REPUBLIQUE DU SENEGAL

Un Peuple-Un But-Une Foi

Ministère de la Justice

Centre de Formation Judiciaire

MEMOIRE DE FIN DE FORMATION

THEME :

LA PREUVE NUMERIQUE

Présenté par :
Véronique FAYE
Auditeur de Justice

Sous la Direction de :
M. Jean Aloise NDIAYE
Magistrat, Auditeur à la Cour Suprême

ANNÉE ACADÉMIQUE 2007-2009

Je dédie ce mémoire spécialement :

A

Ma mère

Que cette dédicace soit la preuve de mon amour et de ma reconnaissance.

Je rends grâce à Dieu le Tout-Puissant de m'avoir toujours soutenu et d'avoir rendu possible ce travail.

- ✓ *A mes parents : ma mère Madeleine FAYE à qui je ne dirai qu'un seul mot : que le Seigneur te rende au centuple ton amour, ton attachement et ton dévouement pour tes enfants.*
- ✓ *A mon père Philippe FAYE*
- ✓ *A Monsieur Jean FAYE*
- ✓ *A mes Sœurs : Evelyne Rose, Yvonne et Gisèle Thérèse FAYE que le seigneur guide vos pas et vous protège*
- ✓ *A Mon Directeur de mémoire Monsieur le Président Jean Aloïse NDIAYE à qui je dirai un grand merci, de par sa disponibilité, son soutien et ses conseils nous avons pu réaliser ce travail.*
- ✓ *A tous mes camarades de promotion du Centre de Formation Judicaire (CFJ) et en particulier ceux qui sont devenus de véritables amis.*
- ✓ *A Monsieur El Hadji Malick NGOM, Informaticien*
- ✓ *A tous ceux qui de prés ou de loin ont contribué à la réussite de ce travail, et à tout ce qui m'ont incité à étudier le droit.*

Plan

Introduction

Trouvant son étymologie dans le mot latin « *probare* », la preuve est « la démonstration de l'existence d'un fait ou d'un acte dans les formes admises par la loi »[1]. En cas de contestation, le fait de ne pas pouvoir prouver son droit équivaut, en pratique, à être privé du droit contesté dès l'instant que l'obstacle de la preuve empêche son exercice (sachant que, dans de nombreux cas, la question de la preuve va se poser dans le contexte d'un litige dont est saisi le juge ou dans le cadre d'une transaction).C'est en ce sens que le droit a prévu cinq modes de preuves que sont la preuve littérale, l'aveu, le serment, le témoignage et la preuve par présomption.

L'expérience a toutefois montré que l'évolution du monde se traduit, entre autres, par la multiplication des découvertes scientifiques et leurs applications concrètes c'est-à-dire des innovations techniques, ainsi les modes de communication (ou circulation des informations) ont littéralement explosé avec, notamment, l'avènement de l'informatique et, à sa suite, de l'Internet.

En effet, la naissance [2]et l'essor de l'informatique et de l'Internet ont bouleversé les manières et les moyens de communiquer (faire circuler des informations), de penser et/ou d'agir, les rapports des hommes au temps et à l'espace, leurs rapports aux sources d'informations et, au-delà, leurs rapports à l'écriture ou aux signes etc. « Notre époque est dédiée, pour le meilleur et pour le pire, à la

---

[1] Vocabulaire juridique H. Capitant, sous la dir. de G. Cornu, Quadrige/Puf, V° Preuve, 1.

[2] Cf article Moussa Thioye, preuve et signature électronique p 4

technologie, qui permet notamment aux êtres humains de communiquer entre eux par l'intermédiaire des ordinateurs et de se passer en un trait de temps, d'un point à un autre de la planète, des images, des sons et des textes ». Traduisant une forme de triomphe du « système technicien », ce nouvel élément a suscité la naissance de nouvelles disciplines juridiques au premier rang desquelles figure, notamment, ce qu'il a été convenu d'appeler le droit de l'informatique ou, plus spécialement, celui de l'Internet.

Nombreuses sont aujourd'hui les interactions du droit et de l'informatique. Si l'informatique juridique documentaire devient indispensable au juriste qui doit apprendre à interroger les grandes banques de données, d'un autre côté, comme tout grand phénomène social, l'informatique est progressivement « encadrée » par le droit .Par ailleurs, l'avènement du « clic » et de la « Souris [3]», comme manifestation du consentement ou de l'action, est désormais une réalité : pour ne pas entraver le commerce électronique et les contrats ou actes en ligne par des règles de formation ou de preuve qui ne leur sont pas adaptées, il a été créé la preuve numérique que nous allons voir dans le cadre de cette étude. Il faut aussi noter que la preuve électronique est apparue suites aux nouvelles lois qui ont été élaborées dans le but d'adapter les fonctions probatoires traditionnelles aux réalités de l'environnement immatériel il en est ainsi de la loi L200-23 du 13 mars 2000 modifiant l'article1316 du code civil qui consacre l'existence de l'écrit et de la signature électronique.

Et si nous prenons l'exemple de la France, cette loi précitée est née à la suite d'une longue évolution .Tout au début, le droit de la preuve a été Consacré dans

[3] www.adie/adic/docs/moussathioye.pdf

l'ordonnance de Moulins[4] de 1566 qui posa " la règle de la preuve écrite des actes juridiques " .Depuis 1804, notre système de droit privé vit essentiellement sous le monopole de l'écrit papier, signé. Toujours En droit français, Il faut savoir que les règles de preuve sont différentes, selon que l'on se trouve dans le domaine commercial ou civil. L'article 109 du Code de commerce prévoit qu'« *À l'égard des commerçants, les actes de commerce peuvent se prouver par tous moyens à moins qu'il n'en soit autrement disposé par la loi* ». La règle vaut aussi bien, dans le cadre d'un acte mixte, entre un commerçant et un non-commerçant, à l'égard de la partie commerçante. Le droit français de la preuve reste tout de même marqué par le principe de prééminence de l'écrit. Même si le contrat est valablement formé sans écrit du seul fait de l'échange des consentements des parties, la nécessité pour les parties de se ménager la preuve de leur contrat impose en réalité le recours à un écrit. Dans les relations entre consommateurs, l'écrit est ainsi exigé pour les actes dont la valeur dépasse la somme de 800[5] euros. L'écrit correspond de façon traditionnelle au titre original revêtu d'une signature manuscrite et matérialisée dans un document papier. La jurisprudence a toutefois permis certaines évolutions. Tout d'abord, la validité des conventions de preuve a été reconnue par la Cour de cassation le 8 novembre 1989 dans l'affaire Credicas à propos des cartes de paiement et de crédit. Puis en 1997, la Chambre commerciale a clairement énoncé les conditions nécessaires à la valeur probatoire d'un document produit par télétraitement: « *l'écrit [...] peut être établi et conservé sur tout support, y compris par télécopies, dès lors que son*

---

[4] http://fr.jurispedia.o/rg/index.php/droit de la preuve sur l'internet

[5] Article1341du code civil et décret n°2001-476du30mai2001

intégrité et l'imputabilité de son contenu à l'auteur désigné ont été vérifiées ou ne sont pas contestées[6]».

Le droit de la preuve numérique proprement dit s'est d'abord manifesté avec l'utilisation de la carte bancaire, le code à quatre chiffres tenant lieu de signature manuscrite. Cependant, l'émergence des réseaux ouverts et notamment de l'Internet ainsi que l'obsolescence du Code civil en matière de preuve, ont justifié une réforme de ce cadre juridique.

Dans l'Union européenne un grand pas a été fait avec la publication de la directive du 13 décembre 1999 garantissant la reconnaissance de la valeur juridique de la signature électronique dans tous les pays de l'Union[7]. La preuve des transactions étant un élément essentiel pour le développement du commerce électronique dans un cadre juridique sûr, le Conseil des ministres français a adopté, le 1er septembre 1999, un projet de loi « *portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique* ». Le 29 février 2000, l'Assemblée Nationale adoptait le projet de loi après que le Sénat se soit lui même prononcé en faveur de cette adaptation législative, laquelle viendra modifier en profondeur les articles du Code civil relatifs au droit de la preuve. Cette réforme se justifie par la sécurité juridique nécessaire pour favoriser les échanges dans la société de l'information actuelle. La loi correspondante a été votée dès le 13 mars 2000.

Ainsi, la loi du 13 mars 2000 a modifié le droit français de la preuve, en admettant tout d'abord l'écrit électronique au rang des preuves littérales :

---

[6] Cour de cass . chambre commercial.1997-12 -02.95-1425 publié au bulletin

[7] Directive1999/93sur un cadre communautaire pour les signatures électroniques

"Lorsque la preuve est littérale, elle résulte d'une suite de lettres, de caractères, de chiffres ou de tout autre signe ou symbole doté d'une signification intelligible quel que soit leur support et leurs modalités de transmission"[8].

La loi a introduit dans le Code civil à l'article 1316-3 une définition de la preuve littérale, indépendante des supports utilisés et incluant l'écrit électronique au même titre que l'écrit papier.

Et même si d'aucuns y verront une nouvelle manifestation de mimétisme juridique, le Sénégal à l'instar du monde se devait de ne pas faire exception à la regle d'adaptation et de modernisation de sa législation avec notamment le Règlement n° 15/2002/CM/UEMOA relatif aux systèmes de paiement dans les Etats membres de l'Union Economique et Monétaire Ouest-Africaine (UEMOA). Mais depuis 2008 on note une prolifération de lois dans ce domaine avec la loi sur les transactions électroniques et celle sur la cybercriminalité et leurs décrets d'application qui ont parachevé le processus de consécration de la preuve numérique.

Mais il faut quand même noter que le Sénégal, tout comme l'ensemble des pays africains excepté le nord islamique et l'Ethiopie, a toujours été dominé par la tradition orale et le droit coutumier autrement dit l'écriture n'y a vu le jour que tardivement.

Les Sénégalais ont été, tout de même, du fait de la mondialisation, brutalement précipités (en théorie) dans la « toile d'araignée mondiale[9] ». Alors que l'écrit sur support papier n'a toujours pas complètement évincé l'oralité de l'univers

---

[8] Article1316-1du code civil

[9] Désignation de World Wide Web V. article Moussa Thioye sur la prevue et la signature électronique p7

juridique africain, alors que l'accès à l'Internet est encore très restreint dans le « continent noir », le support électronique y est pourtant apparu et s'y installe progressivement malgré tout.

En vainquant certaines « cyber résistances », une des grandes innovations du projet de loi tient à la reconnaissance de l'écrit électronique en tant que preuve littérale. Alors qu'elle était jusqu'alors assimilée à l'écriture manuscrite (ou Dactylographiée) fixée sur support papier, la preuve par écrit fait l'objet d'une redéfinition dans l'objectif de l'adapter aux nouvelles technologies de l'information et de la communication, car Jusqu'à une époque récente, l'*instrumentum* n'était, pour l'essentiel, concevable et conçu que dans le sens de support papier – manuscrit ou dactylographié.

Matérialisant l'accord de volonté des parties voir l'acte ou l'engagement Unilatéral avec, à la fin du document, la signature autographe, réalisée par l'apposition manuelle d'un signe, généralement le nom, sur une feuille de papier, en tout cas sur un support tangible[10].

Certes il s'agit de nouveaux modes de preuves apparus sous l'ère de l'informatique, à cotés des preuves classiques, toutefois le juge réfute toute hiérarchie entre eux et s'en rapporte prudemment au juge auquel il reviendra de trancher en cas de contestation en déterminant le titre le plus vraisemblable quel qu'en soit le support.

Le champ d'application de l'écrit numérique est très étendu toutefois ne bénéficient toujours pas de la faculté de recourir à l'écrit électronique, les actes sous seing privé relatifs au droit de la famille ainsi que les actes relatifs à des

---

[10] idem

suretés personnelles ou réelles de nature civile ou commerciale, sauf s'ils sont passés pour les besoins de la profession[11].

Ces derogations s'inscrivent au nombre de celles que les Etats membre sont expressément autorisés à prévoir en application de l'article 9 al2 de la directive du 8juin 2000.

S'intéresser à la preuve numérique revient donc à voir à un niveau pratique la place de ces nouveaux modes de preuve que sont l'écrit et la signature électronique dans l'économie actuelle dans la mesure où elles cohabitent avec d'autres modes de preuve. Mais il s'agira également de voir l'impact de ces preuves difficiles à rapporter dans le cadre d'un procès.

De ce sujet se dégage un intérêt pratique en ce sens que la connaissance et l'accès à ces moyens de preuve permettra ,entre autre, de réduire le taux d'infractions commises via le net mais aussi de prouver certaines transactions effectuées en ligne dans le cadre du commerce électronique afin de réduire l'aspect insécurité dans le net considéré par certains cybercriminel comme un paradis où tout est permis, un lieu où chacun peut faire et dire ce qu'il veut sans être identifié.

Partant de ces considérations, nous pouvons nous interroger sur la valeur juridique de la preuve numérique dans ces systèmes où les preuves dites traditionnelles occupent une place prépondérantes .En d'autres termes, qu'elle est la force probante de l'écrit et de la signature électronique dans le procès civil ou au pénal ?

---

[11] Article l108du code civil

Avec l'apparition des nouvelles technologies la reconnaissance de l'écrit et de la signature électronique comme mode de preuve est devenue plus que nécessaires à l'état actuel de l'évolution du monde. C'est en ce sens que nous allons d'abord voir l'admission de l'écrit et de la signature électronique comme mode de preuve et ensuite l'impact de ces modes preuves dans nos systèmes juridiques.

Chapitre I : L'admission de l'écrit et de la signature électronique comme mode preuve

Le législateur français à travers la loi L2000-230 du13mars 2000 modifiant l'article 1316 du code civil a consacré l'existence de l'écrit électronique et de la signature électronique comme mode de preuve dans ses articles 1316 à1316-4.

L'article 1316 du code civil français ne dispose que la « preuve littéral ou preuve par écrit résulte d'une suite de lettres, caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible quel que soient leur support et leur modalités de transmission »

En adoptant une conception large de la notion d'écrit le législateur du code civil étend le droit de la preuve au vaste domaine de l'informatique et des télécommunications.

A l'instar de la France, le droit sénégalais à travers la loi n°2008-08 du 25 janvier 2008 a reconnu l'existence de l'écrit et de la signature électronique comme preuve au même titre que les preuves dites traditionnelles[12].

---

[12] Article 37 à 42 du de la loi sénégalaise sur les transactions électroniques

Dés lors quelqu'en soit le support (matériel ou immatériel) l'écrit et la signature sont admis comme mode de preuve.

Toutefois pour être considéré comme preuve, l'écrit électronique et la signature électronique doivent remplir un certain nombre de conditions de recevabilité.

Des restrictions peuvent néanmoins être apportées à la recevabilité de ces modes de preuve.

Section I : les conditions de recevabilité de la preuve électronique

L'écrit sous forme électronique est admis en preuve au même titre que l'écrit support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit identifié et conservé dans des conditions de nature à en garantir l'intégrité[13] .

Le droit sénégalais à l'image du code civil français pose donc par là une double exigence à la validité de l'écrit numérique : l'identification de la personne dont émane l'écrit et la garantie de l'intégrité du message.

Paragraphe I : l'identification de la personne

L'exigence de cette condition se justifie par le fait que plusieurs personnes peuvent intervenir dans le transfert de données informatiques (l'auteur du message, le gérant du site, le récepteur de message ...). Il est donc nécessaire d'identifier l'auteur exact du message parmi tous ces intervenants. La partie ayant en charge de rapporter la preuve de l'existence et du contenu devra démontrer l'origine du document car il ne suffira pas d'aller cueillir un quelconque fichier ou textes stockés sur une bande de sauvegarde pour apporter

[13] Même article

cette preuve. Le juge doit, malgré les difficultés que cela présente, avoir la plus grande certitude possible que l'acte juridique en cause émane de celui auquel on l'oppose. Cette approche conduit à deux exigences : l'origine de cet échange électronique doit être sécurisée et sa non-falsification garantie. Ceci implique l'authentification de la personne du signataire (A) ainsi que des garanties quant à la possibilité de vérifier l'identité de l'auteur (B).

L'authentification de la personne du signataire

Préalablement à tout développement, une distinction importante tant sur le plan technique que sur le plan juridique, mérite d'être présentée. En effet, les procédés relatifs à l'identification d'un système de signature doivent être appréciés et analysés distinctement des procédés relatifs à l'identification du titulaire d'un dispositif de signature électronique. L'illustration la plus parlante pour comprendre cette différence est celle des numéros d'identification personnels (P.I.N.) à quatre chiffres liés à l'utilisation de cartes à puce (téléphone portable, carte bancaire, ...) ou des certificats de signature quelque soit leur support (matériels ou logiciels) qui constituent un procédé n'identifiant pas directement la personne dont l'acte émane, mais identifiant la personne à laquelle il sera imputé. Comme nous l'avons déjà indiqué dans nos propos introductifs, la jurisprudence exigeait pour que l'écrit sous forme électronique puisse valoir preuve, en sus de l'intégrité de l'acte, que l'imputabilité de son contenu à son auteur désigné ait été vérifiée ou ne soit pas contestée. Ce qui veut dire que le Sénégal depuis l'avènement de loi la loi du 25 janvier 2008 sur les transactions électroniques retient, la notion d'imputabilité qui résulte de la formulation retenue à l'article 37 de cette loi. Ce texte reconnaît la force probante d'un écrit sous forme électronique au même titre que l'écrit papier, «

sous réserve que puisse être dûment identifiée la personne dont il émane (...) ».

L'emploi du terme "*dûment*[14]" avant le mot "*identifiée*" implique que l'identification de la personne dont l'écrit émane doit faire l'objet d'une vérification minutieuse. En ce sens que le droit Sénégal tout comme le code civil français a posé d'abord comme condition, pour que les écrits électroniques soient probants l'imputabilité de l'acte à la personne qui l'a signé et la vérification de l'identification du signataire. Dès lors, cette acception est plus large que la seule notion d'imputabilité traditionnellement retenue par la jurisprudence et la doctrine.

A la lecture de cet article il en ressort donc que, c'est indirectement que le régime probatoire institué pour les écrits électroniques impose un lien évident entre l'écrit et la signature qui sont pourtant deux notions juridiques distinctes. Cette exigence d'identification dûment constatée pour l'acte peut surprendre puisqu'il s'agit en réalité d'une fonction propre à la signature et non à l'écrit lui-même. Dés lors, il est clair que l'on exige des écrits électroniques, pour leur reconnaître la même force probante que les écrits papier, qu'ils soient signés. De la sorte, l'écrit s'inspire étroitement de la notion d'acte sous seing privé original. Le procédé de signature électronique basé sur la cryptologie à clé publique (signature numérique) offre la garantie d'identification telle qu'exigée des écrits sous forme électronique pour qu'ils valent preuve grâce au certificat à clé publique qui est l'un de ses composants fondamentaux. Avec la signature numérique, l'identification du signataire correspond au nom de la personne

[14] http://www.caprioli-avocats.com sur la traçabilité et le droit de la preuve

inscrite dans le certificat en qualité de signataire lié à une paire de clé asymétrique.

Bien entendu, en pratique, la personne figurant sur le certificat peut mettre à disposition temporairement sa clé privée, son code ou son mot de passe à une personne de son choix (un proche, un collaborateur, ...). Dans ces hypothèses, l'acte n'émane pas directement de la personne qui est identifiée, mais d'une autre et ce, sans que l'on puisse le savoir justement parce que le code d'activation de la clé privée du signataire est parfaitement correct.

Il convient de noter au demeurant que la notion d''authentification au sens juridique revêt deux significations. Soit elle correspond à "l'opération (contemporaine de la rédaction d'un acte) consistant à conférer l'authenticité à cet acte (spécialement à observer les formes dont dépend celle-*ci*" il faut donc noter que l'authenticité est ici entendue comme la "qualité (spécialement force probante) dont est revêtu un acte du fait qu'il est reçu, ou au moins, dressé par un officier public compétent, suivant les formalités requises" par exemple la signature quand elle est apposée par un officier public , confère l'authenticité à l'acte . L'authentification peut également être définie comme l'opération "*consistant à vérifier l'authenticité d'un objet ou d'un document.*", l'authenticité étant cette fois-ci la "qualité de l'objet ou du document (œuvre, écrit, etc.) dont l'auteur ou l'origine sont attestés, notamment sur la foi d'un certificat".

Dans le cadre de notre étude, c'est cette seconde définition qui nous intéresse puisqu'elle recouvre bien la notion d'identification. D'un point de vue technique, l'opération d'authentifier consiste à vérifier l'origine du message ; ce qui implique une identification de l'émetteur-signataire garantie par un tiers indépendant et qui peut être vérifiée par le destinataire.

Si nous prenons, l'exemple de la France, le P.S.C[15] n'authentifie jamais le contenu des actes, dont il ne connaît d'ailleurs en principe ni le nombre, ni la nature, ni la teneur, ni les noms des destinataires. Ce tiers a pour seule fonction d'identifier le signataire auquel il a octroyé un certificat numérique d'identité unique. Ainsi, le P.S.C. ne certifie à aucun moment l'écrit sous forme électronique mais seulement le dispositif de création de signature (bi clé) sous le contrôle du signataire, étant noté au demeurant que le certificat émis par le P.S.C. n'établit que le lien qui existe entre une personne et un bi-clé. Par suite, si le P.S.C. participe indirectement à l'écrit électronique en étant l'un des rouages du processus de la signature électronique, il n'a ni les moyens ni pour fonction de garantir les écrits électroniques. En revanche, son rôle est primordial dans l'opération d'identification électronique.

B - La vérification de l'identité de l'auteur de l'acte

L'article 27 du règlement de l'UEMOA, pour la délivrance de certificat électronique, impose dans tous les cas la vérification de l'auteur de l'acte. Le procédé retenu qui correspond concrètement aux signatures numériques, permet de l'identifier, la délivrance de l'identité s'effectue donc au moyen d'un certificat électronique qui est émis par le P.S.C. Selon le niveau de sécurité juridique souhaité, les conditions d'enregistrement de ses abonnés par le P.S.C. peuvent varier. Ainsi, l'enregistrement peut s'effectuer directement et seulement en ligne. Dans ce cas, la certitude de l'identité déclarée par l'abonné n'est pas totale, il s'agit donc d'une identification correspondant à un niveau de sécurité minimum. L'enregistrement peut également se faire en ligne et sur envoi par

[15] Sigle qui signifie : prestataire de service de certification (PSC)

voie postale de pièces justifiant de l'identité des personnes morales et/ou physiques déclarée par le titulaire du certificat.

Le P.S.C. peut aussi prévoir que ses abonnés s'inscrivent en ligne et procèdent au retrait du certificat (et des données d'activation) sur présentation des pièces justificatives en face à face, c'est à dire à un guichet organisé dans un lieu physique par le P.S.C. L'enregistrement peut enfin être réalisé en dehors de toute inscription en ligne et exclusivement sur présentation d'un certain nombre de pièces justifiant de l'identité de la personne inscrite dans le certificat. Ce dernier est émis sous la responsabilité du P.S.C. En pratique, ce certificat qui contient la clé publique de l'abonné est le plus souvent joint au message que la partie entend signer à l'aide de sa clé privée, mais il peut également être mis à disposition dans une base contenant les certificats émis par le P.S.C.

Dès lors, le récepteur du message ou du fichier signé (partie qui se fie) doit s'assurer que le certificat qui contient la clé publique correspondant à la clé privée ayant servi à signer est en cours de validité et qu'il n'est pas révoqué. Pour ce faire, il devra consulter la liste de révocation des certificats sur un annuaire publié et mis à jour par le P.S.C. émetteur du certificat. Le destinataire devra également vérifier la signature que le prestataire aura apposé sur le certificat jusqu'à l'autorité de certification racine c'est à dire celle qui se trouve au sommet de la pyramide hiérarchique (Infrastructure à Clé Publique ou I.C.P.)

Avec ce procédé de signature électronique, l'exigence d'identification est ainsi honorée.

Ceci étant posé, les traces de l'écrit sous forme électronique doivent également garantir son intégrité.

Paragraphe II : la garantie de l'intégrité du message

L'écrit doit être établi et conservé sans qu'aucune altération, ni changement ne soit intervenu depuis la manifestation de volonté d'adhésion au contenu de l'acte jusqu'au moment où il devra faire foi, apporter la certitude de son contenu au juge.

Dans l'univers numérique, le système juridique a besoin de s'appuyer sur des éléments de preuve matérialisés sous forme de traces électroniques préconstituées. De sorte que si la loi sur la preuve prescrit que la trace électronique soit établie et conservée encore convient-il d'en assurer l'intégrité (A) ; toutefois, cette obligation probatoire a pour but de garantir la restitution de la trace par la conservation (B).

L'intégrité de la trace électronique

Si on se réfère au droit sénégalais la loi sur les transactions électroniques. la conservation de ces documents peuvent se faire sur une période de 10 ans[16], ce qui pose dés lors le problème de sa conservation car le document au moment d'être consulté doit être intact , intègre ,sans altération de manière générale , il doit être lisible en dépit même de la durée de conservation. Avec le support papier, la notion de trace intègre était caractérisée par « l'original ». L'intégrité de l'écrit, c'est à dire la certitude que l'écrit est demeuré intact dans le temps, correspond à une fonction juridique fondamentale. Cette notion facilement perceptible dans le monde matériel pouvait poser un problème particulier dans le monde numérique.

---

[16] Article 37de la loi sur les transactions électroniques

En effet, l'informatique et d'une façon plus générale, les échanges électroniques ne permettent pas une transposition parfaite de la notion d'original telle qu'appréhendée dans le monde matériel. En informatique, il n'y a point d'original (sauf sur le système d'information utilisé), mais des copies alors que l'article 40 de la loi sur les transactions électroniques précitées soumet la copie ou toute autre reproduction d'actes passés par voies électroniques à des conditions notamment la certification par les organismes agrées par l'agence de l'informatique de l'Etat.

Dans cette optique, l'analyse menée par les parlementaires luxembourgeois lors du projet de loi sur le commerce électronique doit, selon nous, être partagée. Ainsi, il est exact que " *Classiquement, la distinction original-copie s'appuie sur une différenciation relative à la nature du support. A cette différenciation correspond un traitement juridique différent. L'information contenue sur le support original se voit reconnaître une force probante supérieure à celle apparaissant sur la copie.*" . Apparaît alors justifié l'article 7 de la loi luxembourgeoise du 14 août 2000 qui ajoute un article 1322-1 dans le code civil rédigé de la façon suivante : «*L'acte sous seing privé électronique vaut comme original lorsqu'il présente des garanties fiables quant au maintien de son intégrité à compter du moment où il a été créé pour la première fois sous sa forme définitive*». C'est dans le même sens que la loi-type de la C.N.U.D.C.I a intégré la fonction d'intégrité dans la notion de forme originale. Le législateur français lors des premiers textes spéciaux qui traitaient de la dématérialisation des factures et des déclarations administratives par voie électronique n'avait pas procédé à une totale assimilation, se contentant d'énoncer un principe d'équivalence fonctionnelle.

D'une manière générale ,les termes « intégrité » et « fidélité » constituent deux notions qui permettent de transposer l'exigence du caractère intact de l'écrit dans le monde électronique en ce que les données doivent être conservées sous la forme sous laquelle , elle a été crée , envoyée ou reçue ou sous une forme dont on peut démontrer qu'elle n'est susceptible ni de modification ni d'altération dans son contenu et que le document transmis et celui conservé sont strictement identiques[17] En revanche, la notion de fiabilité ne répondait pas au besoin de sécurité juridique dans la mesure où ce terme s'applique, exclusivement aux procédés et autres processus techniques, ainsi qu'aux systèmes informatiques qui produisent des documents, des écrits. Or, ce sont les écrits qui doivent être intègres voire fidèles, les moyens utilisés devant être fiables. A l'heure actuelle, seule la signature électronique basée sur un certificat à clé publique permet de garantir cette fonction d'intégrité. En effet, ce procédé opère de façon automatique un condensé (abrégé) du message signé qu'il chiffre au moyen d'un algorithme de cryptographie (par une fonction dite « hasch » ou « contrôle »). Le message signé est alors accompagné de l'« *empreinte* » obtenue qui garantit que le document envoyé est identique au message reçu. Dès lors, le destinataire d'un message ou un fichier signé qui entend s'y fier, doit vérifier que la signature est valable c'est à dire qu'il doit comparer le résultat du calcul numérique (suite de chiffres) de l'abrégé du message chiffré à l'émission avec le résultat du calcul obtenu lors de réception. Cette opération permet de s'assurer que le message est bien intègre qu'il n'est ni altéré ni modifié. Aussi, est-il permis d'affirmer que le fait qu'un écrit sous

[17] Article 37 al 2dc la loi sur les transactions électroniques

forme électronique soit signé lui confère la qualité d'un écrit tenant lieu d'original. Par conséquent, le procédé de signature numérique répond aux attentes juridiques en matière de traces intègres car dés qu'elle est créée, il ya une présomption de fiabilité qui s'attache au document. Cette solution permet ainsi d'établir de façon certaine une assimilation parfaite entre la force probante des écrits papier et celle des actes sous forme électronique dès lors qu'ils sont signés. La signature est donc nécessaire à la perfection d'un acte juridique[18]

Rappelons que lorsque ces preuves sont portées devant le juge, ce dernier est très regardant sur la valeur probante des écrits numériques portés à sa connaissance. Ainsi, récemment, la jurisprudence a considére que dans la mesure où l'existence même de l'original n'était pas établie et qu'elle était contestée par le destinataire d'une télécopie litigieuse, la preuve de l'acte juridique n'était pas rapportée. En outre, dans l'hypothèse des photocopies certifiées conformes, c'est à dire des copies dont la conformité à l'original est certifiée par une personne digne de foi et ayant procédé à la vérification entre le contenu de l'original et la copie, on peut penser que la condition de « fidélité » est respectée. Dans ce cadre, les photocopies certifiées conformes peuvent être considérées comme des traces intègres de l'acte juridique.

Ce qu'il faut donc ajouter c'est que, l'exigence d'un écrit sous forme électronique établie et conservé dans des conditions de nature à en garantir l'intégrité permet, tel que mentionné dans l'article 37 de la loi sur les transactions électroniques, d'appréhender entre autre l'écrit de la création de l'enregistrement informatique jusqu'à l'expiration de son délai de conservation

---

[18] Article 41 de la loi sur les transactions électroniques

(10 ans). Dès lors, la fonction intrinsèque d'intégrité de l'acte sous forme électronique est assurée pendant tout son cycle de vie. Cette approche fait de l'écrit électronique un document indépendant du support utilisé.

De manière générale l'écrit électronique doit etre gardé dans des conditions de nature à pouvoir toujours servir de preuve au moment opportun.

Restitution de la trace probante par la conservation

La restitution est la finalité essentielle de la conservation. L'écrit électronique doit être intelligible lisible et accessible pour être consultée ultérieurement[19].

Toutefois, la preuve par écrit définie comme une suite "de lettres, de caractères, de chiffres ou de tous autres signes ou symboles" doit être donc dotée d'une signification intelligible. Ceci signifie de manière générale que les écrits exprimés, même sous une forme chiffrée (ce qui vise directement les messages cryptés) ou de code informatique, ne vaudront preuve que si leur contenu informationnel peut être produit de façon lisible et compréhensible par l'homme.

En conséquence, pour que le juge lors d'un procès puisse retenir un écrit sous forme électronique à titre de preuve, il devra pouvoir le comprendre. La condition de l'intelligibilité qui concerne tous les écrits - qu'ils soient notamment sous forme électronique ou sur support papier - implique que le contenu informationnel de l'écrit puisse être restitué en langage clair au juge, par exemple sous la forme d'une sortie imprimée sur papier. Il convient de noter en cet endroit que l'intelligibilité de l'écrit induit qu'il soit conservé de telle sorte que cette condition soit respectée, c'est à dire que la restitution de l'écrit à plus

---

[19] Article 37 al2 sur les transactions électroniques

ou moins long terme garantisse que l'homme pourra avoir accès au contenu de l'écrit de telle sorte qu'il soit intelligible par lui.

En plus d'une trace identifiable de la personne dont l'acte émane, l'article 37 de la loi sur les transactions électroniques, impose également que l'acte soit conservé dans des conditions qui garantissent son intégrité. Dès lors, la notion de conservation ainsi exigée par ce texte renvoie à celle d'accessibilité ultérieure du document étant donné que l'intégrité demeure une fonction intrinsèque de l'écrit électronique pour qu'il puisse valoir preuve. Qui plus est, le législateur sénégalais à l'image de la France a posé le principe de la conservation de l'intégrité de l'écrit électronique .Mais ne traite pas, à juste titre des modalités et des conditions d'une telle conservation. Ainsi, pour les écrits papier, aucun texte de loi général ne précise quelles méthodes utilisées pour protéger ce support pourtant altérable par nature au fil du temps (du fait des bactéries, des insectes, de l'humidité voire des incendies notamment). Pour l'heure, la doctrine comme les acteurs de la société de l'information concernés par cette préoccupation primordiale ont réfléchi sur ce sujet. La question est importante sur le fond et correspond à un réel besoin de la pratique. Car, à quoi peut servir l'admissibilité de la preuve électronique si la conservation y afférente n'est pas résolue ? L'instauration de nouveaux prestataires de services d'archivage permettra de garantir la conservation de l'intégrité des écrits électroniques. Une telle solution serait intéressante dans la mesure où ces prestataires de services contribueraient utilement à assurer la traçabilité des actes juridiques électroniques au moment où même le code civil a tourné une page pour s'adapter à l'ère du numérique. En tout état de cause, pour répondre à l'obligation d'intelligibilité de l'acte et d'accessibilité ultérieure de la trace probante, la conservation devra donc être

faite dans de bonnes conditions, afin que les écrits électroniques soient admis en preuve.

La conservation doit également permettre le déplacement des écrits sur différents supports sans altération. Cette caractéristique nous semble fondamentale dans la mesure où l'évolution des technologies est susceptible à plus ou moins brève échéance de rendre techniquement possible la réalisation de faux indétectables en cassant la clé de signature conservée avec l'écrit électronique.

Il convient toutefois de préciser que La signature électronique, comme garantie de la fiabilité de l'écrit numérique n'est plus à démontrer.

Elle permet également, par un procédé cryptographique, de garantir l'intégrité du document signé et l'identité du signataire. La cryptographie est une technique ayant pour but de chiffrer un message, c'est-à-dire de le rendre inintelligible aux yeux de ceux qui ne sont pas les destinataires du message.

Avec la signature électronique, on va utiliser la méthode de la cryptographie asymétrique, c'est-à-dire qu'on va chiffrer le document que l'on souhaite envoyer à l'aide d'une clé et pour déchiffrer (c'est-à-dire rendre le message intelligible), le destinataire devra utiliser une autre clé : ceux que l'une peut faire, seule l'autre peut le défaire. Les deux clés sont délivrées par un organisme tiers de confiance, que l'on appelle le prestataire de service de Certification. Les deux clés sont désignées sous le terme de clé privée et de clé publique. La clé privée est une clé unique et personnelle qui est utilisée pour le chiffrement, tandis que la clé publique est celle que l'on remet à tous ceux dont on veut faire se procurer la clé publique auprès du prestataire de service de certification.

Le législateur a certes admis l'écrit électronique en preuve au même titre que l'écrit support papier lorsque les conditions sus évoquées sont réunies mais il existe toutefois des restrictions à cette recevabilité.

Section : II les restrictions apportées à la recevabilité de la preuve numérique

L'arrêt rendu par la deuxième chambre civile de la Cour de Cassation le 4 décembre 2008 (pourvoi n° lire le document, la clé qui servira donc au déchiffrement du message. On peut 07-17622) pose une remarquable première pierre à l'édifice jurisprudentiel qui reste à construire concernant la reconnaissance par les tribunaux de la valeur probatoire de l'écrit numérique.[20] Il affirme qu'aux yeux du juge, la valeur probatoire de tout écrit électronique repose sur la capacité de la partie dont il émane de démontrer que les conditions de l'article 1316-1 du Code civil sont remplies, à savoir : possibilité d'identifier son auteur et garantie de son intégrité depuis sa création et pendant toute sa durée de conservation. Cet arrêt précise que l'écrit numérique doit être horodaté, ce que la loi ne mentionne pas.

Le juge ne peut dés lors rejeter par avance un email[21], une copie d'écran Web, une adresse IP au motif que la preuve est justement un email, une copie d'écran Web ou une adresse IP. Non, la Loi inverse le système : ces preuves sont par avance admissibles : en revanche, la preuve devra emporter la conviction du juge et il pourra la rejeter à une double condition : d'abord parce

---

[20] Commentaire d'Isabelle Renard du1er arrêt rendu sur la preuve numérique voir www.legifrance.gouv.fr

[21] O. ITEANU preuve numérique devant les tribunaux illustration des difficultés par l'adresse IP http://blog.iteanu.com/php?techologie

que la pièce ne le convainc pas et il devra dire pourquoi, ensuite et corrélativement, en motivant son rejet.

Cette preuve, ne doit pas non plus être obtenue en violation des libertés individuelles.

Paragraphe I : l'intime conviction du juge

Tous les éléments de preuves recueillis, sont soumis au juge qui a un pouvoir souverain d'appréciation et qui décide selon son intime conviction, une notion utilisée souvent en droit pénal mais qui garde son importance avec l'apparition des nouvelles technologies.

A -la notion d'intime conviction en droit pénal

Lorsqu'on parle de l'intime conviction, cela veut dire que la valeur probante des différents éléments de preuve, produits devant le juge du fait, est laissée à sa libre appréciation.

La conviction c'est donc le sentiment intérieur, la certitude de la culpabilité ou de la non-culpabilité. C'est ainsi qu'aux termes des dispositions de l'article 330 du Code de Procédure Pénale, le Président donne lecture de l'instruction suivante aux jurés avant qu'ils ne se retirent dans la salle de délibération, « la loi ne demande pas compte aux juges des moyens par lesquels ils se sont convaincus, elle ne leur prescrit pas de règles desquelles ils doivent faire particulièrement dépendre la plénitude et la suffisance d'une preuve ; elle leur prescrit de s'interroger eux-mêmes dans le silence et le recueillement et de chercher, dans la sincérité de leur conscience, quelle impression ont faite, sur leur raison, les preuves rapportées contre l'accusé, et les moyens de sa défense.

La loi ne leur fait que cette seule question, qui renferme toute la mesure de leurs devoirs : "Avez-vous une intime conviction ? »

La force probante des éléments de preuve relève dés lors du pouvoir souverain d'appréciation du juge.

Aux termes des dispositions de l'article 414 alinéa 2 du Code de Procédure Pénale [22]« le juge ne peut fonder sa décision », son intime conviction « que sur des preuves qui ont été apportées au cours des débats et discutées devant lui ». L'intime conviction du juge peut ainsi être considérée comme une restriction au principe de la liberté de la preuve en matière pénale. Elle est la conséquence naturelle d'un système de preuve morale

Mais elle peut néanmoins constituer une limite à la recevabilité des nouveaux modes de preuve qui ont vu le jour avec l'avènement de la nouvelle technologie dans la mesure où, le juge peut rejeter les éléments de preuve contenu dans le disc dur d'un ordinateur ou un fichier électronique s'il n'est pas convaincu.

B-L'intime conviction du juge face à la nouvelle technologie

Même si avec la loi du 13 mars 2000, reprise par la loi sénégalaise sur les transactions électroniques, toute preuve est admissible indépendamment de son support il n'en demeure pas moins que le dernier mot revient au juge qui a un pouvoir souverain d'appréciation sur les éléments de preuves portés devant lui ;

Si nous prenons un exemple en matière pénale avec la liberté de la preuve, l'accusation et la défense peuvent utiliser tous les moyens possibles

[22] Equivaut a l'article427du code de procedure pénale français

parmi lesquels nous avons les moyens électroniques comme les photographies numérisées, les enregistrements , ou des éléments contenu dans le disque dur d'un ordinateur ou dans le réseau mais encore, faudrait il que ces preuves électroniques soient assez édifiants pour emporter la conviction du juge.
Il revient ainsi au juge de déterminer, librement et en toute conscience, si les preuves numériques, qui lui sont présentées, emportent sa conviction.
Les juges ne pouvant pas écarter par principe aucun moyen de preuve, il reste pour eux à déterminer non pas la recevabilité mais bien la valeur probante des preuves numériques qui auront été collectées.

Pour ce faire, « le juge décide d'après son intime conviction » (art. 427 CPP français), tous les éléments de preuve apportés étant laissés à sa « libre appréciation » Comme Jean Pradel, éminent auteur du droit pénal et des sciences pénales, il est permis de considérer que l'intime conviction est l'équivalent exact du concept anglo-saxon de « beyond reasonable doubt » (au-delà du doute raisonnable) c'est-à-dire, selon la formule de preuve recueillie de manière illégale. Il incombe alors au tribunal de rechercher si le procès a présenté dans son ensemble un caractère équitable .

Pour autant, la décision du juge ne repose pas sur un simple raisonnement de type probabiliste. En effet, si l'on en admettait l'hypothèse dans le cadre d'un conflit de preuve littérale (ou preuve par écrit), le juge devrait alors considérer au regard des statistiques émises en matière d'écrit et de signature électronique, que les systèmes informatiques sur lesquels ils reposent, possèdent (au moins pour certains) une force probante supérieure à celle du papier. Au contraire, conformément aux articles 1316-2 et 1316-3 du Code civil, l'écrit sur support électronique a bien la même force probante que l'écrit sur support papier et c'est

le juge (et non pas les statistiques) qui détermine « par tous moyens le titre le plus vraisemblable, quel qu'en soit le support [23]».

Ainsi, chargés d'apprécier librement la fiabilité des preuves numériques présentées devant eux, les tribunaux ont pu rendre, notamment dans le domaine commercial, des décisions très disparates, dont l'analyse permet néanmoins de tirer quelques enseignements.

Lorsqu'il admet la force probante de la preuve électronique, le juge s'appuie généralement sur plusieurs preuves concordantes.

Le juge (comme le législateur) tend à réclamer une preuve que l'on considère généralement difficile à rapporter, à savoir la preuve négative de l'absence de négligence ou de tout dysfonctionnement du système.

Dans ce cas il est obligé de recourir à son intime conviction.

Il apprécie ainsi de manière libre et discrétionnaire tous les éléments de preuve produits et les arguments de la défense. Il n'est pas tenu de s'expliquer sur les éléments de preuve qui ont emporté sa conviction. La force probante de ces éléments de preuve relève de son pouvoir souverain d'appréciation. Ce qui pourrait expliquer le rejet des fois de certaines preuves obtenues par le biais de l'Internet ou des nouvelles technologies de manière générale mais en rejetant, il est tenu de dire le pourquoi en motivant son rejet.

Ce qui veut dire donc que cette intime conviction du juge doit dans tous les cas être affirmée en des termes non équivoques et non en de simples probabilités.

---

[23] Voir article 39dela loi sur les transactions électroniques

Il faut également ajouter que le juge en appréciant les éléments de preuves portés à sa connaissance doit également veiller à ce qu'ils ne portent pas atteintes à la vie privée des personnes.

Paragraphe II : la protection des libertés individuelles

La liberté de la preuve ne saurait autoriser le recours à toute sorte de pratiques et excès. En effet, certains modes de preuve sont proscrits depuis longtemps, car attentatoires aux libertés individuelles.

Dans un Etat de droit, la question de la preuve est nécessairement soumise au principe de la légalité et au respect des droits fondamentaux de chaque individu.

L'administration de la preuve, c'est-à-dire sa recherche et son recueil, doit se faire en respectant la légalité tant procédurale que matérielle.

Cette dernière est constituée par certains principes généraux que doivent respecter les acteurs de la procédure pénale. Ces principes imposent aux acteurs de la procédure pénale d'agir honnêtement sans recourir à des ruses ou stratagèmes.

En effet, on estime que l'obtention de la preuve en droit ne peut se faire au prix de violations des libertés individuelles. C'est ainsi qu'aux termes des dispositions de l'article 12 de la déclaration universelle des droits de l'homme « nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance »

Et c'est cette protection de la vie privée, devenue de plus en plus difficile à l'heure actuelle, surtout avec l'apparition des nouvelles technologies de

l'information, qui a entrainé l'apparition d'un nouveau concept celui des données à caractère personnels qui nécessite une très grande protection.

A- l'apparition de la notion de données à caractère personnel

Les enjeux attachés à la protection de la vie privée deviennent de plus en plus importants mais aussi plus compliqués à aborder au niveau individuel sous l'ère numérique.

Peu à peu émerge le concept d'*identité numérique*[24], dont la *vie privée numérique*, évoquée ici, est la partie relevant de cette intimité, en principe protégée par les lois (notamment l'article 9 du code civil, et les articles 226-1 et suivants du code pénal), mais parfois mis à mal par Internet dont la transnationalité fait parfois échec aux législations et aux juridictions nationales. Comment, par exemple, se prémunir ou se défendre contre la divulgation d'informations relevant de sa vie privée et pouvant nuire à l'intéressé, sur un blog canadien ou néo-zélandais ? C'est toute la question de plus en plus connue sous le nom d'*e-réputation* ou de *web-réputation* : la *réputation numérique* [25]d'une personne, notamment via les réseaux sur Internet (forums, réseaux sociaux…)

Chacun devrait être conscient que l'usage des données à caractère personnel doit être entouré de garanties appropriées en termes de loyauté, de proportionnalité et de transparence des traitements et de préservation de la confidentialité et de la sécurité des données.

---

[24] Didier Frochot les données à caractères personnels ; http://www.les-stratèges.com/tag/

[25] ibid

Ouverte à la signature le 28 janvier 1981, la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe reste dans ce domaine l'instrument juridique international de référence et a largement inspiré les directives adoptées en la matière par l'Union européenne le 24 octobre 1995 (protection des données personnelles et libre circulation) et le 12 juillet 2002 (vie privée et communications électroniques)

Le Sénégal, à l'instar des pays européens surpris par l'ère de la souri a voulu mettre en place un système de sécurité destiné à la protection de la vie privé d'autant plus que les données à caractère personnel se révèlent être des ressources très convoitées. C'est ainsi qu'il a été mis en place la Loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel dans le but de lutter contre les atteintes à la vie privée susceptibles d'être engendrées par la collecte, le traitement, la transmission, le stockage et l'usage des données à caractère personnel.

Si on se réfère à l'article 2 de la loi Informatique et Libertés française, constitue une « donnée à caractère personnel » « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son

identification, dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne[26]. »

Cependant l'étendue à donner à cette notion n'a pas été sans susciter quelques problèmes. En effet, si l'identification des données directement nominatives « (accompagnées d'une identification) ne pose aucune difficulté celle des données indirectement nominatives « est affectée d'un coefficient d'incertitude ».

En effet, ces données permettant d'identifier une personne sans être accompagnées de leurs identités (numéro d'immatriculation, de téléphone, de voiture, adresse IP, peuvent être considérées comme personnel si le numéro est attribué à une seule personne. Il en est ainsi des numéros d'immatriculation à la sécurité sociale, des numéros fiscaux des empreintes digitales etc.

La question de la qualification de l'adresse IP en tant que « donnée à caractère personnel » au sens de la loi Informatique et Libertés du 6 janvier 1978 est déterminante, à l'heure de rechercher et de constater des actes de contrefaçon commis sur Internet par le biais, par exemple, de logiciels permettant la mise à disposition de fichiers musicaux.

L'adresse IP fait en effet partie des données de trafic conservées pendant un an par les opérateurs de communication électronique, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales (article L.34-1 du Code des Postes et des Télécommunications Electroniques). Il est possible, à partir de cette adresse IP, d'identifier le titulaire de l'abonnement

---

[26] Voir aussi son pendant en droit sénégalais, l'article 1er de la loi sur la protection des données à caractère personnel

Internet à partir duquel a été commis l'infraction reprochée. Cette identification est, le plus souvent, rendue possible sur requête adressée à un juge et ordonnant au fournisseur d'accès à Internet de communiquer l'identité des abonnés concernés.

Ainsi, dans un avis du 20 juin 2007[27] relatif au concept de données à caractère personnel considéré les adresses IP comme des données concernant une personne identifiable, en précisant que les fournisseurs d'accès à Internet et les gestionnaires des réseaux locaux peuvent, en utilisant des moyens raisonnables, identifier les utilisateurs Internet auxquels ils ont attribué des adresses IP du fait qu'ils enregistrent systématiquement dans un fichier les dates, heures, durées et adresses dynamiques IP données à l'utilisateur d'Internet
Dans une affaire du 6 septembre 2007, le Tribunal de Grande Instance de SAINT BRIEUC[28] a estimé que l'adresse IP n'était, au même titre qu'un numéro de téléphone, que l'identifiant d'une ligne déterminée, mais pour laquelle un abonnement était souscrit par une personne déterminée. Dans ces circonstances, il a estimé que l'agent assermenté avait, du fait du recours à des logiciels spécifiques lui ayant permis d'obtenir l'adresse IP de l'ordinateur à l'origine d'une infraction, effectué un traitement de données à caractère

---

[27] Par Blandine Podevin et Viviane Gelles. L'adresse IP une donnée à caractère personnelle ?
http://www.legalbiznext.com/droit/-potection des-donnees-

[28] TGI ST BRIEUC 6septembre 2007 Ministère public et autres c/P

personnel ne respectant pas les formalités préalables à la mise en œuvre d'un tel traitement, prévues par la loi Informatique et Libertés.

Plus récemment, la Cour de Cassation[29] est intervenue pour rappeler que les constatations visuelles effectuées sur Internet par un agent assermenté sans recourir à un traitement préalable de surveillance automatisé, en utilisant un appareillage informatique et un logiciel de paire à paire, pour accéder manuellement aux fins de téléchargement à la liste des œuvres protégées irrégulièrement proposées sur la toile par un internaute dont il se contente de relever l'adresse IP pour pouvoir localiser son fournisseur d'accès, en vue de la découverte ultérieure de l'auteur des contrefaçons, rentraient dans les pouvoirs conférés à cet agent et ne constituaient pas un traitement de données à caractère personnel.

C'est dire donc que la facilité des intrusions ou divulgations de données à caractère personnel est apparue comme une menace pour la vie privée, les libertés individuelles et publiques. Ce qui soulève désormais la question de la protection des ces données à caractère personnel.

B - La protection des données à caractère personnel

La question, de la protections de ces données est aujourd'hui particulièrement préoccupante du fait du développement surtout du commerce électronique qui se fonde notamment sur un "marché" des données personnelles : celles-ci sont en effet des outils de marketing permettant au commerçant de fidéliser son client en lui proposant un service sur mesure déduit de l'analyse de

---

[29] C cass. ch crim 13janvier 2009

Voir www.legifrance.gouv.fr

son comportement sur le réseau. Ainsi, les annonceurs publicitaires ont recours à des spyware[30] ou logiciels espions, installés sur l'ordinateur à l'insu de l'utilisateur, qui collectent des informations sur l'internaute ou ses habitudes de connexion.

Un autre phénomène mettant en danger la protection des données personnelles des internautes se développe actuellement : le phishing ou hameçonnage. Il s'agit d'un courrier électronique qui persuade l'utilisateur de révéler des données personnelles sensibles par usurpation d'identité en imitant un site internet censé représenter une véritable société. Le courrier électronique non sollicité a donc cessé d'être une simple nuisance et devient peu à peu une activité de nature frauduleuse.

Il n'existe pas en outre de parade absolue garantissant l'échec des tentatives de vol d'informations sur internet mais des outils technologiques se développent comme les pare-feu, le cryptage des données, les outils de filtrage du courrier électronique ou encore les services de signalement des "pollupostages" par les internautes.

Le Sénégal, suite à la loi française 78-17 du 06 janvier 1978, a réagi contre les atteintes à la vie privée liées à l'utilisation de l'informatique relative aux données à caractère personnel à travers la loi n°2008-12 du 25 janvier 2008 qui réprime tout traitement de donnée à caractère personnel lorsque le consentement de la personne concernée n'est pas obtenu.

Cette loi est considérée comme une avancée considérable pour la protection de la vie privée dans l'époque actuelle ou les infractions sont

---

[30] www.ladocumentationfrançaise.fr/dossiers:internet-mondeglossaire.shtml/ spyware

commises tous les jours par le biais de l'informatique et au mépris même des données nominatives c'est dire donc que l'utilisation des nouvelles technologies, présente des dangers pour la vie privée et les libertés de chacun. L'information qui y circule se rapporte le plus souvent à des personnes physiques. Elle est liée à des actions de la vie courante (surfer sur Internet) ou à l'utilisation des bases de données professionnelles. Ces informations personnelles peuvent être constituées, utilisées, communiquées ou vendues, parfois à votre insu. De ce fait, les risques d'abus ne cessent de grandir.

Les objectifs de la présente loi visent donc à lutter contre les atteintes à la vie privée susceptibles d'être engendrées par tout traitement des données à caractère personnel permettant d'identifier directement ou indirectement une personne, et ces atteintes ne peuvent être sanctionné que par la réunion de preuves adaptées au modernisme, mais qu'elle est donc leur place dans nos système juridiques actuels ?

Chapitre II : L'impacte de ces modes de preuves dans les systèmes juridiques actuelles.

La société évolue, son droit avec lui. Les dossiers contentieux présentés devant les Tribunaux comportent de plus en plus de pièces versées au débat judiciaire par les parties issues de l'identité numérique. Pour cause, les procès sont issus de faits ayant pris place en totalité ou en partie sur le réseau. Le salarié licencié au motif qu'il échangeait des e-mails en trop grande quantité avec l'extérieur, l'entreprise qui poursuit son client qui lui refuse le paiement d'une commande passée sur son site Web, la banque victime d'une tentative d'intrusion sur son site de banque en ligne etc. ....

Ces différents exemples posent un problème de taille pour le praticien du droit. Comment convaincre, un tribunal correctionnel du bien fondé d'une prétention dont les éléments de preuve sont sur le disque dur d'un ordinateur, dans une boite à lettres électronique, dans le réseau ? Sont autant d'éléments qui méritent réflexion.

Section II : la place de l'écrit et de la signature électronique sur le plan pénal

Les nouvelles technologies ont entrainé de nouvelles formes de criminalité auxquelles il faut lutter mais encore faudrait il trouver des preuves appropriées pour le faire dans la mesure où les preuves classiques ne sont plus adaptées, tout se déroule Dans le cyber espace.

La preuve numérique permet donc de prouver les agissements frauduleux commis par le biais des nouvelles technologies c'est donc au moyen de lutte non

négligeable contre la cybercriminalité. Toutefois, le juge doit s'attendre à une bataille juridique su la force probante des ces éléments de preuves recueillis.

Paragraphe I : un moyen de lutte contre la cybercriminalité

La prolifération, des nouvelles technologies de l'information et de la communication a suscité une multiplication de nouveaux types de délits liés à l'information qui constituent une menace non seulement pour la confidentialité, l'intégrité et la disponibilité des systèmes informatiques mais aussi pour la sécurité d'infrastructures.

L'irruption de ce nouveau phénomène dénommé, cybercriminalité renvoie à l'ensemble des délits et infractions susceptibles d'être réalisés ou favorisés par l'usage des nouvelles technologies, notamment Internet. Elle constitue un prolongement naturel de la criminalité traditionnelle.

Ces nombreux délits informatiques se commettent de manière anonyme et les traces qu'ils laissent sont fugaces. Il est donc nécessaire de pouvoir agir vite avant que les preuves de la commission d'un délit ne disparaissent. Des moyens d'identification des auteurs des infractions sont également indispensables.

Mais il faut cependant noter que lorsque que ces preuves, aussi éphémères qu'elles soient, sont stockées dans un système informatique ou dans un support permettant de conserver ces données, le juge d'instruction en cas de besoin peut opérer une perquisition ou accéder à un système informatique.

A - La recherche et la conservation rapide des données informatisées

Les systèmes d'information constituent un important progrès pour nos sociétés, mais présentent aussi des risques et des vulnérabilités dont il est nécessaire de prendre conscience. Ainsi, depuis que l'*Internet* s'est développé dans le grand public, il ne se passe pas une semaine sans que les médias ne rapportent une affaire liée, de près ou de loin, à l'utilisation frauduleuse des réseaux.

Ainsi ,donc, lorsqu' une procédure est engagée devant le juge pénal contre ces pratiques illégales commises via l'informatique, et qu'il existe des raisons de penser que des donnés informatisées archivées dans un système informatique sont particulièrement susceptibles de perte ou de modification, le juge d'instruction peut, au cours de l'information , faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée au moins de deux ans maximum pour la bonne marche des investigations judiciaires.[31]

C'est dire donc que la volatilité des informations numériques constitue un obstacle de taille en matière de recherche des preuves, et de lutte contre la cybercriminalité dans la mesure ou celles-ci peuvent disparaître instantanément d'où la nécessité pour le juge de les conserver avant leur disparition .

Et cette volatilité ne s'explique, entre, autre que par les possibilités de modifications de déplacement voir même de destruction des données.

Force est de constater également que l'émergence d'actions et d'attentats terroristes a accéléré les évolutions législatives concernant les réseaux numériques et l'*Internet*. Ainsi, la loi française du 15 novembre 2001 a posé le

[31] Article67?-35 de la loi sur la cybercriminalité

principe de la conservation pour une durée d'un an des données de connexion des abonnés par les opérateurs de téléphonie fixe et mobile et aux fournisseurs d'accès à *Internet* pour les besoins d'une procédure pénale.

Le texte pose un principe, celui de l'effacement des données, accompagné de trois exceptions autorisant la conservation des données de connexion, à savoir d'une part la recherche, la constatation et la poursuite des infractions pénales, pour les besoins de facturation des entreprises et pour des questions de sécurité informatique.

La loi permet aussi aux autorités judiciaires de disposer désormais de moyens renforcés de l'Etat couvert par le secret de la défense nationale aux fins de procéder à un décryptage des données. Tel est le cas lorsqu'un moyen de cryptologie aurait été utilisé pour commettre un crime ou un délit en matière de terrorisme par exemple.

Ce qu'il faut également noter, c'est qu'il faut certes une conservation rapide de ces éléments de preuve du fait de leur caractère éphémère pour éviter quelle ne disparaissent mais cela soulève aussi le problème de leur conservation dans le temps d'autant plus qu'elles doivent être gardés dans des conditions de nature à garantir leur intégrité et de ce fait faciliter le travail du juge.

Si on se réfere à l'article 677-35 « de la loi sur la cybercriminalité » le juge peut faire injonction à ce que les données soit conserver pendant une durée maximum, il se posera dans tous les cas, un autre problème celui de la brièveté du délai de prescription de certaines infractions commises par tous moyens de diffusion publique.

Ce qui constitue un handicap sérieux pour la lutte contre ce fléau car à quoi bon de collecter et de conserver des éléments de preuve si avant d'entamer des poursuites l'infraction est prescrite dans la mesures ou certains actes commis à travers internet (par exemple la diffusion d'images pornographique sur internet) sont assimilés aux infractions commis par tous moyens de diffusion publique au sens de l'article 248 du CP Selon ce texte « sont considérés comme moyen de diffusion publique, la radio-diffusion, la télévision, le cinéma, la presse, l'affichage, l'exposition, la distribution d'écrits ou d'images de toutes natures, les discours, chants, cris ou menaces préférés dans les lieux ou réunions publiques et généralement tous procédé technique destiné à atteindre le public ».

Dans tous les cas, l'émergence du cyberespace amène à poser la question suivante : Internet, véhicule des messages contraires à l'ordre public peut-il être considéré comme un moyen de diffusion publique, au sens des dispositions de l'article 248 du code pénal ? C'est donc, cette question qui a amené
La jurisprudence sénégalaise à se prononcer dans le jugement n° 2 rendu par le tribunal régional de Ziguinchor le 06 janvier 2004.[32]

Dans cette affaire, Christian Costeaux a été prévenu d'avoir diffusé sur son site dénommé « sénégalaisement. com » des propos diffamatoires contre Robert Sagna maire de Ziguinchor et propriétaire de l'hôtel « Kadiandoumogne », propos aux termes desquels, le maire se livraient « à une concurrence déloyale dans l'irrespect des Casamançais ».

Le juge correctionnel de Ziguinchor a estimé que « l'outil Internet en cause qui constitue un réseau international permettant à des personnes habitant divers endroits du monde et disposant d'ordinateurs de communiquer entre elles» constitue un « procédé technique destiné à atteindre le public », c'est-à-dire un moyen de diffusion publique au sens de l'article 248 du code pénal. Christian Costeaux fut ainsi déclaré coupable du chef de diffamation condamné à un an d'emprisonnement ferme et un mandat d'arrêt international fut décerné contre lui.

En effet, c'est la qualification de « procédé technique destiné à atteindre le public » qui a été retenu par le juge ce qui veut dire que lorsque l'infraction effectuée au moyen de l'internet vise à atteindre le public on est donc dans le domaine des délits de presse et par conséquent elle sera soumis au régime de prescription des infractions commises par tous moyens de diffusion publique[33].
Mais la plus grande difficulté est aujourd'hui il faut le dire c'est celui de la recherche de preuve il est parfaitement possible de nos jours de se promener dans un système ou dans un réseau , de s'introduire illicitement sur des réseaux clients ou serveur pour s'emparer des donnés qui y sont stockées ou introduire dans le serveur des virus ; Même si ces comportements sont répréhensibles et sanctionnés dans la plupart des législations, il n'est toujours pas aisé de déterminer compte tenu du nombre d'intervenants celui qui doit être tenu pour responsable , ce qui soulève donc le problème de l'imputabilité.

Il ne fait pas de doute que la détermination de l'auteur de l'acte et leur poursuite peuvent s'effectuer facilement lorsqu'il s'agit d'actes consistant à

[33] Voir pour la distinction article431-63de la loi sur la cybercriminalité.

accéder et à se maintenir dans le système mais la situation est souvent différente lorsqu'il y utilisation de l'espace électronique pour véhiculer certaines informations. L'adaptation des règles de procédure pénale est d'autant plus nécessaire que les délinquants ont recours à des méthodes de plus en plus sophistiquées pour rendre impossible la découverte de leurs agissements c'est pourquoi la cryptologie constitue un enjeu considérable dans un environnement dématérialisé ou la quasi-totalité des relations s'établit à travers les systèmes électroniques d'informations[34].

Malgré cette tentative d'encadrement du recours à la cryptologie, certains fabriquant mettent au point des logiciels du chiffrement qui assurent même une protection contre les écoutes légales .Et en ce qui concerne certains malfaiteurs, ils n'ont pas attendu la vente de logiciels de déchiffrement pour stocker dans leurs ordinateurs des données codées auxquelles les autorités peuvent difficilement accéder en mettant en œuvre les moyens classiques .

Tout ce ci démontre que la lutte contre cybercriminalités ne peut se faire que par la recherche et la conservation des preuves numérique et l'identification de leur auteur , ce qui est d'ailleurs trés difficile à mettre en œuvre d'autant plus que les enquêteurs et le juge lui-même ,confrontés à la nouvelles technologies ne peuvent utilisés que les méthodes classiques en les adoptant à l'environnement des TIC.

B -les procédés d'interception de perquisition et de saisie

---

[34] Voir article de Ndiaw Diouf sur les infractions en relation avec les nouvelles technologies de l'information et procédure pénale

Il faut noter qu'en cas de commission d'infractions par le biais des nouvelles technologies de l'information, les autorités de la recherche de preuves mènent l'enquête dans le cadre d'actes classiques de la procédure pénale perquisitions saisie.

La perquisition est effectuée dans les conditions posées par l'article 85 du code de procédure pénal qui dispose « que les perquisitions sont effectuées dans tous les lieux ou peuvent se trouver des objets dont la découverte serait utile à la manifestation de la vérité ».

Dans cette même optique l'article 677-36 donne aussi pouvoir au juge d'instruction de procéder à une perquisition lorsque les données stockées dans un système informatique ou dans un support sont utiles à la manifestation de la vérité.

Cette perquisition ne pose aucun problème lorsqu'il s'agit de vol de disque ou de cd mais il en est autrement lorsqu'il s'agit de réunir des preuves contre une personne poursuivie pour avoir manipulé le système informatique d'autrui ou pour avoir stocké des informations illicites.

Cette mesure peut se révéler inefficace dés fois lorsqu'il s'agit d'agir dans un lieu virtuel ou immatériel.

Le respect de certaines dispositions du code de procédure pénale en matière de perquisition est souvent difficile à mettre en œuvre, en ce sens que, par exemple dans certaines législations ou la perquisition doit s'effectuer en

présence de la personne chez laquelle elle a lieu[35]. Et dans ces pays l'accès à un système afin de constituer une preuve ne se prête guerre à ce formalisme.
La suite logique d'une perquisition fructueuse serait donc la saisie des données trouvées et qui sont susceptibles de servir à la manifestation de la vérité , cette saisi ne peut se faire que par le respect de certains formalisme telles que la mise sous scellés conformément aux dispositions de l'article 88 du code de procédure pénale « tous objets et documents saisis sont immédiatement placés sous scellés ».

Une telle mesure conçue pour des objets corporels matériels peut difficilement être mis en œuvre pour les besoins d'une procédure initiée contre l'auteur de la transmission d'informations illicites ;

Il est vrai qu'on peut envisager la saisie des supports d'informations mais la difficulté réside dans le fait qu'il serait extrêmement fastidieux de savoir si une telle saisie englobe les informations qu'ils sont supposés contenir.

Le problème reste entier même si dans certain pays on a essayé de surmonter cette difficulté c'est le cas par exemple de la Luxembourg qui a admis que la saisie des supports matériels d'information engendrent celles des données qu'ils sont supposés contenir[36]

De même que la saisie des supports peut également se révéler impraticable lorsque les données utiles à l'établissement et la poursuite de l'infraction sont disséminées dans tout le système informatique d'une entreprise.

---

[35] Article86et87du code de procédure pénale sénégalais

[36] Pape A Touré. Le traitement de la cybercriminalité devant le juge sénégalais mémoire de DEA , université Gaston Berger de Saint Louis

C'est particulièrement le cas lorsque l'entreprise est une multinationale et héberge des données dans des systèmes informatiques localisés dans différents Etats.

Par exemple la loi belge du 28 novembre 2000 n'autorise pas la saisie de données immatérielles.

Seules les données stockées sur un support informatique, disquettes, CDs ou disques durs, étaient donc généralement saisies.

C'est d'ailleurs conscient de ces difficultés que le comité des ministres du conseil de l'Europe a rappelé dans une recommandation n° (95), 13[37], la nécessité d'adapter les règles de procédure pénale « de permettre aux autorités chargées de l'enquête de perquisitionner dans le système informatique et d'y saisir des données dans des conditions similaires à celles utilisées dans le cadre des pouvoirs traditionnels de perquisition et de saisie.

Dans tous les cas, il est encore nécessaire de doter le magistrat instructeur de moyens plus pratiques, lui permettant d'effectuer des saisies de biens incorporels, tels que les données informatiques, traitées par les systèmes informatiques même si la loi lui permet de recourir au service d'experts en cas de besoin.

Paragraphe II : la bataille juridique sur la force probante de la preuve numérique

Le juge pénal peut être saisi d'une action publique tendant à réprimer une infraction par le biais de l'informatique, le juge joue un rôle actif dans la

[37] ibid

recherche de preuves. Ce qu'il faut savoir, c'est que le procès pénal est gouverné par le par le principe de la liberté de la preuve. C'est un principe qui est valable devant tous les tribunaux répressifs et qui signifie que tous les moyens de preuve sont recevables devant le juge que toutefois, dans la pratique, la loyauté et la légalité dans la recherche des preuves peuvent être un critère déterminant d'appréciation quant à la recevabilité.

A - le principe de la liberté de la preuve

La preuve électronique est admise en matière pénal en vertu même du principe de la liberté de la preuve. Ce principe a été consacré par les dispositions de l'article 414 al. 1 du Code de procédure pénale sénégalais en ces termes:

« Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tous modes de preuve et le juge décide d'après son intime conviction ».

Ce principe de la liberté de la preuve s'explique aisément par le fait que les délinquants, une fois leur forfait accompli, s'empressent de faires disparaitre toute trace de l'information. Dans ces conditions il serait hasardeux de vouloir limiter ces modes de preuve. Ainsi, tous les moyens de preuves sont admis (écrits, témoignage, aveu, perquisition, saisies ...), pourvus qu'ils aient été rapportés « au cours des débats et discutés devant le juge » (article 414 alinéa2) Force est de constater qu'on est obligé d'admettre que le juge ne peut utiliser comme fondement de sa décision que les éléments de preuves régulièrement obtenus , car même si la preuve est libre , les juges ont tendance à rejeter certaines preuves , et ce n'est pas qu'elles ne sont pas admises comme preuve

mais les procédés utilisés pour les recueillir sont déloyaux ou portent atteinte aux droits fondamentaux de la personne humaine.

Il peut arrive que la collecte des preuves soit régulière, or dans la plus part des législations, il est prévu que lorsque les éléments de preuves sont régulièrement produits aux débats, il appartient donc au juge d'apprécier souverainement leur valeur probante.

Il faut savoir que le cybercriminel opère généralement seul depuis son domicile ou dans un autre lieu, en tout cas à l'abri des regards indiscrets, dans ce contexte il serait très difficile d'utiliser, les autres modes de preuve même si on est dans le domaine de la liberté de la preuve. En ce sens qu'on est dans un univers particulier celui de l'immatériel du cyber espace ou le concept de flagrant délit ne joue que très rarement et personne d'autre n'est au courant des agissements du cybercriminel qui va prendre le soin de tout nettoyer sur son passage.

Le juge sera obligé de se rabattre sur des indices ou de procéder à des perquisitions qui soulèvent souvent beaucoup de problèmes.

Avec cette nouvelle technologie s'il y a une chose, c'est qu'on est jamais tout à fait sure de l'exactitude des données recueillies, on s'est demandé si les images, les sons et voix numérisés sont toujours fiables. Indépendamment des manipulations toujours possibles, la technologie, si perfectionnée soit elle laisse subsister un risque d'erreur du à un mauvais fonctionnement de l'outil informatique alors que le droit pénal recherche la certitude d'où donc la nécessité d'avoir, recours dans certains cas, au service d'un expert à la matière, d'un technicien informatique pour certaines questions.

Il faut également préciser que la loi sur la cybercriminalité pose un autre débat lorsqu'elle dispose dans son article 677-40 que « l'écrit électronique en matière pénal est admis au même titre que l'écrit sur support papier conformément à l'article 40 de la loi sur les transactions électroniques »

Alors que l'article 40 de la loi sur les transactions électroniques nous parle des cas dans lesquelles la copie ou la reproduction des actes passés par voie électroniques peut avoir la même force probante que l'acte copié et pour ce faire cette loi nous dit qu'il faut que la copie soit certifiée conforme par des organismes agrées par l'Agence de l'informatique de l'Etat .

Mais ce qu'il faut préciser c'est qu'en matière pénale la preuve est libre quelque soit le support alors que la loi sur les transactions électronique vise la matière civile ou l'admission de l'écrit numérique est contrôlée car elle obéit à certaines des conditions.

Il est également certain que dans le procès pénal le principe de loyauté dans la recherche des éléments de preuve de l'infraction occupe une place importante.

B -la légalité et la loyauté dans la recherche de preuves

Le Doyen Carbonnier écrivait à propos de la *loyauté* procédurale: « Les coups bas sont interdits, les simples ruses de guerre ne le sont pas ». Toute la question est alors de déterminer la limite entre les méthodes qui relèvent des « coups bas » et celles qui ne sont que des « ruses de guerres ».

La recherche de preuve des infractions commis au moyen de l'informatique est également soumise au respect des normes édictées par la jurisprudence, et les juges accordent une importance particulière aux moyens

déployés pour obtenir ces preuves. C'est ainsi que le caractère loyal est souvent mis en exergue dans l'étude de la recevabilité de celle ci.

En effet, la recherche doit être menée de façon loyale et franche à visage découvert, sans recours à la ruse ni à la dissimulation.

Compte tenu de l'exigence de la régularité dans la recherche des preuves, les preuves obtenues au moyen de procédés électroniques mis en œuvre en prescription légale doivent donc être écartées des débats car même si le recours aux procédés électroniques est admis, c'est sous réserve que les preuves soient légalement obtenues. Dans ce cas, une preuve obtenue au moyen d'intrusion dans un système informatique, situé à l'étranger, en violation des règles en vigueur doit etre simplement rejeté et vertu du principe de loyauté dans la recherche de preuve.

Il ya lieu de rappeler que pour certaines infractions liées aux nouvelles technologies ce sont les victimes elles mêmes qui organisent et collectent la preuve des agissements et elles peuvent être tentées de mettre en œuvre dans un but probatoire des procédés illicites de repérage et de fichage de ceux qui accèdent à leur système

Lorsque les preuves ont été régulièrement recueillies il appartiendra au juge d'en apprécier la valeur probante. C'est ce qu'on appelle le système de l'intime conviction qui dispense au juge « de rendre compte du cheminement par lequel il est parvenu à la certitude »

Toutefois il faut signaler que le principe de la loyauté peut connaitre certaines restrictions relatives à la défense des intérêts supérieurs de la Nation, il en est ainsi des infractions relatives aux atteintes à la sûreté de l'Etat, au terrorisme...etc.

Dans tous ces cas la preuve obtenue d'une manière déloyale, peut en comparaison avec l'intérêt sauvegardé, être déclaré recevable par le juge.

Section I : la preuve numérique en matière civile

L'apparition de l'informatique et le développement du commerce électronique a été freiné par les craintes engendrées par la dématérialisation des opérations et le remplacement du support papier par un support électronique (sur écran). En effet le contrat par l'Internet étant dématérialisé à la différence des contrats traditionnels, l'absence de support physique paraissait et parait encore générateur d'insécurité juridique. Toutefois il a été prévu des dispositions textuelles sur la preuve et la signature électronique de nature à atténuer voir à dissiper les appréhensions et par voies de conséquence, accroitre les transactions électroniques.

Paragraphe I : la réduction de l'insécurité dans les transactions bancaire en ligne

La présence de l'écrit et de la signature électronique dans les transactions bancaires ont considérablement réduit l'insécurité dans ce domaine et tout ceci , passe par la sécurisation des systèmes de paiement qui se fait par l'utilisation d'un certain nombre de procédés notamment par la signature électronique gage essentiel d'un climat de confiance.

A -la sécurisation des systèmes de paiement

La consécration des nouveaux outils nés de l'évolution technologique allait poser un certain nombre de problèmes, les auteurs du règlement 15/2002 /CM/UEMOA[38] ont expressément entendu mettre la lumière sur « l'identification de l'expéditeur ainsi que du destinataire du message de données ; la confidentialité des données transmises sur support électronique et par conséquent la sécurité des échanges dématérialisés ».

Dés lors, le nouveau dispositif vise expressément à garantir la sécurité des messages transmis ou à transmettre en permettant « d'une part, de prendre en considérations les nouveaux instruments électroniques de paiement et, d'autre part de tirer les conséquences, au plan criminel, de cette nouveauté en prévoyant un traitement approprié des infractions pouvant naitre de l'utilisation des nouveaux instruments de transfert électronique de fonds.

L'article 3 du règlement dispose que « la banque centrale veille au fonctionnement et à la sécurité des système de paiement ».
Des études ont montré qu'aussi bien les internautes que les marchands sont réticents en ce qui concerne le commerce en ligne du faits de nombreux problèmes et cas de fraudes dans ce domaine ;

Il faut donc trouver des solutions visant à sécuriser ces échanges. Ce qui nécessite impérativement la suppression de certains problèmes techniques pour sécuriser les paiements sur Internet. Le premier a trait à la *confidentialité*[39] des données. Ce problème est généralement résolu par l'usage de systèmes

---

[38] www.adie/docs/moussathioye.pdf

[39] Bounie. D et Bourreau M. sécurité des paiements et

Développement du commerce électronique. revu économique vol 55juillet 2004 P89

cryptographiques qui permettent le codage d'un message intelligible en un texte chiffré incompréhensible (sachant que le destinataire légitime doit pouvoir déchiffrer le texte chiffré et obtenir le texte clair). Le deuxième problème technique concerne la garantie de l'origine *(authenticité)* et de l'*intégrité* des messages expédiés. En d'autres termes, les interlocuteurs doivent être assurés que les messages n'ont pas été modifiés durant leur transit sur le réseau et que ceux-ci proviennent bien de leur partenaire en relation. Ces problèmes sont généralement résolus par l'emploi d'une signature électronique. Enfin, le troisième problème technique concerne l'*authentification* des utilisateurs. Autrement dit, il convient de s'assurer que les dispositifs, les clés électroniques, qui permettent de chiffrer et de déchiffrer les messages, appartiennent bien aux utilisateurs déclarés. Pour garantir cette authentification, un certificat électronique émis par une autorité de certification entreprise, banque, administration) est utilisé. Le certificat électronique garantit le lien entre une clé et son « propriétaire » (une personne, un routeur, un serveur).

L'ensemble de ces problèmes techniques doivent donc être résolus pour assurer un niveau de sécurité maximal des paiements sur Internet.

Plusieurs offres de sécurisation des paiements par carte bancaire, caractérisées par des niveaux de sécurité croissants, sont en concurrence sur le marché.

Ce qui veut dire donc que les transactions financières sont protégées contre les possibles altérations qui, si elles surviennent, doivent être détectées. La modalité pratique pour réaliser tout cela est d'utiliser les certificats numériques par une infrastructure de clés publiques ou de signature électronique, technique reconnue légalement dans plusieurs pays du monde.

B - un système de sécurisation par la signature électronique

Les banques se sont associées à plusieurs reprises pour mettre au point des protocoles de sécurisation des paiements qui authentifient l'internaute dans la transaction par différents procédés.

Ces systèmes ont pour ambition de réduire les risques de fraude en garantissant aux e-marchands le paiement des ventes effectuées en ligne et en supprimant pour les consommateurs le droit de répudiation des paiements. Pour ce faire, ils utilisent un système de signature électronique authentifiant à distance l'internaute.

Dans le modèle avec signature électronique, il n'existe aucune asymétrie d'information entre le e-marchand et l'internaute ; le niveau de sécurité est maximal.

Mais le coût d'un système de paiement électronique est une fonction croissante du niveau de sécurité du système.

Le système de sécurisation avec signature électronique met en relation cinq acteurs : le porteur de la carte bancaire, l'e-marchand, leurs banques respectives et l'offreur de sécurité. Pour adhérer à la solution, le porteur doit se porter acquéreur soit d'un lecteur de carte à puce sécurisé s'il possède une carte à puce, soit d'un certificat électronique (porteur étranger muni d'une carte à piste ou puce magnétique).

De même, le e-marchand obtient un certificat électronique auprès de sa banque qui l'autorise à accepter le paiement par carte bancaire. Ces dispositifs matériels ou logiciels ont pour fonction d'authentifier l'internaute et le e - marchand au cours de la transaction. L'internaute est donc assuré qu'il est en liaison avec un e-marchand certifié, c'est-à-dire reconnu par une banque et,

réciproquement, l'e-marchand est assurer de l'identité de l'internaute *via* sa signature électronique. Mais la sécurisation des paiements est coûteuse car elle implique un équipement logiciel ou matériel pour les internautes et les e-marchands.

La signature électronique voit son usage s'amplifier car, au-delà de son caractère probant, elle instaure la confiance, et permet d'augmenter le nombre de transactions effectuées en ligne (signatures de contrats, souscriptions, actes de vente, échanges de données confidentielles de consentement, etc.) et donc de favoriser le développement des affaires. Il faut se rappeler toutefois que la signature électronique permet « de satisfaire le critère de fiabilité » et d'établir une relation de confiance nécessaire dans toutes les transactions dans la mesure où elle permet d'identifier l'auteur d'acte. Et cette fiabilité au regard de la loi sur les transactions électroniques est présumée jusqu'à preuve contraire .

La signature est nécessaire à la perfection d'un acte juridique identifie celui qui L'appose. Elle est aussi la manifestation du consentement des parties aux obligations qui découle d'un acte[40]. Aucune des parties ne peut plus ce dérober ou contester une transaction en ligne dés lors qu'on a la preuve de son engagement.

Paragraphe II : Le développement des transactions électroniques dans l'univers numérique

Avec le développement des réseaux informatiques le nombre de transaction est en constante augmentation. L'informatique permet aujourd'hui

[40] Voir article 41 de la loi sur les transactions électroniques

de dématérialiser les rapports. Ainsi l'on peut s'engager en ligne à partir d'un simple clic. Plus besoin de se voir ou de se déplacer. Ce développement S'explique par la conclusion fréquente de contrat en ligne du fait de la présence de certain garanties accordées au consommateurs, à cela s'ajoute la possibilité de prouver devant le juge.

A - la conclusion de contrat dans l'univers numérique

C'est avec le développement du commerce électronique que la notion de contrat par voie électronique s'est trouvée vulgarisée. Dans le but de veiller à ce que le commerce électronique puisse bénéficier dans sa globalité aux usagers du marché, le législateur communautaire a édicté des normes visant à protéger le consommateur, partie vulnérable dans le contrat.

Ainsi, « *l'utilisation de techniques de communication à distance ne doit pas conduire à une diminution de l'information fournie au consommateur...* ». Outre les exigences en matière d'information prévues par le droit communautaire, certaines obligations sont spécifiques aux prestataires de services qui interviennent dans le réseau pour mettre les usagers dans une relation contractuelle. Outre l'obligation de rendre possible un accès facile, direct et permanent, ils doivent fournir certaines informations qui permettent de les identifier clairement.

La loi sur la confiance dans l'économie numérique10 complétée par le décret du 16 février 2005 sur l'archivage électronique et l'ordonnance du 16 juin 2005 sur la dématérialisation, des contrats, a renforcé l'information du consommateur et éclairé son consentement à toutes les étapes de la formation du contrat.

On peut cependant regretter le caractère unilatéral des obligations instituées par le législateur communautaire.

Si le consommateur profane n'a pas à prendre d'initiative et peut attendre que son cocontractant professionnel lui fournisse toutes les informations dont il a besoin, on peut au moins attendre d'un consommateur professionnel qu'il prenne l'initiative de se renseigner.

Le commerce électronique a été défini par un certain nombre d'auteurs mais au Sénégal l'article 8 de la loi sur les transactions électroniques le défini comme l'activité économique par laquelle une personne propose ou assure, à distance et par voie électronique la fourniture des biens et la prestation de service

Le développement du commerce électronique est encore très limité au Sénégal par rapport au autre pays européens du fait des nombreuses appréhensions des gens sur le monde numérique c'est en ce sens qu'a été adopté la loi n°2008 du 25 janvier 2008 sur les transactions électroniques.

Dans le contexte électronique, les contrats de vente d'un bien matériel, de services et de licence d'utilisation peuvent faire l'objet d'une preuve dans une instance. De plus, à cause des questions de sécurité inhérentes au droit, la sécurité informatique est devenue essentielle et a opéré des changements importants, notamment en ce qui a trait aux régimes de preuve. La sécurité exige alors que l'environnement soit fiable et que le document soit intègre. L'ère Internet nous a emmené à réévaluer les principes traditionnels du droit afin de nous adapter à cette révolution technologique.

C'est pourquoi, en 1996, la Commission des Nations Unies pour le Droit Commercial International (CNUDCI), proposait à ses membres une loi qui allait

servir de cadre juridique au commerce électronique : Loi modèle sur le commerce électronique (Loi modèle).

Cette dernière a servi de modèle pour plusieurs pays dont le Canada[41], qui, par la Conférence d'harmonisation des lois adoptait deux lois miroir de la *Loi modèle*, la Loi uniforme sur le commerce électronique (Loi uniforme) et la Loi uniforme sur la preuve électronique qui confirmait que l'information électronique était présentable en preuve. Vu que ces deux lois uniformes ne constituent pas des lois au sens législatif, plusieurs provinces ont adopté leurs propres législations. Puisque la preuve peut être plus difficile à faire dans un contexte électronique, les documents faisant la preuve de la transaction, deviennent primordiaux. Voilà pourquoi, les législateurs provinciaux canadiens, plutôt que de refondre leur droit en entier ont décidé d'adapter et d'élargir les concepts déjà existants. Les politiques canadiennes concernant les transactions dans le cadre du commerce électronique exigent maintenant que l'intégrité et la confidentialité soient maintenues en tout temps. Ainsi, les questions de confiance et de sécurité des transactions sont devenues essentielles. Plusieurs règles telles que les règles classiques du droit des contrats, les règles particulières au commerce électronique, les lois sur la protection du consommateur ainsi que les ententes entre les parties, sont susceptibles de déterminer le droit applicable entre les parties.

Les solutions sécurisant les transactions électroniques peuvent donc contribuer sans conteste à l'accélération et à l'automatisation des processus dont

---

[41] Dinu I .le droit de la preuve appliqué au commerce électronique au canada

Voir http://www.lex-electronica.org/articles/v11-1/dinu.pdf

ceux liés à l'acte de vente en ligne, à l'accroissement de l'efficacité, au développement de nouveaux services et à l'optimisation de la relation client.
La preuve du contrat par voie électronique constitue un autre élément qui contribue à apporter quelques garanties à l'usager qui s'y lance.

B -la preuve dans le contrat électronique

La preuve est essentielle dans l'exercice des droits. Elle permet de justifier la revendication de son droit. Il faut déterminer ce que l'on doit prouver et savoir à qui incombe la preuve. En général, le régime de la preuve dépend de la nature du litige. C'est ainsi que dans un litige ayant une nature civile, un écrit sera exigé si le litige dépasse un certain montant.

En matière commerciale, la célérité et la rapidité des opérations ont permis d'assouplir les règles de preuve. Aussi l'existence d'un droit peut être prouvé par tous les moyens.

Cependant, l'informatique est venue poser des questions nouvelles relatives à la preuve avec la dématérialisation des échanges. Comment prouver une transaction réalisée par internet ?
Quelle valeur accordée à un écrit électronique en tant que preuve ?

Quelques réponses ont été apportées par le législateur sénégalais. Ainsi, « l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier». Cependant, cet écrit n'est recevable que « sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».

Mais force est donc de reconnaitre que c'est cette loi sur les transactions électroniques qui a posé les bases de la reconnaissance des nouveaux modes de

preuve dans le but de prouver les transactions en lignes écartant ainsi les contraintes juridiques qui bloquent le recours au contrats électroniques faute de pouvoir prouver l'acceptation ou le consentement de l'autre partie.

La reconnaissance de la signature électronique et la valeur juridique reconnue à l'écrit électronique sont venues parachever ce processus de dématérialisation des rapports pour faciliter les liens contractuels.

Il convient de noter que les règles valables pour le papier le sont aussi pour le numérique et, par conséquent, celui qui veut détruire une apparence doit en prendre l'initiative.

Or, en matière informatique, la difficulté[42] est que celui contre lequel l'apparence est invoquée (« bénéficiaire de l'apparence ») sera le plus souvent le prestataire qui excipera d'un état. Par ailleurs, dans de très nombreuses conventions, seul le prestataire conservera sérieusement la trace informatique de l'opération.

Ainsi, son partenaire récalcitrant, qui n'aura pas pris les mêmes précautions, exigera et obtiendra (en pratique), pour combattre l'apparence qui lui est défavorable, que la trace informatique présente dans les systèmes du prestataire soit représentée. Ce qui, le cas échéant, aboutira, du point de vue des dogmes classiques, à un renversement de la charge de la preuve.

Dans tout les cas les règles propres à la preuve papier peuvent s'appliquer à la preuve numérique, sauf exception juridiquement explicite ou techniquement implicite

---

[42] Consulter www.adic/doocs/moussathoye.pdf

Quoiqu'il en soit, Même en cas de conflit de mode de preuve, la loi reconnaît au juge le pouvoir de choisir celui qui lui semble le plus vraisemblable. Ainsi, « lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support ».

Conclusion

Notre réflexion sur la preuve numérique nous a permis de savoir qu'à coté des preuves dites traditionnelles est apparus d'autres modes de preuves qui sont nés avec l'avènement de l'informatique et des nouvelles technologies.

L'écrit électronique au regard de l'article 1316 du code civil français sont admis comme mode de preuve qu'à condition que l'on puisse identifier son auteur et la signature électronique joue un rôle important dans ce domaine qu'elle permet d'authentifier l'auteur de l'acte auquel elle s'attache.

L'écrit pour valoir preuve doit également être conservé dans des conditions de nature à garantir son intégrité, évité que l'acte soit altéré.

Une fois que le document électronique a été jugé comme preuve il faudra décider du poids que le juge lui accorde, savoir les moyens mis en place pour obtenir ces preuves ;

Nous avons vu également que dans les sociétés modernes, nul ne songe à contester l'intérêt que représentent, pour les individus, les entreprises et les institutions, les nouvelles technologies de l'information, on ne peut que se réjouir des possibilités qu'offrent les moyens électroniques pour la collecte, le stockage, la conservation et la transmission des informations. Mais Force et de constater que le développement des nouvelles technologies engendre beaucoup de problèmes auquel il faut faire face et ces difficultés viennent en partie de l'idée, au départ que tout est permis, il n'ya plus à obéir aux conventions et aux traditions du monde réels quand on est dans le cyberespace dans la mesure ou par exemple dans l'internet on ne voit ni n'entend ceux avec qui on

communique, l'anonymat aidant, un certain nombre d'infractions y sont commises tous les jours

L'admission de l'écrit et par là de la signature électronique comme mode de preuve a été d'un grand apport pour lutter contre ces nouvelles formes de délinquance même s'il se pose à certain égard beaucoup de difficultés dans la recherche de preuves et la conservation des éléments de preuves surtout lorsque l'auteur de l'infraction est localisé à l'étranger. Dans une telle hypothèse il y a de forte chance que les éléments de preuve se trouvent aussi à l'étranger, or le principe de la souveraineté des Etats s'oppose à ce que l'activité des autorités judiciaires ou policières relevant d'un Etat puisse s'exercer en dehors des frontières de cet Etat. Une perquisition des systèmes automatisés de traitement de l'information situés à l'étranger serait indispensable. Il ne reste donc qu'une solution, solliciter de l'Etat sur le territoire duquel est situé le site (commission rogatoire internationale, communication transfrontalière de pièces) .mais on mesure immédiatement la faiblesse d'une telle solution car voit mal un Etat s'engager dans une entreprise d'entraide judiciaire ou policière qui conduit à la répression d'un agissement qu'il juge licite.

Il faut donc, pour lutter contre ceux qui se livrent à des activités illicites en utilisant les nouvelles technologies, harmoniser les législations des différents pays, car ce qui importe en fin de compte, sur le plan juridique, ce n'est pas d'édicter des règles contraignantes, mais de s'entendre sur ce qui constitue une conduite appropriée sur l'internet mais aussi de développer la coopération entre les Etats.

Dans le cadre du commerce électronique les problèmes juridiques liés à la sécurité informatique sur un réseau ouvert comme Internet ne concernent pas en

premier lieu la validité des contrats qui pourraient s'y conclure puisqu'une signature manuscrite et un support papier ne sont que rarement exigés par la loi pour les transactions en cause. La preuve n'est pas non plus impossible, même si elle risque d'être coûteuse, pour autant qu'elle s'appuie sur un ensemble de mesures préventives efficaces.

Dès lors, la véritable problématique juridique liée à la sécurité des transactions en ligne consiste à faciliter la preuve de l'intégrité des communications et l'identification des partenaires commerciaux sur le réseau.

Bibliographie

Ouvrages généraux

Benoit (A), l'écrit électronique, Paris Masson 1998

Prade (J), procédure pénal cujas, 5e édition 1990

Catala (pierre), le droit à l'épreuve du numérique, édition puf 19998

Ouvrages spéciaux

Ultmark (c), les dimensions internationales du droit du cyberespace, collection droit du cyberespace édition Unesco, Economica

Bounie(D)et Bourreau (M), sécurité des paiements et développement du commerce électronique vol 55 n°4, juillet 2004 p 689- 714

Articles

Diouf (Nd), infractions en relation avec les nouvelles technologies de l'information et procédure pénale : l'inadaptation des réponses face à un phénomène de dimension international,

Thioye (M), preuve par écrit et signature électronique, www.adie/docs/moussathioye.pdf

Caprioli (E) le juge et la preuve électronique, juriscom.net ,10 janvier 2000

Mémoire

Touré (P. A), le traitement de la cybercriminalité devant le juge sénégalais, mémoire de DEA, St louis (Sénégal)

WEBOGRAPHIE

Dinu (I) droit de la preuve appliqué au commerce électronique au canada , droit civil / Common Law http://www .lex-electronica.org/articles/v11-1/dinu .htm

Caproli (E) traçabilité et droit de la preuve http:// www.caprioli-avocats.com

Sécurité des paiements et développement du commerce électronique http://www.legifrance.gouv.fr/ppEAU.htm

Droit de la preuve sur internet http://fr.jurispedia.org/index.php

www.adic.docs.moussa.tove.p.fr

Lois et règlements

Règlements n°15/2002/CM/UEMOA relatif au système de paiement dans les Etats membre de l'union économique et monétaire Ouest Africaine.

Loi n°2008-08 du 25janvier 2008portant sur les transactions électroniques.

Loi n°2008-11du25janvier 2008 portant loi sur la cybercriminalité.

Loi n°2008-12 du 25janvier 2008 portant sur la protection des données à caractère personnel.

TABLE DES MATIÈRES