RETOUR SUR L'ADAPTATION DU DROIT AU NUMERIQUE

Par

Djibril SOW[*],
Docteur d'Etat en Droit privé, Maître-Assistant à
l'Université des Sciences juridiques et politiques de Bamako.
djibrilhamatt@gmail.com

Résumé

L'adaptation du droit au numérique apparaît comme une nécessité résultant de l'essor considérable du numérique. Le numérique offre beaucoup d'opportunités, mais engendre beaucoup de contraintes d'ordre juridique. Une assez appréciable adaptation du droit au numérique est opérée par le législateur malien et les législateurs de certaines communautés sous régionales telles que l'UEMOA, la CEDEAO et l'OHADA. Cette adaptation est justifiée par la nécessité de donner aux acteurs les moyens de tirer profit du numérique avec une sécurisation juridique du cyberspace. Toutefois, elle doit être poursuivie afin de suivre l'évolution rapide du numérique.

Mots clefs : Adaptation, droit, numérique, Mali, UEMOA, Afrique de l'Ouest, OHADA**.**

RETURN ON ADAPTING THE LAW TO DIGITAL

Abstract

The adaptation of the Law to digital is an necissity resulting at the big progress of the digital. The digital gives many opportunities, but creates so much diffuculties relating to law. Quite appréciable adaptation of malian law to the digital is done by national lawyer and lawyers of some communauties regarding Mali, such as WAMU, ECOWAS and OHADA. This adaptation is justified by the necessity to give the aims to use cyberspace and juridical security to the differents actors relating this space. But it must be continued in order to follow the evolution of the digital.

Keywords : *Adaptation, law, digital, Mali, West Africa, OHADA.*

[*] Mode de citation : Djibril SOW
« Retour sur l'adaptation du droit au numérique », *Revue CAMES/SJP*, n°001/2016, p. 77-100

PLAN DE L'ARTICLE

INTRODUCTION[1]

« *Le droit est nécessairement influencé par les données, qui lui sont extérieures, mais qu'il est appelé à régir. Les faits transforment toujours le droit* » [2]. L'informatique, « *science de traitement automatique et rationnel de l'information en tant que support des connaissances et des communications* »[3], a pénétré depuis longtemps différents domaines de la société. L'informatique conjuguée avec les technologies de communication a donné naissance à l'Internet, « *la toile d'araignée mondiale* ». L'Internet a bouleversé le monde grâce aux formidables opportunités en matière d'information et de communication. Ces nouvelles opportunités sont importantes pour la société toute entière et dans les domaines les plus variés. C'est ainsi qu'apparurent diverses applications du numérique. Le numérique ou l'électronique, renvoie à une technique informatique fondée sur la numérisation qui consiste à transformer les données en chiffres, ce qui facilite leur reproduction, leur conservation et leur transmission.

L'essor des nouvelles technologies a soulevé beaucoup de questions, y compris en droit. Ces technologies étant devenues une réalité quotidienne, il est important que le droit s'adapte à cette nouvelle donne. Les juristes sont appelés à trouver des réponses aux questions posées par ce développement du numérique. Le droit de

[1] Le présent article revient sur un autre que nous avons auparavant publié en l'améliorant et l'actualisant (Voir D. SOW, "L'adaptation du droit au numérique", *RCDA*, N° 1, Janvier-Mars 2013, p. 5. C'est ce qui justifie l'utilisation du mot "retour" dans le titre.

[2] Ph. Le TOURNEAU, *Contrats informatiques et électroniques*, 2ème éd. refondue, Dalloz, coll. Dalloz Référence, 2002, n° 0.15.

[3] *Le petit Larousse illustré*, Larousse HER 2000, p. 546.

l'informatique se forme petit à petit. L'ouvrage du professeur Pierre CATALA, « *Le Droit à l'épreuve du numérique. Jus ex machina* », fut l'un des précurseurs en la matière[4]. L'adaptation du droit au numérique renvoie à la mise en adéquation du droit avec le numérique. Il s'agit de prendre en compte, au point de vue juridique, des enjeux du numérique et d'y apporter des réponses appropriées.

Aussi, toutes les branches du droit subissent, certes à des degrés différents, l'influence des nouvelles technologies. Plus concrètement, l'adaptation du droit au numérique est justifiée par la double nécessité de saisir les opportunités offertes par le numérique et de faire face aux contraintes juridiques engendrées par le numérique. Les technologies de l'information et de la communication jouent, avant tout, un rôle important pour le développement. Les TIC ne se limitent pas seulement à Internet, mais elles concernent « *aussi la téléphonie, la radio, la télévision, en bref, tous les moyens permettant d'échanger des informations et des connaissances à une plus grande échelle* »[5]. Dans le même rapport, l'OCDE, dans un encadré, met l'accent sur les opportunités qu'offre le numérique pour le développement. Ainsi l'utilisation expresse des TIC au service des objectifs de développement, peut permettre aux pays de parvenir à faire profiter le plus grand nombre des avantages des TIC, ce qui contribue à « *assurer une croissance économique à large assise et la réalisation d'objectifs de développement spécifiques* ». Il est en outre précisé qu'il importe d'utiliser les TIC afin d'améliorer la position concurrentielle des pays en développement dans l'économie mondiale, mais qu'il faudra en même temps une stimulation des entreprises et des marchés locaux pour l'atteinte des objectifs de développement[6].

L'Internet se caractérisant par la dématérialisation des actes, la maîtrise remarquable de la distance et le gain considérable de temps, a suscité parallèlement l'épanouissement des transactions électroniques. Aussi, le commerce électronique est en constante évolution. On peut envisager les applications les plus variées des TIC dans beaucoup de domaines du développement économique, social et culturel à l'échelle planétaire. En droit, on s'est très tôt intéressé aux avantages que l'on peut tirer du numérique. L'article 2 *in fine* de l'avant-projet de loi sur la société malienne de l'information, précise que les dispositions de ce texte tiennent compte des exigences légales relatives au développement durable, et concourent à la mise en place d'un cadre propice au développement de l'économie numérique[7].

Quant à l'Acte additionnel de la CEDEAO sur les transactions électroniques, il précise qu'avec le développement des réseaux de communications électroniques, le nombre

[4] P. CATALA, *Le Droit à l'épreuve du numérique. Jus ex Machina*, PUF, 1999 ; *adde* : VIVANT (M.), "L'informatique dans la théorie générale du contrat", *D.* 1994, chron., p. 117.

[5] OCDE, – *Rapport 2001*, Encadré VI-1. 2002, *in* : VI : L'économie du savoir et les opportunités du numérique », Revue de l'OCDE sur le développement, 2002/1 no 3, p. 181-197.

[6] Voir OCDE, – *Rapport 2001*, Encadré VI-1. 2002, précité. .

[7] L'exposé des motifs de la loi sénégalaise de 2008 sur les transactions électroniques rappelle qu' « *Avec le développement des réseaux informatiques, le nombre de transactions électroniques est en constante augmentation. A titre indicatif, les transactions électroniques portent sur la production, la promotion, la vente, la distribution de produits et les échanges par des réseaux de télécommunications ou informatiques (interrogation à distance, envoi d'une facture, etc.)* »

des transactions électroniques augmente constamment, notamment en matière de production, de promotion, de vente, de distribution de produits, de fourniture de services et d'échanges par des réseaux de communication, telles que l'interrogation à distance et l'envoi d'une facture. Le législateur communautaire CEDEAO constate en même temps que le potentiel de l'utilisation du numérique est énorme et mérite d'être exploité[8]. Le législateur de l'OHADA n'a pas également manqué de signaler les opportunités offertes par le numérique à travers l'informatisation du RCCM. L'exposé des motifs du Règlement n° 15 de l'UEMOA, précité, fait allusion également à la nécessité de pouvoir tirer profit des développements technologiques pour la modernisation des systèmes de paiement, le renforcement de leur efficacité et de leur sécurité[9]. Mais pour pouvoir tirer profit des opportunités offertes par le numérique, il s'est aussi avéré nécessaire que le droit puisse faire face aux contraintes qui sont également engendrées par le numérique.

Par ailleurs, les besoins de sécurisation également à l'origine de la nécessité de l'adaptation du droit au numérique peuvent être analysés sous deux aspects. D'abord, il y a le besoin d'une sécurisation générale des acteurs, ce qui est un des objectifs majeurs recherchés dans le cadre de cette adaptation du droit au numérique. Ensuite, l'on constate la nécessité d'une sécurisation spécifique des acteurs en la matière, ce qui n'échappe pas également aux législateurs. La nécessité de sécurité générale des acteurs a conduit à la prise de dispositions visant à sécuriser le paiement ainsi que la preuve et la signature électronique. Ensuite, il y a la sécurisation spécifique des acteurs. Elle passe par aussi plusieurs mesures. Il y a, en premier lieu, la sécurisation spécifique de certains acteurs par l'information qu'on doit leur fournir dans le cadre des transactions électroniques. Ainsi, pour faire face à cette nécessité de protection spécifique des acteurs, l'adaptation du droit au numérique accorde une attention particulière à la protection des consommateurs. Il y a, en second lieu, la protection des données à caractère personnel, envisagée notamment par les législateurs malien, sénégalais et communautaires.

L'étude de ce thème permet de comprendre davantage comment, directement ou indirectement, le droit malien s'adapte au numérique. Pour ce faire, l'attention porte d'abord sur le cas du Mali et ensuite sur la situation des principales communautés auxquelles fait partie le Mali[10]. En réalité, le droit positif malien est riche des différentes règles sécrétées çà et là. En effet, l'adaptation du droit au numérique est réalisée aussi bien au plan interne, qu'au plan communautaire. La méthodologie de l'étude a notamment consisté, d'abord, dans les recherches documentaires, l'analyse et la synthèse, la déduction et l'induction. Ensuite, le droit comparé est également souvent mis à profit, avec un certain regard sur les cas de la France et du Sénégal, entre autres. L'on constate, d'une part, dans l'ensemble, que l'adaptation du droit au numérique est assez variée dans son domaine et, d'autre part, qu'elle est assez justifiée dans ses objectifs. L'on peut retenir que l'adaptation de notre droit au numérique est assez appréciable et est opérée aussi bien au plan

[8] Voir les considérants de l'Acte additionnel de la CEDEAO portant sur les transactions électroniques du 16 février 2010.

[9] Voir l'Exposé des motifs du Règlement en question.

[10] L'Organisation Africaine de la Propriété Intellectuelle (OAPI) et la Conférence Interafricaine des Marchés d'Assurance (CIMA) ne retiendront pas particulièrement notre attention.
Il faut juste souligner que le numérique est envisagé dans les règlementations correspondantes, mais pas de façon particulière.

interne qu'au plan communautaire. C'est une adaptation assez prometteuse au plan interne (I), tandis qu'elle est fortement diversifiée au plan communautaire (II).

I. Une adaptation interne fortement prometteuse

Actuellement, le Mali a un vaste chantier de réformes législatives et réglementaires en vue d'assurer l'adaptation du droit au numérique. Cette adaptation intervient aussi bien à travers la création d'un cadre juridique général tenant en compte le numérique (A), mais aussi à travers l'adaptation de certains domaines spécifiques du droit au numérique (B).

A. L'adaptation du cadre juridique général au numérique

Dans le cadre de cette adaptation, il est important de souligner la loi sur la protection des données à caractère personnel (1) ainsi que les avant-projet de lois portant respectivement sur la l'orientation de la société malienne d'information et sur la cryptographie (2).

1) La loi sur la protection des données à caractère personnel

La loi portant sur la protection des données à caractère personnel date du 2013. A travers elle, le Mali assure à toute personne, physique ou morale, publique ou privée, la protection de ses données à caractère personnel[11], sans aucune discrimination. Elle garantit le respect des libertés et droits fondamentaux des personnes physiques dans tout traitement. Sont également pris en compte par cette loi, les prérogatives de l'Etat, les droits des collectivités territoriales, ainsi que les intérêts des entreprises et de la société civile. Aux termes de son article 2, al. 1, "*l'informatique doit être au service de chaque personne*", et "*doit respecter l'identité humaine, les droits de l'homme, la vie privée, les libertés publiques et individuelles*".

Le champ d'application de la loi en question est déterminé par ses articles 4, 5 et 6. Territorialement, elle s'applique à tout traitement de données à caractère personnel réalisé en tout ou en partie sur le territoire malien. Sont en outre visés les traitements provenant de l'Etat, des collectivités territoriales, des organismes personnalisés, des personnes physiques et des morales de droit privé. C'est le cas également de tout traitement du fait d'un responsable, établi ou non sur le territoire national, excepté l'hypothèse où les moyens ne sont utilisés qu'à des fins de transit au Mali. Est aussi visé le traitement de données relatives à la sécurité publique, la défense nationale, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, même liées à un intérêt économique ou financier important de l'Etat, sous réserves des dérogations prévues par les textes.

Les dispositions de l'article 6 de la loi sur la protection des données à caractère personnel, prévoit quelques exclusions de

[11] Le point 5 de l'article de 3 de la loi portant sur la protection des données à caractère personnel, définit les données à caractère personnel ou données personnelles, comme étant "*des informations existant sous diverses formes et permettant d'identifier directement ou indirectement une personne, par référence à un numéro d'immatriculation ou à un ou plusieurs éléments propres à son identité physique, physiologique, biométrique, génétique, psychique, culturelle, sociale ou économique*". Il peut s'agir d'identifiants universels permettant de raccorder entre eux plusieurs fichiers constituant des bases de données, ou de procéder à leur interconnexion. Différentes catégories de données sont également définies par l'article 3 de la loi précitée.

son champ d'application[12]. Sont prévus différents principes visant à protéger les données à caractère personnel[13].

Les moyens de protection des données à caractère personnel envisagés sont variés. Le législateur a posé des principes à respecter dans la collecte, le traitement et l'utilisation des données à caractère personnel. Il s'agit notamment de ceux de loyauté, de licéité, du respect des finalité, de la proportionnalité, ainsi que de la pertinence et de la conservation pendant une durée n'excédent pas celle nécessaire aux finalités pour lesquelles les données sont collectées et utilisées. Cependant, ces principes ne font pas obstacle à la satisfaction des besoins de gestion des archives, historiques, statistiques ou scientifiques en conformité avec la loi. De façon particulière sont envisagées l'obligation de sécurité du responsable du traitement, le principe d'interdiction de traiter des données sensibles, des règles strictes relatives aux traitements d'infractions ou de condamnation, sans oublier celles portant sur le transfert de données personnelles à l'étranger.

Des droits variés sont reconnus aux personnes en matière de traitement de données. Fort logiquement, leur sont reconnus le droit d'accès et de rectification directe et indirect; le droit de s'informer, tout comme le droit de s'opposer à figurer dans un traitement.

Une importante mesure de protection réside dans la création de l'Autorité de Protection des Données à Caractère personnel (APDP)[14]. L'APDP est une autorité administrative indépendante; elle comprend un organe délibérant collégial de quinze (15) membres désignés pour un mandat de sept (7) ans non renouvelable[15]. Elle a pour mission fondamentale d'assurer la protection des données à caractère personnel et de participer à la règlementation du Secteur[16]. Elle se réunit de plein droit, en session ordinaire, deux (2) fois par an. L'APDP a aussi des rapports avec les responsables de traitement et les usagers ordinaires, conformément aux dispositions des articles 53, 54 et 55 de la loi précitée. Elle assure notamment la coordination et le contrôle du traitement des données à caractère personnel sur toute l'étendue du territoire national.

Enfin, d'importantes sanctions sont prévues pour inobservations des règles de protection des données à caractère personnel. En effet, sans préjudice des sanctions pénales prévues par la loi concernée et les autres textes dont le Code

[12] Il s'agit, d'abord, des traitements de données mis en œuvre par une personne physique exclusivement dans le cadre de ses activement personnelles ou domestiques, pourvu que les données ne soient pas destinées à une communication systématique à des tiers ou à la diffusion. Ensuite, c'est le cas des copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à la seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises.

[13] Voir "La sécurisation spécifique des acteurs", vers la fin de la deuxième partie de notre article de 2013 sur "L'adaptation du droit au numérique", précité.

[14] Voir art. 20 de la loi sur la protection des données à caractère personnel, précitée.

[15] Voir art. 21 de la loi sur la protection des données à caractère personnel, précitée.

[16] Les différentes missions sont prévues par l'article 31 de la loi portant protection des données à caractère personnel. il s'agit notamment des missions de contrôle, d'administration, d'avis, de saisine du Procureur de la République, tout comme de sanction.

pénal[17], l'APDP inflige des sanctions administratives et pécuniaires.

La loi sur la protection des données à caractère personnel, comme on peut le remarquer, constitue une étape importante dans l'adaptation du droit malien au numérique. Il ne rester qu'à souhaiter sa bonne application afin notamment que l'APDP, à l'image de certains de ses homologues étrangers, puissent contribuer de façon significative à l'atteinte des objectifs fixés par le législateur.

2) Les avant-projets de lois sur la société de l'information et la cryptographie

Le cas de chacun de ces avant-projets de textes mérite d'être examiné à part.

- L'avant-projet de loi sur la société malienne de l'information

Cet avant-projet de loi est destiné à définir les fondements juridiques, institutionnels et éthiques de la société de l'information. Considérant que, conformément à son article 2, l'"*information, le savoir et plus généralement toutes les ressources immatérielles constituent les principales valeurs économiques et stratégiques de la société de l'information et de l'économie numérique*", il envisage la mise des lois des règlements en harmonie avec ses dispositions et leur conformité aux exigences de l'information, du respect des principes fondamentaux, de l'ordre public et des bonnes mœurs. Il tient compte des exigences légales se rapportant aux développement durable, tout en participant au développement de l'économie numérique, ce qui était fort attendu du législateur malien.

Le texte envisagé fixe dans son Chapitre II, les principes fondamentaux de la société malienne de l'information. Il prévoit ainsi le principe d'intégration à la société de l'information; le principe de liberté; le principe de sécurité principe; le principe de neutralité technologique; le principe du pluralisme, tout comme le principe de responsabilité sociétale. Compte tenu de l'importance de ces différents principes, nous y consacrerons ultérieurement un article à part entière.

Par ailleurs, sont déterminés les droits, rôles et responsabilités des différents acteurs de la société de l'information. Il est notamment envisagé que l'"*Etat, les établissements publics et les collectivités locales, les organisations de la société civile, les entreprises et les personnes privées mettent en œuvre, chacun dans le domaine de sa compétence et dans les limites de sa responsabilité, des politiques adaptées orientées vers un développement harmonieux de la société de l'information et de l'économie numérique conformément aux orientations de la présente loi*"[18].

Ils participent à la création, au développement, à la vulgarisation et à la promotion des technologies de l'information et de la communication dans tous les secteurs de la vie économique, sociale, scientifique et culturelle. Ces actions sont elles-mêmes considérées comme une mission prioritaire de service public.

Les différents acteurs de la société de l'information et de l'économie numérique sont tenus de prendre les mesures appropriées, notamment préventives utiles pour promouvoir la paix et pour empêcher les utilisations abusives, illégales et illicites des technologies de l'information

[17] Voir *infra*, sur l'apport de l'avant-projet de loi sur la cybercriminalité.

[18] Voir art. 19 de l'avant-projet de loi d'Orientation sur Société Malienne de l'Information et de l'Economie numérique.

et de la communication. En outre, dans ses dispositions transitoires et finales, l'avant-projet prévoit seize (16) secteurs prioritaires dans les lesquels les réformes nécessitées par la société d'information et l'économie numérique seront menées[19], et ce conformément aux engagements régionaux et internationaux du Mali. Les différents acteurs internes vont collabore étroitement avec l'Etat dans le chantier envisagé.

- L'avant-projet de loi sur la cryptographie

Cet avant-projet de loi a pour objet la définition du cadre de régulation des activités et prestation de cryptologie et la fixation des règles applicables aux moyens, modalités et systèmes de cryptologie. Ses dispositions ne sont pas applicables, aux termes de son article 2, aux : "*1) applications spécifiques utilisées en matière de défense et de sécurité nationale ; 2) moyens de cryptologie utilisés par les missions diplomatiques et consulaires visées par la Convention de Vienne sur les relations diplomatiques ainsi que ceux relatifs à la sécurité de l'Etat*".

Parmi les diverses définitions données par le texte, la cryptographie est présentée comme étant l'étude des moyens et produits de chiffrement permettant de rendre illisible des informations afin de garantir l'accès à un seul destinataire authentifié. Quant à la cryptologie elle est considérée comme une science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation des données transmises. Elle est composée de la cryptanalyse et de la cryptographie[20].

L'Autorité malienne de régulation des télécommunications/TIC et postes mise en place par l'ordonnance n°2011-024/P-RM du 28 septembre 2011 portant régulation du secteur des télécommunications, des technologies de l'information, de la communication et des postes est, en plus des missions qui lui sont assignées par les lois et règlements en vigueur, chargée de la régulation des activités et services de cryptologie.

L'avant-projet de texte sur la cryptographie prévoit, en outre, le régime juridique des moyens et prestations de cryptologie, les obligations et la responsabilité des prestataires de services de cryptologie; l'agrément des organismes exerçant des prestations de cryptologie, sans oublier les sanctions en matière de cryptologie. Il s'inspire largement des réglementations communautaires et internationales en matière de cryptographie et participera sans doute à la sécurisation dans le domaine du numérique.

B. L'adaptation de certains domaines spécifiques du droit au numérique

Les domaines spécifiques visés par l'adaptation du droit au numérique renvoient notamment au cas du droit pénal (1), ainsi qu'à celui des transactions électroniques (2).

1) L'adaptation du droit pénal au numérique

A ce niveau, on assiste à une faible adaptation opérée par le code pénal de 2001, à côté de l'apport important attendu

[19] Il s'agit des secteurs prioritaires suivants: "*1. l'éducation et la recherche ; 2. les grands registres de l'Etat ; 3. l'aménagement numérique du territoire ; 4. l'audiovisuel ; 5. la fiscalité ; 6. la propriété intellectuelle ; 7. l'économie ; 8. l'environnement; 9. la santé ; 10. les investissements et les affaires ; 11. l'emploi et la sécurité sociale ; 12. l'énergie ; 13. les transports ; 14. la justice ; 15. la sécurité ; 16. la défense*".

[20] Ces deux dernières notions sont également définies par l'article 3 de l'avant projet en question.

dans le cadre de l'avant-projet de loi sur la cybercriminalité.

- La faible adaptation réalisée par le Code pénal de 2001

Le législateur malien a profité du nouveau Code pénal pour prendre quelques mesures d'adaptation du droit pénal malien au numérique. Ainsi, la loi N° 01-079 du 20 Août 2001 portant Code pénal comporte quelques articles relatifs à la fraude informatique[21]. Les dispositions prévues par ce texte concernent plusieurs infractions. L'article 264 du Code pénal vise d'abord l'accès et le maintien frauduleux « *dans tout ou partie d'un système de traitement automatisé de données* »[22].

L'article 265 du Code pénal du Mali prévoit, quant à lui, une incrimination frappant quiconque aura, « *intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1 000 000 à 10 000 000 de francs ou de l'une de ces deux peines* ». Là, il s'agit de la sanction de l'entrave ou du fait de fausser le fonctionnement d'un système de traitement automatisé de données accomplis intentionnellement et au mépris des droits d'autrui.

L'article 266 punit l'introduction des données dans un système de traitement automatisé ou la suppression ou la modification des données qu'il contient ou de leurs modes de traitement ou de transmission accomplies intentionnellement, directement ou indirectement et au mépris des droits d'autrui. La sanction prévue par cet article consiste dans un emprisonnement de trois mois à trois ans et une amende de 200 000 à 50 000 000 de francs ou l'une de ces deux peines. L'article 267 du Code pénal, quant à lui, réprime la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui. Là, il s'agit du faux portant les documents informatisés étant de nature à causer préjudice à autrui. Cette infraction est intentionnelle et elle est punie d'un emprisonnement d'un an à cinq ans et d'une amende de 2000 000 à 200 000 000 de francs.

L'usage des documents informatisés falsifiés est sanctionné par l'article 268 du Code pénal. La peine prévue par le législateur malien consiste dans un emprisonnement d'un an à cinq ans et une amende de 2 000 000 à 200 000 000 de francs ou dans l'une de ces deux peines. Le législateur malien ayant prévu ces diverses fraudes informatiques, rend également punissable la tentative de ces différentes infractions. Les sanctions prévues dans ce cas sont les mêmes que celles frappant lesdites infractions[23]. En outre, la participation à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 264 à 268 est punie des peines

[21] Il s'agit des articles 264 à 271 du nouveau Code pénal du Mali.

[22] L'article 264, alinéa 1 du Code pénal a prévu un emprisonnement de deux mois à un an et d'une amende de 200 000 à 5000 000 de francs ou de l'une ces deux peines, à l'encontre de celui qui commet l'infraction d'accès ou du maintien dans un système de traitement automatisé de données. L'alinéa 2 du même article, prévoit l'aggravation de la sanction de cette infraction lorsque de l'accès ou du maintien dans un système de traitement automatisé aura résulté « soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système ». Dans ce cas, la sanction est aggravée et consiste dans l'emprisonnement de deux mois à deux ans et d'une amende de 1 000 000 à 10 000 000 de francs.

[23] Article 267 du Code pénal du Mali.

prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. Les différentes infractions prévues en matière de fraude informatique précédemment indiquées peuvent en outre être sanctionnées par la confiscation des matériels appartenant au condamné et ayant servi à commettre les infractions en cause.

L'œuvre du législateur malien en 2001, en vue d'adapter le droit pénal au numérique a consisté ainsi à réprimer certaines infractions liées à l'essor du numérique. L'irruption du numérique engendre en effet de nombreux problèmes en droit pénal. Comme le souligne le Professeur DIOUF, la plupart de ces problèmes sont connus et trouvent une solution dans les règles existantes. Mais on assiste également à l'apparition de nouveaux problèmes aussi bien en droit pénal de fond, qu'en procédure pénale[24]. La création des différentes incriminations examinées en est une illustration. L'adaptation du droit pénal malien au numérique à travers les dispositions des articles 264 à 271 du nouveau Code pénal, est une œuvre salutaire. Il était urgent de réprimer certains comportements dangereux dans le cadre de l'utilisation de l'informatique. Cependant, cet effort du législateur malien reste tout de même limité. Malgré cette intervention, il a manqué de vision globale sur la cybercriminalité. Or une telle approche est indispensable pour une adaptation plus élargie du droit pénal au numérique. En effet, « *La mondialisation et le développement du virtuel ouvre aux criminels des perspectives nouvelles et favorables pour se livrer à leur activité illicite et commettre des infractions* »[25]. La cybercriminalité est elle-même à la base de « l'émergence d'un nouveau risque » à travers la sophistication des outils et des moyens à la disposition de cette catégorie de criminels[26]. L'avant projet de loi sur la cybercriminalité vise notamment à répondre à ces différentes préoccupations.

- L'apport attendu de l'avant-projet de loi sur la cybercriminalité

L'apparition marquée de ce nouveau phénomène criminel appelé cybercriminalité caractérisé par une forte transnationalité, une immatérialité, une volatilité et l'anonymat de ses acteurs impose nécessairement la prise de mesures visant à adapter le droit pénal à cette nouvelle donne[27]. On peut citer l'exemple du Sénégal qui a adopté une loi sur la cybercriminalité en 2008[28]. A l'image du législateur sénégalais, il est indispensable, dans le cadre de l'adaptation du droit pénal malien au numérique, de prendre en compte aussi bien le droit pénal substantiel, que le droit pénal processuel. Il est à noter que l'Union Africaine (UA) a un projet de convention sur la cybersécurité, comportant un passage sur la lutte contre la cybercriminalité[29].

---

[24] Ndiaw DIOUF, « Infractions en relations avec les nouvelles technologies de l'information et Procédure pénale : l'inadaptation des réponses nationales face à un phénomène de dimension internationale », *AFRILEX*, N° 4, p. 251, in : http://www.afrilex.u-bordeaux-4.fr.

[25] C'est une déclaration faite par le président d'Interpol M. Khoo Boon Hui, dans son discours d'ouverture de la 41e Conférence régionale européenne de cette organisation, qui s'est déroulé du 7 au 12 Mai 2012 à Tel Aviv, cité par E. BAILLY et E. DAOUD, *in* « Cybercriminalité et réseaux sociaux : la réponse pénale », *AJ Pénal* 2012, p. 252.

[26] Voir J. CAZENEUVE, « Cybercriminalité : l'émergence d'un nouveau risque », *AJ Pénal* 2012, p. 268.

[27] Voir l'exposé des motifs de la Loi sénégalaise du 25 janvier 2008 sur la cybercriminalité, *in* www.jo.gouv.sn/spip.php?page=imprimer&id_article=6662.

[28] *Ibidem*.

[29] L'Union Africaine a un projet de convention sur la cybersécurité, comportant une partie consacrée à la lutte contre la cybercriminalité (*Draft african*

L'avant-projet sur la cybercriminalité de janvier 2013 améliorera fortement l'adaptation du droit pénal malien au numérique. il vise précisément à modifier la loi n°01-079 du 20 août 2001 portant Code Pénal et de la loi n°01-080/du 20 août 2001 portant Code de procédure pénale et "*a pour objet, d'adapter le droit pénal de fond et la procédure pénale au phénomène de la cybercriminalité en République du Mali*". Il définit précisément les principales notions techniques utilisées, ce qui est à saluer.

L'avant-projet de loi sur la cybercriminalité en République du Mali envisage, dans son Titre II, les "crimes et délits liés aux technologies de l'information et de la communication". Son article 3 ajoute au livre III de la loi n° 01-079 du 20 août 2001 portant Code pénal un Titre IV intitulé « Des crimes et délits liés aux technologies de l'information et de la communication », comprenant les articles 324-1 à 324-82. Y sont d'abord prévues, les atteintes à la confidentialité des systèmes d'information. Il s'agit de l'accès frauduleux à un système informatique, ainsi que du maintien frauduleux dans un tel système[30].

Ensuite, sont ciblées plusieurs autres infractions. On peut citer, en premier lieu, les atteintes à l'intégrité et à la disponibilité des systèmes d'information, à travers l'incrimination de l'entrave au fonctionnement d'un système d'information et de l'introduction frauduleuse de données dans un système d'information[31]. Il y a également le cas des atteintes à l'intégrité des données d'un système d'information, tout comme la fraude informatique. Plusieurs articles sont, par ailleurs, consacrés aux atteintes aux données à caractère personnel; à la disposition d'un équipement pour commettre des infractions; à l'association formée ou l'entente en vue de commettre des infractions informatiques, sans oublier la pornographie infantile. D'autres dispositions visent les actes racistes et xénophobes (faits) par le biais d'un système d'information; les infractions liées aux activités des prestataires de services de communication au public par voie électronique; celles en matière de prospection directe; en matière de publicité par voie électronique, tout comme en matière de cryptologie.

De façon particulière, le chapitre XIV du titre II, porte sur l' "*adaptation des infractions classiques aux technologies de l'information et de la communication*". Ce chapitre de sept sections se rapporte aux infractions portant sur les biens commises par le biais des technologies de l'information et de la communication; aux infractions de presse commises par le même biais[32]; celles qui sont commises par tout moyen de diffusion publique[33];

Convention on Cybersecurity, *in* : http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/draft%20convention%20cybersecurity%20french%2019%20sept%202011.pdf, consulté en décembre 2012).

[30] Articles 324-1 et 324-2 de l'avant-projet sur la cybercriminalité, précité.

[31] Articles 324-3 et 324-4, de l'avant-projet sur la cybercriminalité, précité.

[32] Là il faut préciser que sont visées par l'article 324-59, "*Les infractions de presse, prévues par la loi n° 00-46/AN- RM du 7 juillet 2000 portant régime de la presse et délit de presse, commises par le biais des technologies de l'information et de la communication, à l'exception de celles commises par la presse sur Internet, sont soumises au régime de droit commun de la responsabilité pénale*".

[33] L'article 324-60 dispose, en effet, que "*Sont considérés comme moyens de diffusion publique : la radiodiffusion, 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 proférés dans les lieux ou réunions publics, tout procédé technique destiné à atteindre*

l'usurpation d'identité numérique; les atteintes au droit d'auteur et aux droits voisins; le refus d'assistance, ainsi que les atteintes à la défense nationale en rapport avec le numérique[34].

Un autre élément à mettre particulièrement en exergue concerne la reconnaissance très claire de la responsabilité pénale des personnes morales, envisagée par le Chapitre XV du même titre, de l'avant-projet[35]. Il est, en outre, précisé que la responsabilité des personnes morales telle que définie aux articles 324-71 et 324-72 n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits[36].

Par ailleurs, il est question de l'adaptation de certaines sanctions aux technologies de l'information et de la communication. Ainsi, l'article 324-75 dispose qu'en cas de condamnation pour une infraction commise par le biais des technologies de l'information et de la communication, la juridiction a la possibilité de prononcer, à titre de peines complémentaires, l'interdiction d'émettre des messages de communication numérique, l'interdiction à titre provisoire ou définitif de l'accès au site ayant servi à commettre l'infraction, ou l'injonction d'en couper l'accès par tous moyens techniques disponibles ou même en interdire l'hébergement. Le juge pourra aussi faire injonction à toute personne responsable légalement du site ayant servi à commettre l'infraction ou à toute personne qualifiée de mettre en œuvre les moyens techniques de nature à garantir l'interdiction d'accès, d'hébergement ou la coupure de l'accès au site incriminé.

Le Titre III de l'avant-projet de loi sur la cybercriminalité précité, envisage la procédure en matière de crime et délit liés aux technologies de l'information et de la communication. Il s'agit là de la réparation d'une grosse lacune de la première adaptation réalisée par le Code pénal en 2001, qui oubliait les aspects procéduraux en rapport avec le numérique. Dans les dispositions générales, il est précisé que les dispositions de ce titre "*sont appliquées et mises en œuvre dans le respect des droits des citoyens garantis par la Constitution et protégés par les conventions internationales auxquelles la République du Mali est partie, particulièrement la Charte africaine des droits de l'Homme, ainsi que notamment les droits tels que le droit à la liberté d'expression, le droit au respect de la vie privée et le droit à une instruction équitable*".

Dans le droit pénal processuel en matière de cybercriminalité, il est prévu,

---

le public et généralement tout moyen de communication numérique par voie électronique".

[34] Ce domaine n'échappe pas non plus à la vulnérabilité liée au numérique.

[35] Ainsi l'article 324-71 précise que "*Les personnes morales autres que l'Etat, les collectivités locales et les établissements publics sont pénalement responsables des infractions prévues par la présente loi, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein fondé:*

1) *sur un pouvoir de représentation de la personne morale ;*
2) *sur une autorité pour prendre des décisions au nom de la personne morale ;*
3) *sur une autorité pour exercer un contrôle au sein de la personne morale*".

L'Article 324-72 envisage les conditions dans lesquelles les personnes morales visées à l'article 324-71 peuvent être tenues pour responsables. Il peut s'agir de l'absence de surveillance ou de contrôle de la part de leurs organes ou représentants qui a rendu possible la commission des infractions établies par l'avant-projet de loi pour le compte de ladite personne morale par une personne physique agissant sous leur autorité.

[36] Article 324-73 de l'avant-projet de loi sur cybercriminalité, précité.

après l'article 630 de la loi n° 01-080 du 20 août 2001 portant Code de procédure pénale, d'insérer un titre XI *bis* intitulé « *Procédure en matière crime et délit lies aux technologies de l'information et de la communication* » comprenant les articles 630-1 à 630-27. Au niveau de ces différents articles, est d'abord envisagée la reconnaissance de la preuve électronique en matière pénale[37], un peu à l'image de ce qui est prévu en matière de transactions électroniques. Sont aussi prévus d'autres actes procéduraux tels que la perquisition et la saisie informatique(s); la conservation immédiate des données informatisées stockées; la collecte en temps réel des données relatives au trafic; l'utilisation de logiciels à distance. L'injonction de produire et l'interception de données informatisées relatives au contenu, sont aussi concernées[38].

Enfin, des mesures particulières sont prévues concernant la protection des données à caractère personnel[39], ainsi que des dispositions en matière de coopération et d'entraide judiciaire internationales, toute chose indispensable en matière de cybercriminalité[40]. Quant à l'entraide judiciaire, elle est réglementée par les articles 630-25 et suivants envisagés par le même avant-projet de loi[41]. L'un des mérites de l'avant-projet étudié est de permettre au Mali d'essayer d'être à jour dans le domaine de l'adaptation de la procédure pénale au numérique. En effet, en la matière, restent d'une brulante actualité les questions relatives notamment à la géolocalisation[42], à l'accomplissent de certains actes de procédure via le numérique, et de façon générale en matière d'investigations liées au numérique.

2. L'adaptation du droit des transactions au numérique

A ce sujet, est d'abord concerné le cadre technique et institutionnel des transactions électroniques, ensuite le cas particulier des contrats électroniques. Ces différents aspects sont envisagés par l'avant-projet de loi sur les transactions électroniques au Mali, de janvier 2013. Cet avant-projet s'applique notamment aux services de la société de l'information tels que définis à

[37] Voir art. 630-1 prévu par l'avant-projet.

[38] Sur ce point, l'article 630-16 dispose que "*Lorsque les nécessités de l'enquête l'exigent, le procureur de la République ou le juge d'instruction peut utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques, transmises au moyen d'un système d'information ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer lesdites données, en application de moyens techniques existants, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer ces données*".

[39] Voir notamment l'article 630-18, prévu par l'avant-projet

[40] A cet effet, l'article 630-21 prévoit que le Mali peut établir des conventions de coopération en matière de cyber sécurité et de lutte contre la cybercriminalité avec d'autres pays ayant les mêmes objectifs, en prenant en compte le standard minimum adopté dans les législations en vigueur au plan international.

[41] Sur l'entraide judiciaire internationale, voir les articles 630-25 à 630-27 de l'avant-projet sur la cybercriminalité, précité.

[42] Sur le cas de France Voir, par exemple, M.-Ch. DAUBIGNEY, "La marche vers la dématérialisation de la procédure pénale", *AJ Pénal* 2007 p. 460; J. BOSSAN, "La dématérialisation de la procédure pénale", *D.* 2012, p. 627; M. QUEMENER, "La procédure pénale à l'épreuve de la géolocalisation", *AJ Pénal*, 2013, p. 568; S. SONTAG-KOENIG, "La signature électronique en procédure pénale: une évolution amorcée", *AJ Pénal* 2014, p. 123; J. PRADEL, "De la géolocalisation en procédure pénale. A la recherche d'un statut", *JCP G*, 2014, doctr. 100; J. PRADEL, "La géolocalisation: un exemple de vide législatif rapidement comblé dans l'urgence. A propos de la loi n° 2014-372 du 28 mars 2014", *JCP G*, 2014, act. 415.

son article 1.27; aux activités dépourvues de caractère économique, accomplies à distance et par voie électronique, portant sur des biens, des services, des droits ou des obligations ; aux activités accomplies à distance et par voie électronique, portant sur des biens, des services, des droits ou des obligations, lorsqu'elles mettent en relation des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle, qu'elle soit commerciale, industrielle, artisanale ou libérale ; à la dématérialisation des procédures et formalités administratives ; à la mise en ligne des informations publiques par l'Etat, les collectivités territoriales et toute personne de droit public ou de droit privé chargée de la gestion d'un service public.

Par contre, ne sont concernés les domaines relatifs aux jeux d'argent qui impliquent des mises ayant une valeur monétaire dans des jeux de hasard, y compris les loteries, et les transactions portant sur des jeux de hasard, mêmes légalement autorisés ; les activités de représentation et d'assistance devant les cours et tribunaux ; les activités exercées par les notaires ou les professions équivalentes, dans la mesure où elles comportent une participation directe et spécifique à l'exercice de l'autorité publique[43].

L'avant-projet de loi sur les transactions électroniques réglemente, de façon assez détaillée, la communication au public par voie électronique; le commerce par voie électronique; la sécurisation des transactions électroniques; l'administration électronique; le règlement des litiges, les sanctions civiles et pénales, ainsi l'agence nationale de certification électronique. Plusieurs aspects dudit avant-projet sont abordés par notre article sur l'adaptation du droit des contrats au numérique[44].

Les transactions électroniques figurent aussi parmi les éléments de l'adaptation du droit au numérique au plan communautaire.

II. Une adaptation communautaire fortement diversifiée

Au plan communautaire, un apport remarquable est fait par les législateurs. Là l'intervention a eu lieu aussi bien au plan communautaire ouest africain (A), qu'au niveau de l'OHADA (B).

A. L'adaptation opérée par le législateur communautaire ouest africain

L'adaptation opérée par le législateur ouest africain s'entend de l'apport de l'UEMOA (1), ainsi que de l'apport de la CEDEAO (2).

1. L'adaptation opérée par l'UEMOA

L'intervention de l'UEMOA a été déterminante dans l'adaptation du droit des Etats membres au numérique. Cette intervention est assez intéressante dans le domaine de la preuve et du paiement électronique. Le paiement électronique[45] est un paiement effectué avec un procédé électronique. La reconnaissance du paiement électronique s'inscrit dans la même logique d'adaptation du droit aux exigences du numérique. Dans l'espace UEMOA, c'est le règlement n° 15 du 19

[43] Les dispositions de l'avant-projet sont sans préjudice des règles applicables en matière de protection des données à caractère personnel; ainsi que des régimes dérogatoires ou spéciaux applicables aux établissements de crédit et aux services financiers, notamment en matière de preuve électronique.

[44] Voir D. SOW, "Réflexion sur l'adaptation du droit des contrats au numérique", *Revue C.A.M.E.S./ S.J.P.*, N° 001/2015, p. 63.

[45] Voir M. VASSEUR, « Le paiement électronique Aspects juridiques », *JCP*, 1985, I, 3206.

septembre 2002, portant instruments de paiement et de crédit, qui régit le paiement électronique. Au paiement électronique s'appliquent, avant tout, les règles de droit commun. C'est plutôt à travers les moyens de paiement et certains mécanismes du paiement que se remarquent certaines spécificités du paiement électronique. Il s'agit notamment des moyens de paiement électronique, du virement électronique ainsi que de la sécurisation du paiement en question.

Le règlement n° 15 du 19 septembre 2002, précité distingue les cartes de paiement et les cartes de retrait, tout en admettant l'existence de tout autre support de paiement électronique. La carte de paiement est définie par l'article premier du règlement comme une carte émise par les organismes visés à son article 42 et permettant à son titulaire de retirer ou de virer des fonds. Les organismes émetteurs visés par l'article 42 sont constitués par les établissements de crédit, les services de chèques postaux, le Trésor public et tout autre organisme dûment habilité par la loi (voir art. 131 du règlement précité). Le porte-monnaie électronique est une carte de paiement prépayée, c'est-à-dire sur laquelle une certaine somme d'argent a été chargée et permettant d'effectuer des paiements de montants limités. La carte de retrait est définie par l'article 1er du règlement comme celle permettant à son titulaire de retirer exclusivement des fonds. Elle est émise par les mêmes organismes que pour les cartes de paiement. La carte de garantie est expressément prévue en matière de chèque, conformément à l'article 79 du règlement n° 15.

Le paiement électronique peut aussi se faire par virement électronique. Le virement électronique est défini comme une série d'opérations commençant par l'ordre de paiement du donneur d'ordre effectué par des moyens ou procédés électroniques de paiement dans le but de mettre des fonds à la disposition d'un bénéficiaire. Il peut notamment être effectué au moyen d'une carte bancaire, d'un porte-monnaie électronique ou par le procédé du télépaiement ou de tout autre mode électronique de paiement[46]. Les parties au virement électronique sont constituées par l'émetteur, le titulaire de la carte ou de tout autre instrument de paiement électronique, et le bénéficiaire. Leurs rapports sont régis par une convention, conformément à l'article 136 du règlement précité. Cette convention précise les modalités d'utilisation, le coût, la durée, les conditions de remboursement et les cas de retrait anticipé de la carte. Par ailleurs, le règlement précise les obligations de l'expéditeur et celles du destinataire de l'ordre de virement électronique[47].

Le règlement n° 15, précité, prévoit plusieurs mesures de sécurisation du paiement par carte. Cette sécurisation passe d'abord par certaines règles communes aux systèmes de paiement. Le règlement n° 15 a prévu des mesures préventives spécifiques de sécurisation du paiement électronique. Les organismes émetteurs sont tenus d'une obligation d'information et de vérification en vue de protéger les tiers et les divers acteurs concernés. Les organismes visés à l'article 42 du Règlement n° 15, précité, sont tenus d'informer toute personne qui en fait la demande des conditions d'utilisation des cartes bancaires, instruments et procédés électroniques de paiement qui lui sont délivrés, ainsi que des sanctions encourues en cas d'utilisation abusive. Ils doivent, préalablement à la délivrance d'une carte de paiement, s'assurer que le demandeur n'a pas fait l'objet d'une décision de retrait de carte, d'une mesure d'interdiction bancaire ou judiciaire d'émettre des

[46] Voir art. 1, *in fine*, du Règlement n°15, précité.

[47] Voir articles 133 à 136 du Règlement n° 15, précité.

chèques ou d'une condamnation pour les infractions visées aux articles 143 et suivants du règlement, n° 15, précité[48].

En outre, la BCEAO centralise les incidents relatifs aux paiements par carte, conformément aux dispositions de l'article 138 du Règlement n° 15, précité. Enfin, l'irrévocabilité de l'ordre de paiement est une mesure importante de sécurisation des paiements par carte (art. 142 du règlement). Aux termes de cet article, l'ordre ou l'engagement de paiement fait au moyen d'une carte ou d'un autre instrument et procédé électronique de paiement est irrévocable. Cette irrévocabilité signifie que l'ordre ou l'engagement concerné ne peut être remis en cause, en principe. En France le nouvel article 133-1 du Code monétaire et financier, issu de l'Ordonnance n° 2009-886 du 15 juillet 2009, envisage aussi l'irrévocabilité de l'ordre de paiement, « *quel qu'en soit l'émetteur, le payeur ou le bénéficiaire, une fois reçu par le prestataire du payeur* »[49]. L'on constate ici que le moment de l'irrévocabilité en question c'est à partir de la réception par le prestataire du payeur. Le règlement n° 15 du 19 septembre 2002, n'apporte pas cette précision utile. Le principe de l'irrévocabilité de l'ordre de paiement connaît des aménagements, voire des exceptions. En effet, l'opposition à l'ordre de paiement est permise dans les conditions prévues à l'article 142, alinéa 1 du règlement précité. Il en est ainsi notamment en cas de perte, de vol ou d'utilisation frauduleuse de la carte ou du porte-monnaie, ou encore en cas d'ouverture d'une procédure collective contre le bénéficiaire[50]. L'émetteur qui reçoit une opposition au paiement par carte doit en informer la BCEAO.

Au-delà des mesures préventives de sécurisation, le règlement a aussi prévu plusieurs infractions réprimant les fraudes, les abus et les contrefaçons des cartes de paiement et des instruments assimilés. Ces infractions sont désormais prévues par les articles 15 et suivants de la Loi uniforme relative à la répression des infractions en matière de chèque, de carte bancaire et d'autres instruments et procédés électroniques de paiement[51]. Les auteurs de ces infractions encourent diverses peines également prévues par la loi uniforme en question[52].

La preuve joue un rôle très important dans la réalisation des droits. L'admission des contrats électroniques suite à l'essor du numérique conduit forcément à la reconnaissance de la preuve électronique. Mais cela ne va pas sans trouver des garanties de l'efficacité de ce type de preuve. Suite à la loi française du 13 mars 2000, portant adaptation du droit de la preuve aux nouvelles technologies de l'information, et relative à la signature électronique, la preuve électronique a été admise dans l'espace UEMOA par le Règlement n° 15/2002/CM/UEMOA du 19 septembre 2002 relatif aux systèmes de paiement dans les États membres de l'Union Économique et Monétaire Ouest Africaine (UEMOA). Cette dernière « *résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une*

[48] Voir aussi, art. 137 et art. 139 du Règlement n° 15, précité

[49] Voir R. BONHOMME, « Le déclenchement de l'opération de paiement : le consentement et l'ordre », *JCP E*, 2010, 1032, n° 30.

[50] J.-L. GUILLOT – P.-Y. BERARD, « Com. 20 janvier 2009 » Chron. *Revue Banque*, 07/05/2009, n° 712.

[51] Voir art. 15 à 24 de la Loi uniforme relative à la répression des infractions en matière de chèque, de carte bancaire et d'autres instruments et procédés électroniques de paiement.

[52] *Ibid*.

signification intelligible, quels que soient le support et les modalités de transmission ». Cette large définition permet ainsi d'englober, pour reprendre l'expression du professeur HUET, en même temps l'écrit électronique et l'écrit dressé sur un papier, sans tenir compte de leur support[53].

S'agissant de la sécurité de la preuve électronique, elle a rendu nécessaire la reconnaissance de la signature électronique elle-même sécurisée. La signature électronique est définie par le règlement n° 15/2002/CM/UEMOA précité, comme consistant en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle se rattache. Le dispositif sécurisé de signature repose sur certains critères de fiabilité, conformément aux articles 21, 22, 23, 24 et 25, du règlement n° 15, précité, dont l'exigence d'une certification qualifiée, implique que le dispositif sécurisé de création de la signature électronique soit certifié conforme aux conditions requises à cet effet. Cette certification doit se faire par des organismes agréés par la BCEAO. En outre, la délivrance du certificat de conformité doit être publiée dans un journal habilité à recevoir des annonces légales ou selon les modalités fixées par instruction de la Banque Centrale.

Par ailleurs, pour qu'un certificat électronique puisse être considéré comme qualifié, il doit être délivré par un prestataire de services de certification qualifié et comporter les mentions prévues à l'article 26 dudit règlement. Ces différentes mentions sont destinées à identifier le certificat et à le sécuriser. En effet, le respect de ces exigences permet d'obtenir un certificat fiable qui peut, ainsi, être reconnu comme étant qualifié. Une des garanties de cette fiabilité tient à la qualité du prestataire de services de certification électronique. C'est pourquoi ce dernier doit satisfaire à diverses exigences. Celles-ci tendent à assurer la fiabilité des services en question en mettant à la charge du prestataire plusieurs obligations. À côté des obligations tenant à la gestion administrative du service fourni, il assume des obligations à l'égard du demandeur de certification concernant la révocabilité du certificat. Enfin, une autre obligation importante pèse sur le prestataire quant aux garanties financières suffisantes qu'il doit présenter pour l'exercice de ses activités. Le cas échéant, il est tenu de l'indemnisation des utilisateurs de ses services ayant subi des dommages du fait de l'inexécution ou de la mauvaise exécution de ses obligations.

Les autres garde-fous de la fiabilité des services de certification électronique se rapportent à la procédure d'accréditation des organismes de qualification et à celle d'évaluation et de qualification des prestataires de services en question. Le contrôle du respect des exigences en matière de certification électronique est assuré, pour ce qui concerne les systèmes de paiement dans l'espace UEMOA, par les services de la BCEAO, qui fixent également les sanctions encourues à cet effet. Par ailleurs, la cryptographie joue un rôle important dans la sécurisation de la signature électronique. Une fois que la signature électronique est sécurisée et qu'elle est liée à un certificat électronique

[53] Pour jouer la fonction de preuve littérale, l'écrit électronique doit remplir certains critères. Il doit être intelligible et son auteur identifiable. En outre, il doit être établi et conservé dans des conditions de nature à garantir son intégrité. L'on constate, en outre, que certains des caractères de l'écrit électronique renvoient à son efficacité qui doit aussi être garantie, ce qui est indispensable pour atteindre les objectifs de fiabilité et de sécurité, toute chose qui a attiré aussi l'attention dans le cadre de l'adaptation au numérique. La signature électronique est définie par le règlement n° 15/2002/CM/UEMOA précité, comme consistant en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle se rattache.

qualifié, elle acquiert la même force probante que la signature manuscrite.

2. L'adaptation opérée par la CEDEAO

L'intervention de la CEDEAO peut être particulièrement signalée dans le domaine des transactions électroniques, ainsi qu'en matière de protection des données à caractère personnel. Dans le domaine des transactions électroniques, l'Acte additionnel du 16 février 2010 vise plusieurs aspects liés aux transactions électroniques. Son champ d'application est déterminé par ses articles 2 et 3. Au-delà des aspects sécuritaires, l'on cible l'adaptation de la formation du contrat au numérique. Cela passe d'abord par la reconnaissance du consentement[54] électronique. Le consentement électronique est celui donné par voie électronique. La question est donc de savoir comment le numérique joue sur l'offre[55] et l'acceptation[56].

La protection des consommateurs est une des priorités de la règlementation en matière de publicité. Cela est particulièrement vrai lorsqu'il s'agit de la publicité électronique. Dans le cadre de l'adaptation du droit au numérique, cet aspect a retenu l'attention du législateur. A l'image du législateur sénégalais, le législateur communautaire de la CDEAO a prévu plusieurs règles protectrices des consommateurs en matière de publicité électronique. D'abord, il est imposé une obligation d'identification de toute publicité, quelle que soit sa forme, accessible par un service de communication au public en ligne. Il faut qu'elle puisse être clairement identifiée comme telle. Cette publicité doit également permettre une identification claire de la personne physique ou morale pour le compte de laquelle elle est effectuée[57].

Est ensuite exigée l'identification des prix. Les publicités, et notamment les offres promotionnelles, telles que les rabais, les primes ou les cadeaux, ainsi que les concours ou les jeux promotionnels, adressés par courrier électronique, doivent être identifiables de manière claire et non équivoque sur l'objet du courrier dès leur réception par leur destinataire, ou en cas d'impossibilité technique, dans le corps du message. L'Acte additionnel de la CEDEAO sur les transactions électroniques comporte des dispositions similaires en matière de publicité[58]. De façon générale, le consommateur est protégé par plusieurs autres mesures dans le cadre des transactions électroniques, qu'il s'agisse des choix à faire, ou de la validité des procédés utilisés. Il bénéficie d'une relative bienveillance du législateur dans ses rapports avec les professionnels.

Le législateur communautaire de la CEDEAO a aussi adopté un autre Acte additionnel, celui portant protection des données à caractère personnel, à la même date que l'acte additionnel sur les transactions électroniques déjà invoqué. Il donne la définition du cadre juridique général de la protection des données à

[54] Le consentement est l'expression de la volonté des parties en vue de former le contrat.

[55] L'offre ou pollicitation est définie comme une manifestation de volonté suffisamment ferme et précise adressée à une personne déterminée ou au public et dont l'acceptation par le destinataire suffit à conclure le contrat (voir art. article 14-1 de la convention de Vienne sur la vente internationale de marchandises du 11 Avril 1980).

[56] Voir D. SOW, "Réflexion sur l'adaptation du droit des contrats au numérique", article précité.

[57] Art. 13 de la Loi sénégalaise du 25 janvier 2008 sur les transactions électroniques ; art. 8 de l'Acte additionnel de la CEDEAO, du 16 février 2010 portant transactions électroniques dans l'espace CEDEAO.

[58] Voir art. 8 et suivants dudit Acte additionnel.

caractère ; indique les formalités nécessaires au traitement des données à caractère personnel ; fixe le cadre institutionnel garantissant le respect des règles prévues ; dégage les principes directeurs ainsi que des principes spécifiques, sans oublier les droits des personnes fichées, tout comme les obligations du responsable du traitement. Le principe de légitimité impose la licéité et la loyauté de l'opération tout comme consentement de la personne concernée. Le principe de finalité nécessite la prise en compte les objectifs visés et de la durée. Il y a aussi le principe de proportionnalité, le principe de sécurité et de confidentialité, ainsi que le principe du respect des droits de la personne dont les données sont concernées[59].

B. L'adaptation réalisée par le législateur de l'OHADA

L'Acte uniforme de l'OHADA portant droit commercial général (AUDCG) a été révisé en 2010. La nouvelle version de cet acte uniforme est fortement marquée par l'impact des nouvelles technologies, notamment l'électronique. Cela est d'une importance capitale, afin de tenir compte de ces nouvelles technologies. Le législateur communautaire de l'OHADA, en vue de l'informatisation du Registre du Commerce et du Crédit Mobilier (RCCM), a admis l'écrit et la signature électronique (1), et prévu un dispositif de mise en œuvre de cette adaptation des règles du RCCM au numérique, sans oublier l'apport de l'AUDSC/GIE du 30 janvier 2014 (2).

1. L'admission de l'écrit et de la signature électroniques

Le législateur communautaire de l'OHADA précisé, suivant la même technique que celle employée en France, dans l'UEMOA et dans beaucoup d'autres pays, que « *Les documents sous forme électronique peuvent se substituer aux documents sur support papier et sont reconnus comme équivalents lorsqu'ils sont établis et maintenus selon un procédé technique fiable, qui garantit, à tout moment, l'origine du document sous forme électronique et son intégrité au cours des traitements et des transmissions électroniques.*» Cette reconnaissance de l'écrit électronique et de son équivalence à l'écrit sur support papier, a été nécessaire en vue de l'informatisation du RCCM.

Il faut toutefois rappeler que, déjà en 2003, l'Acte Uniforme de l'OHADA sur les contrats de transport de marchandise par route (AUCTMR) a eu l'occasion de consacrer la lettre de voiture électronique. Pour l'application de cet Acte uniforme, il a été précisé que l'écrit est entendu comme "*une suite de lettres, de caractères, de chiffres, ou de tous autres signes ou symboles dotés d'une signification intelligible et mis sur papier ou sur un support faisant appel aux technologies de l'information*"[60]. La consécration de la lettre de voiture électronique à travers l'extension de la notion d'écrit est une importante innovation en droit OHADA[61].

Les formalités accomplies auprès des Registres du Commerce et du Crédit

[59] Voir l'Acte additionnel de la CEDEAO du 16 février 2010, sur la protection des données à caractère personnel, articles 38 et suivants. Le cas malien déjà examiné est similaire.

[60] Voir art. 2, point c, de l'AUCTMR.

[61] Voir, pour plus de détails, sur la lettre de voiture électronique, voir A. OUATTARA, "Une innovation technologique dans l'espace OHADA: la lettre de voiture électronique en matière de contrats de transport de marchandises par route". *In*: *Revue internationale de droit comparé*. Vol. 60 N° 1, 2008. pp. 61-85.

Mobilier au moyen de documents électroniques et de transmissions électroniques ont, aux termes de l'article 82 AUDCG, les mêmes effets juridiques que celles accomplies avec des documents sur support papier, notamment quant à leur nature juridique et leur force probatoire. Les documents sous forme électronique sont substituables aux documents sur support papier et sont reconnus comme équivalents lorsqu'ils sont établis et maintenus selon un procédé technique fiable, garantissant, à tout moment, l'origine du document sous forme électronique et son intégrité au cours des traitements et des transmissions électroniques. L'usage d'une signature électronique qualifiée est défini comme étant un procédé technique fiable et garantissant, à tout moment, l'origine des documents sous forme électronique, leur intégrité au cours de leurs traitements et de leurs transmissions électroniques[62]. L'article 84, AUDCG, quant à lui, définit le certificat électronique employé en support de la signature électronique qualifiée comme étant une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne[63].

2. La création d'un dispositif de mise en œuvre de l'informatisation du RCCM

Le législateur OHADA a prévu un dispositif pour la mise en œuvre de l'information du RCCM. D'abord, est créé un Comité technique de normalisation des procédures électroniques[64]. Le Comité technique de normalisation des procédures électroniques détermine les critères à remplir pour être un prestataire de services de certification électronique. Il est ainsi appelé à jouer un rôle important dans l'effectivité de l'informatisation du RCCM, à travers son pouvoir d'appréciation et de contrôle.

Le législateur de L'OHADA a envisagé des règles concernant l'utilisation et la conservation des documents électroniques. L'article 86, AUDCG, admet la possibilité de présenter la demande ou la déclaration ainsi que les pièces justificatives, totalement ou partiellement, sous forme électronique, à condition de respecter les dispositions de l'article 79 de l'AUDCG, en ce qui concerne le destinataire et du respect des dispositions des articles 82 à 85 dudit Acte uniforme relativement à la conformité des documents. Quand la voie électronique est choisie, les personnes chargées des Registres du Commerce et du Crédit Mobilier délivrent, dans le respect des dispositions de l'AUDCG, les mêmes actes que ceux délivrés en cas d'accomplissement des formalités sur support papier[65].

L'accusé d'enregistrement avec les mentions requises par l'AUDCG, ou par tout autre Acte uniforme ou toute autre disposition légale, doit indiquer que les formulaires, documents, actes ou les informations attendus ont bien été reçus par le destinataire et sont exploitables, notamment par des traitements électroniques. L'accusé d'enregistrement doit être délivré par le greffier ou le responsable de l'organe compétent dans l'Etat Partie en charge du Registre du Commerce et du Crédit Mobilier dès réception de la demande ou de la déclaration par voie électronique

[62] Voir l'article 83 de l'AUDCG, concernant la signature électronique qualifiée.

[63] Voir aussi, l'alinéa 2 de l'article 84, AUDCG.

[64] Art. 81, AUDCG. *Adde*, A. CISSE et B. DIALLO, "L'informatisation du Registre du Commerce et du Crédit Mobilier et des fichiers connexes, *Droit et patrimoine*, n° 281, mars 2011, p. 62., Ohadata D-12-14.pdf.

[65] Voir art. 87, al. 2 AUDCG.

conformément aux dispositions de l'AUDCG[66].

L'article 89 de l'AUDCG prévoit, en outre, que lorsqu'une demande ou une déclaration est faite sous forme électronique et à défaut de la signature électronique du demandeur, du déclarant ou de son mandataire, sa validation est faite par le greffier ou le responsable de l'organe compétent dans l'Etat Partie en charge du Registre du Commerce et du Crédit Mobilier par sa propre signature électronique qualifiée, après examen du document et des pièces justificatives. Une autorité administrative a également la possibilité de communiquer au Registre du Commerce et du Crédit Mobilier, directement sous forme papier ou support électronique, les informations soumises à publicité en vertu des dispositions de l'AUDCG ou de tout autre Acte uniforme ou de toute autre disposition légale, nonobstant la présence de données à caractère personnel[67].

Un accent particulier est mis sur la conservation des documents électroniques. L'article 91 de l'AUDCG, prévoit que la conservation de la déclaration ou de la demande établies sur support électronique est assurée dans des conditions de nature à en préserver la durabilité, l'intégrité et la lisibilité. Il en est de même pour ce qui concerne l''ensemble des informations concernant la déclaration ou la demande dès son établissement, telles que les données permettant de l'identifier, de déterminer ses propriétés, notamment les signatures électroniques qualifiées, et d'en assurer la traçabilité. Une précision importante est faite par le même article en indiquant que les opérations successives justifiées par sa conservation, ne retirent pas aux enregistrements électroniques des déclarations ou des demandes leur valeur d'original. En outre il faut que le procédé de conservation permette l'apposition par le greffier ou le responsable de l'organe compétent dans l'Etat Partie en charge de mentions postérieures à l'enregistrement sans qu'il en résulte une altération des données précédentes.

Le législateur communautaire a aussi réglementé l'utilisation de la voie électronique pour la transmission des documents[68]. Les informations sont considérées être envoyées par moyens électroniques lorsqu'elles sont émises et reçues à destination au moyen d'équipements électroniques de traitement, y compris la compression numérique, et de stockage de données, et entièrement transmises, acheminées et reçues par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques selon des modalités définies par les États parties, mais permettant l'interopérabilité entre le système d'information des émetteurs et récepteurs.

Des accusés de réception sont envoyés par les organismes destinataires aux organismes émetteurs. Ils sont munis de la signature électronique qualifiée du greffier ou du responsable de l'organe compétent dans l'Etat Partie de l'organisme destinataire[69]. L'article 100 de l'AUDCG prévoit la possibilité de la transmission par voie électronique aux organismes administratifs destinataires de l'État partie les informations et pièces justificatives les concernant, nonobstant la présence de données à caractère personnel, ce qui est une importante mesure pour l'efficacité de l'informatisation. Mais des règles sont prévues pour la protection des données à caractère personnel[70].

[66] Voir aussi l'article 88, AUDCG.

[67] Voir article 90, AUDCG.

[68] Voir articles 92-96, AUDCG.

[69] Voir art. 96, AUDCG.

[70] Voir pour le cas du Mali, *supra*, p. 6 et s.

Pour compléter le dispositif de mise en œuvre de l'informatisation du RCCM, la publicité et la diffusion des informations des registres sous forme électronique est également admise[71]. En effet, tout intéressé a la possibilité d'obtenir sous forme électronique les informations figurant sur les formulaires déposés au Registre du Commerce et du Crédit Mobilier. Il en est de même pour la communication des extraits ou copies de tout ou partie des documents publiés au Registre du Commerce et du Crédit Mobilier en application de l'Acte uniforme portant droit commercial général, de l'Acte uniforme relatif au droit des sociétés commerciales et du groupement d'intérêt économique et de l'Acte uniforme portant organisation et harmonisation des comptabilités des entreprises. La copie sur support électronique de tout ou partie d'un dossier individuel sur papier peut également être obtenu par l'organe en charge du RCCM. La certification des copies électroniques est également réglementée. Elle intervient à la demande expresse de l'intéressé, faute de quoi les informations concernées ne valent que comme simple renseignement[72]. Le législateur communautaire a aussi traité la question relative au coût de l'obtention de l'information. Ce coût ne doit pas dépasser le coût administratif de l'opération[73]. Cette mesure est prévue pour éviter que ce coût ne dépasse certaines proportions, ce qui serait de nature à décourager les utilisateurs du support électronique. La diversité des interventions[74] pour adapter le droit au numérique permet de comprendre qu'il y a une certaine justification à ce processus.

3. L'apport de l'AUDSC/GIE du 30 janvier 2014

Sans rentrer dans les détails, il faut aussi souligner l'adaptation du droit des sociétés au numérique opérée par l'Acte uniforme portant droit des sociétés commerciales et du groupement d'intérêt économique (AUDSC/GIE) du 30 janvier 2014. De façon générale, sont admis la diffusion d'information par voie électronique, les formalités et les publicités électroniques, l'écrit électronique, l'utilisation de l'électronique dans la préparation et la tenue des assemblées générales, dont la visioconférence[75].

Concernant notamment le cas des convocations par voie électronique, l'article 286 de l'AUDSC/GIE précise que "*Les convocations par télécopies et courrier électronique ne sont valables que si l'associé a préalablement donné son accord écrit et communiqué son numéro de télécopie ou son adresse électronique, selon le cas. Il peut à tout moment demander expressément à la société par lettre recommandée avec demande d'avis de réception que le moyen de communication sus mentionné soit remplacé à l'avenir par un envoi postal*". Cette disposition apporte une précieuse protection à l'associé concerné.

La prise en compte du numérique en droit des sociétés constituent une des

[71] Art. 97 et s., AUDCG.

[72] Voir art. 98, AUDCG.

[73] Art. 99, AUDCG.

[74] Voir J. DIFFO TCHUNKAM, envisage les « perspectives d'un Acte uniforme OHADA relatif aux transactions électroniques (voir J. DIFFO TCHUNKAM, « Actualité et perspective du droit OHADA des affaires après la réforme de l'Acte Uniforme relatif au Droit Commercial Général du 15 décembre 2010 », *in :* http://afrilex.u-bordeaux4.fr/sites/afrilex/IMG/pdf/_Actualite_et_perspective_du_droit_OHADA_des_affaires_apres_la_reforme_de_l_Acte_Uniforme_relatif_au_Droit_Comm_.pdf.

[75] Parmi les diverses dispositions de l'AUDSC/GIE portant adaptation du droit des sociétés au numérique, on peut citer les articles 93; 133-1; 256-1 et 256-2; 286; 303: 456; 827-7 et suivants.

innovations majeures de l'AUDSC/GIE du 30 janvier 2014. Ces innovations participent à la modernisation de ce droit et au renforcement de la transparence, de la rapidité, de la simplicité, sans préjudice de la sécurité en la matière.

CONCLUSION

L'adaptation du droit au numérique est diversifiée. Au plan interne, elle est restée pendant longtemps timide; mais actuellement elle est fortement prometteuse. L'intervention assez poussée des législateurs des principales communautés régionales auxquelles fait partie le Mali, est fortement diversifiée. Mais cette intervention est très récente, sauf le cas de l'UEMOA qui date de 2002. Par ailleurs, les diverses adaptations du droit au numérique opérées çà et là, sont toutes justifiées par le souci de tirer le maximum de profit des opportunités offertes par le numérique tout en apportant aux acteurs toute la sécurité juridique et judiciaire nécessaire, ce implique de gagner également le pari technologique.

Mais ce que l'on peut constater c'est que les questions soulevées dans le domaine de l'adaptation du droit au numérique n'ont souvent reçu que des solutions assez partielles, compte tenu de la constante évolution des nouvelles technologies, en donnant naissance, à chaque fois, à de nouvelles interrogations. Il appartient alors aux juristes de continuer à suivre cette évolution, ce qui invite, sans doute, à la poursuite de la réflexion sur la problématique de l'adaptation du droit au numérique. Le législateur malien doit s'inspirer des diverses expériences en la matière, aussi bien au niveau africain qu'au niveau mondial, afin d'avoir une politique législative cohérente et diversifiée en la matière afin de mettre en œuvre les différentes réformes envisagées.

BIBLIOGRAPHIE

1. **ABI-RIZK (D.),** *L'Internet au service des opérations bancaires et financières, (*sous la dir. de Th. BONNEAU), Th., Université Panthéon-Assas (Paris II), 2006.
2. **BERRAULT (C.)** et *alii*., « DADVSI 2, HADOPI, « création et Internet ». … De bonnes questions ? De mauvaises réponses », *D*. 2008, p. 2290.
3. **BAILLY (E.) et DAOUD (E.),** « Cybercriminalité et réseaux sociaux : la réponse pénale », *AJ Pénal* 2012, p. 252.
4. **BONHOMME (R.)**, « Le déclenchement de l'opération de paiement : le consentement et l'ordre », *JCP E*, 2010, 1032.
5. **BOSSAN (J.)** "La dématérialisation de la procédure pénale", *D*. 2012, p. 627.
6. **CATALA (P.)**, *Le Droit à l'épreuve du numérique. Jus ex Machina*, PUF, 1999.
7. **CAZENEUVE (J.)**, « Cybercriminalité : l'émergence d'un nouveau risque », *AJ Pénal* 2012, p. 268.
8. **CISSE (A.)** et **DIALLO (B.**), "L'information du Registre du Commerce et du Crédit Mobilier et des fichiers connexes, *Droit et patrimoine*, n° 281, mars 2011, p. 62., *Ohadata D-12-14*.pdf.
9. **CORNU (G.)**, *Vocabulaire juridique*, Association Henri CAPITANT, 4e éd. PUF, Quadrige, 2003.
10. **DAUBIGNEY (M.-Ch.)**, "La marche vers la dématérialisation de la procédure pénale", *AJ Pénal* 2007 p. 460.
11. **DIFFO TCHUNKAM (J.)**, « Actualité et perspective du droit OHADA des affaires après la réforme de l'Acte Uniforme relatif au Droit Commercial Général du 15 décembre 2010 », http://afrilex.u-bordeaux4.fr/sites/afrilex/IMG/pdf/_Actualite_et_perspective_du_droit_OHADA_des_affaires_apres_la_reforme_de_l_Acte_Uniforme_relatif_au_Droit_Comm_.pdf, publié en Octobre 2012.

12. DIOUF (Nd.), « Infractions en relations avec les nouvelles technologies de l'information et Procédure pénale : l'inadaptation des réponses nationales face à un phénomène de dimension internationale », *AFRILEX*, N° 4, p. 251, *in* : http://www.afrilex.u-bordeaux-4.fr.

13. DUTILLEUL (F. C.), «Quelle place pour le contrat dans l'ordonnancement juridique ? » *in La nouvelle crise du contrat*, (sous la direction de Ch. JAMIN et D. MAZEAUD), éd. Dalloz, 2003, p. 225.

14. FONTAINE (M.), « La formation des contrats, codifications récentes et besoins de la pratique », *in Liber Amicorum Commission Droit et Vie des Affaires*, BRUYLANT, Bruxelles, 1998.

15. FLOUR (J.) et AUBERT (J.-L.), *Droit civil, Les obligations, 1. L'acte juridique*, Armand COLIN, 7e éd., 1996.

16. GEIGER (Ch.), « HADOPI », ou quand la répression devient pédagogique. (…) », *D.*, 2011, p. 773.

17. GUILLOT (J.-L.) –BERARD (P.-Y.), Com. 20 janvier 2009, Chron. *Revue Banque*, 07/05/2009, n° 712.

18. JAMIN (Ch.) et MAZEAUD (D.), (sous la direction de), *La nouvelle crise du contrat*, éd. Dalloz, 2003.

19. LECUYER (H.), « Le contrat acte de prévision », *in Mélanges* TERRÉ, *L'avenir du droit*, éd. Juris-Classeur, Paris 1999, p. 643 et s.

20. *LE Nouveau PETIT ROBERT*, nouvelle édition sous la direction de **J. REY-DEBOVE et A. REY**, Dictionnaires le ROBERT, Paris, 2002.

21. *Le petit Larousse illustré*, Larousse HER 2000.

22. Le TOURNEAU (Ph.), *Contrats informatiques et électroniques*, 2ème éd. refondue, Dalloz, coll. « Dalloz Référence », 2002.

23. LUCAS (A.), *Code civil*, Litec, 2006.

24. OCDE, – *Rapport 2001*, Encadré VI-1. 2002, *in* : VI : L'économie du savoir et les opportunités du numérique », Revue de l'OCDE sur le développement, 2002/1 no 3, p. 181-197.

25. OUATTARA, (A.), "Une innovation technologique dans l'espace OHADA: la lettre de voiture électronique en matière de contrats de transport de marchandises par route". *In*: *Revue internationale de droit comparé*. Vol. 60 N° 1, 2008. pp. 61-85.

26. PRADEL, (J.), - "De la géolocalisation en procédure pénale. A la recherche d'un statut", *JCP G*, 2014, doctr. 100;

27. PRADEL, (J.), -"La géolocalisation: un exemple de vide législatif rapidement comblé dans l'urgence. A propos de la loi n° 2014-372 du 28 mars 2014", JCP G, 2014, act. 415.

28. QUEMENER, "La procédure pénale à l'épreuve de la géolocalisation", *AJP*, 2013, p. 568.

29. SOW (D.), - *Le déséquilibre des relations de crédit entre la banque et les usager*s, Thèse de doctorat d'Etat, FSJP de l'UCAD, 18 octobre 2008;

30. SOW (D.), "L'adaptation du droit au numérique", *RCDA*, N° 1, Janvier-Mars 2013, p. 5.

31. SOW (D.) "Réflexion sur l'adaptation du droit des contrats au numérique", *Revue C.A.M.E.S./ S.J.P.*, N° 001/2015, p. 63.

32. VASSEUR (M.), « Le paiement électronique Aspects juridiques », *JCP*, 1985, I, 3206.

VIVANT (M.), "L'informatique dans la théorie générale du contrat", *D.* 1994, chron., p. 117. /.