل النفي ودور المحامي في مرحلة المحاكمة، مجلة القصر، العدد التاسع، 2004، ص 139

Néanmoins, cette position doctrinale est à rejeter, car en se référant à de nombreux arrêts rendus par la justice marocaine, on constate que le juge traite le PV de la police judiciaire comme un moyen de preuve parmi d'autres. C'est ce qu'a établi un jugement rendu par le tribunal de première instance de Casablanca qui précise : « Attendu que le tribunal, avec le pouvoir dont il dispose pour former sa conviction sur la base de tous les moyens de preuve qui lui sont présentés »[50]. Un autre jugement rendu par le même tribunal, indique ce qui suit : « attendu que le rapport d'expertise réalisé par la cellule anti-cybercriminalité a conclu que l'ordinateur de l'accusé contient des programmes de piratage et des données piratées mises en vente par l'accusé sur Internet, ce qui l'expose aux sanctions prévues par les dispositions de l'article 607-10 du Code pénal»[51].

De ce qui précède, il nous apparaît claire que le juge pénal, dans le cadre de sa volonté de parvenir à la vérité, peut exploiter et analyser tous les détails mentionnés dans le PV de la police judiciaire ou dans le rapport établi par la cellule anti-cybercriminalité. Son pouvoir d'évaluation reste l'un des piliers fondamentaux sur lesquels repose le procès équitable. L'évaluation de la preuve numérique exige la soumission de ses éléments aux débats publics contradictoires en présence des parties au litige, sans exclure les circonstances dans lesquelles ces preuves ont été trouvées[52].

C'est ce que confirme un jugement rendu par le tribunal de première instance de Marrakech, qui précise que : « Le tribunal fonde sa conviction sur les procès-verbaux qui font foi jusqu'à preuve du contraire, sur les conclusions tirées des débats contradictoires, ainsi que sur les preuves électroniques telles les photos et le CD»[53].

Conclusion

La répression d'une infraction informatique pose, en raison de son caractère transfrontière et sa dimension internationale, divers problèmes. Pour qu'elle soit appréhendée, il faut, en plus de ce qui a été développé, assurer «que le mode de présentation de la preuve numérique soit le même entre le pays où elle aura été recueillie et le pays où l'infraction sera jugée, cette compatibilité exige des choix technologiques similaires et des accords internationaux» [54]. En plus, l'environnement technologique évolue plus rapidement que le droit, soulevant des défis pour garantir la force de la preuve. Pour cela, lutter efficacement contre les nouvelles formes de criminalité nécessite l'adaptation d'un arsenal organisationnel et des instruments procéduraux, et surtout une coopération internationale étroite.

[50] حكم جنحي صادر عن المحكمة الابتدائية بالدار البيضاء بتاريخ 28/08/2012 في ملف رقم 6845/101/2012، حكم غير منشور. نفس الاتجاه ذهبت إليه المحكمة الابتدائية بالعيون في حكمها عدد 1101 بتاريخ 2015/03/20، ملف 2015/2105/843.

[51] حكم جنحي صادر عن المحكمة الابتدائية بالدار البيضاء عدد 6465 بتاريخ 27/07/2012 ملف عدد 6251/11/12 حكم غير منشور مشار إليه في ياسين زوباير، مرجع سابق، هامش 430، ص 59.

[52] ياسين زوباير : المرجع السابق ، ص 59.

[53] حكم ابتدائي عدد 4 صادر بتاريخ 02/01/2012 ، ملف جنحي تلبسي ، عدد 3823/2103/11 عن المحكمة الابتدائية بمراكش ، حكم غير منشور مشار إليه في عبد الله ادعول، الدليل الإلكتروني في الإثبات الجنائي، رسالة لنيل دبلوم الماستر في القانون الخاص، جامعة القاضي عياض، كلية العلوم القانونية والاقتصادية والاجتماعية، مراكش، السنة الجامعية 2011/2012، ص 98.

[54] Pierre NAVRO, « la procédure pénale en matière informatique », Lamy droit de l'informatique : bulletins d'actualités, décembre 1995.

Les infractions informatiques sont transnationales[55] et peuvent être commises simultanément dans plusieurs pays. De ce fait, la criminalité informatique n'est plus l'affaire d'un seul pays, mais d'une menace internationale. La coopération internationale s'impose alors comme l'un des meilleurs moyens permettant de renforcer l'action judiciaire et policière sur les réseaux.

REVUE DROIT & SOCIETE
N° 12 JANVIER / MARS 2023

[55] « Une infraction de cybercriminalité présente une dimension transnationale lorsqu'elle comprend un élément ou produit un effet substantiel sur le territoire d'un autre pays, ou y est en partie réalisée. »
Voir : Office des Nations Unies contre la Drogue et le crime, Étude approfondie sur le phénomène de la cybercriminalité, et les mesures prises par les Etats Membres, la Communauté internationale et le secteur privé pour y faire face, p:11.
http://www.unode.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_F.pdf

 ISSN: 2737-8101

Bibliographie

Ouvrages :

En français

Eric OK, « La preuve numérique : Un défi pour l'enquête criminelle du 21e siècle », in les Cahiers du numérique 2003/3 (Vol. 4).

Mohammed Jalal ESSAID, « le procès équitable dans le code de la procédure pénale de 2002 », 1èr édition, 2008

P. Bouzat, « La loyauté dans la recherche des preuves », Mélanges Hugueney, 1964.

S. Canas, « Blockchain et preuve : le point de vue du magistrat », Dalloz IP/IT, févr. 2019.

En arabe

احمد فتحي سرور : الوسيط في قانون الإجراءات الجنائية ، الطبعة السابعة ، دار النهضة العربية، 1996.

خالد ممدوح إبراهيم : الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية، الطبعة الأولى، السنة 2009.

ممدوح عبد الحميد عبد المطلب : البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والأنترنت، دار الكتب القانونية، مصر، 2006.

محمد أمين البشري : التحقيق في الجرائم المستحدثة، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 2004.

عبد الحكيم الحكماوي : الإثبات في الجريمة الالكترونية ، سلسلة ندوات محكمة الاستئناف بالرباط ،تأثير الجريمة الالكترونية على الائتمان المالي، العدد السابع، مطبعة الأمنية ، الرباط، 2014.

Thèses et mémoires et notes de cours

Jean-François TYRODE, « Eléments de procédure pénale dans le cadre de l'atteinte aux personnes par la cybercriminalité endroit européen », MASTER Droit de l'Internet Public - Administration - Entreprises, Année Universitaire 2006 - 2007.

Koulika Arnaud NIKIEMA, « La preuve dans le contentieux du cyberespace », mémoire Master, Université Gaston Berger de Saint Louis (Sénégal), 2010-2011.

P. VERGUCHT, « La répression des délits informatiques dans une perspective internationale », thèse en droit, Montpellier, 1996.

Pierre NAVRO, « la procédure pénale en matière informatique », Lamy droit de l'informatique : bulletins d'actualités, décembre 1995.

ياسين زوباير : قصور الدليل الالكتروني الجنائي في إثبات الجريمة الالكترونية، رسالة لنيل دبلوم الماستر المتخصص، كلية العلوم القانونية والاقتصادية والاجتماعية سلا، 2013-2014.

Revues

Lexbase, Revues n° 280 du 18 janvier 2012.

مجلة جامعة دمشق للعلوم الاقتصادية و القانونية، المجلد 29، العدد الثاني، 2011.

مجلة القصر، العدد التاسع، 2004.

Décisions judiciaires :

القرار عدد 364، صادر عن محكمة الإستئناف بالرباط ملحقة حي السلام بسلا، بتاريخ 2006/04/17، في الملف عدد 22/05/740. غير منشور.

القرار الجنائي عدد 49 الصادر في 19 نونبر 1970، منشور بمجلة قضاء المجلس الأعلى، عدد 20-1970.

قرار المجلس الأعلى عدد 8/474 المؤرخ في 2001/01/25، ملف جنحي عدد 00/7908.

قرار المجلس الأعلى عدد 117 بتاريخ 2011/02/03، ملف 2010/9/6/6581، غير منشور.

القرار الجنائي عدد 49 الصادر في 19 نونبر 1970، منشور بمجلة قضاء المجلس الأعلى، عدد 20-1970، ص 32-33. في نفس الإطار ذهب القرار الجنائي عدد 582 الصادر عن محكمة النقض بتاريخ 2016/05/18، ملف عدد 2014/1/6/10512.

قرار المجلس الأعلى عدد : 745 المؤرخ في 13/01/2000 ، ملف جنحي عدد 17203/6/7/99.

القرار عدد 23 الصادر عن المجلس الأعلى (محكمة النقض حاليا) بتاريخ 2011/01/06، ملف عدد 2010/10/6/14911.

قرار محكمة النقض عدد 1280 بتاريخ 2015/12/30، ملف 2015/5/6/5808، غير منشور.

حكم ابتدائي عدد 4، الصادر عن المحكمة الابتدائية بمراكش بتاريخ 2012/01/02، ملف جنحي تلبسي عدد 11/2103/38323، حكم غير منشور.

قرار عدد 3400 الصادر بتاريخ 21 شتنبر 2010 عن غرفة الجنح الاستئنافية بمحكمة الاستئناف بالرباط ، ملف عند 2751/2010/19 ، حكم منشور بمجلة قضاء محكمة الاستئناف بالرباط العدد

الثاني.

حكم ابتدائي غير مشار إلى عدده، صادر عن المحكمة الإبتدائية بقلعة السراغنة بتاريخ 2011/12/09، في ملف جنحي عادي عدد 2010/400، حكم غير منشور.

حكم جنحي صادر عن المحكمة الابتدائية بالدار البيضاء بتاريخ 28/08/2012 في ملف رقم 6845/101/2012، حكم غير منشور.

حكم جنحي صادر عن المحكمة الابتدائية بالدار البيضاء بتاريخ 28/08/2012 في ملف رقم 6845/101/2012، حكم غير منشور.

حكم عدد 1101 صادر عن المحكمة الابتدائية بالعيون في بتاريخ 2015/03/20، ملف 2015/2105/843.

حكم جنحي صادر عن المحكمة الابتدائية بالدار البيضاء عدد 6465 بتاريخ 27/07/2012 ملف عدد 6251/11/12 حكم غير منشور.

حكم ابتدائي عدد 4 صادر بتاريخ 02/01/2012 ، ملف جنحي تلبسي ، عدد 3823/2103/11 عن المحكمة الابتدائية بمراكش ، حكم غير منشور.

Arrêt la cour espagnole n° 3943/1990 du 24 mai 1990.

Colloques et rapports :

C.C.D.H., rapport annuel sur la situation des droits de l'homme au Maroc en 2003.

Colloque de la première chambre de la cour d'appel de Paris. Preuve numérique à l'épreuve du litige, Compagnie nationale des experts de justice en informatiques et techniques associées

Webographie :

http://blogs.u-paris10.fr/content

https://cours.unjf.fr/

https://www.village-justice.com/

http://www.unode.org/