BANQUE DES MÉMOIRES

Master de Droit du numérique
Dirigé par Monsieur Jérôme PASSA
2022

L'identité numérique et les services de confiance dans l'espace OHADA

Franck ADOPO

Sous la direction de Monsieur Éric CAPRIOLI

Avertissement

« La Faculté n'entend donner aucune approbation ni improbation aux opinions émises dans ce mémoire ; ces opinions doivent être considérées comme propres à leur auteur ».

Remerciements

Je tiens à remercier Monsieur le Professeur Jérôme PASSA pour m'avoir donné la chance de suivre le programme de ce Master, riche tant par sa renommée que par la diversité et la qualité de ses intervenants.

Je remercie tout particulièrement, mon encadreur Monsieur Éric CAPRIOLI, pour avoir accepté de diriger ce mémoire et pour m'avoir conseillé, grâce à son expertise, tout au long de sa réalisation.

Je voudrais enfin remercier toutes les personnes qui de près ou de loin, ont contribué à la réalisation de ce travail, et tout particulièrement Arielle ADJA et la famille ASSE BROU, sans qui ce rêve n'aurait pas été possible.

Table des Matières

LISTE DES ABREVIATIONS

Abréviations	**Libellés**
Acte Uniforme	Acte Uniforme pour l'application du droit OHADA
AUDCG	Acte Uniforme sur le droit commercial général
Art.	Article
AUTMR	Acte Uniforme sur le transport de marchandises par route
Bull. civ	Bulletin des arrêts de la Cour de cassation (chambre civile)
Cass. Com.	Cour de cassation chambre commerciale
CEDEAO	Communauté économique des États de l'Afrique de l'Ouest
CEMAC	Communauté économique et monétaire de l'Afrique centrale
Ed.	Edition
Ibid.	Ibidem
JORF	Journal officiel (Lois et décrets)
OHADA	Organisation pour l'Harmonisation en Afrique du Droit des Affaires
Op. cit.	Opère Citato
RCCM	Registre du commerce et du crédit mobilier
Règlement eIDAS	RÈGLEMENT (UE) N° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique
Rev.	Revue
SGIN	Service de garantie de l'identité numérique
UE	Union européenne
ZLECAf	Zone de libre-échange continentale africaine
UEMOA	Union économique et monétaire ouest-africaine

Introduction

« Seul le sang, la famille,

l'histoire, le temps identifient un être humain.

Le sang est la meilleure carte d'identité »,

Jean-Marie Adiaffi, La carte d'identité,

Coll. Monde Noir poche, Editions Hatier International, 2002

La question de l'identité a toujours été au cœur des préoccupations sociétales[1], plus particulièrement dans les sociétés africaines. La personne a toujours été identifiée à la communauté et non vis-à-vis de l'individu seul. Dans cette conception, l'individu existe grâce à la société. Aujourd'hui, surtout à l'ère du numérique et de la dématérialisation, il ne serait pas superflu de se demander si cette conception de l'identité est toujours d'actualité. Car le digital a renforcé l'individualisation de la personne et a créé de nouvelles communautés dites virtuelles, n'obéissant pas aux normes sociales classiques[2]. Par ailleurs, la question de l'identité n'est plus seulement une question de sang, de famille, mais une donnée économique importante[3]. À tel point que plusieurs entreprises assoient leurs business modèles sur la donnée. Cela montre à quel point la conception de l'identité de l'individu a évolué tant en Afrique que dans le reste du monde. On est passé d'un individu rattaché à la communauté à un individu ultra consommateur et objet de toutes les entreprises.

Dans un contexte actuel marqué par un changement de paradigme dans les modèles économiques, les pays africains en particulier ceux de l'espace OHADA ont décidé de se tourner vers une économie plus libérale en favorisant la zone à l'investissement. L'OHADA est l'Organisation pour l'harmonisation en Afrique du droit des affaires. Elle a été instituée par le Traité du 17 octobre 1993 relatif à l'harmonisation du droit des affaires en Afrique signé à Port-Louis en Ile Maurice. Le traité a été révisé à Québec au Canada le 17 octobre 2008, puis entré

[1] Desgens-Pasanau, Guillaume. Freyssinet, Éric. L'identité à l'ère numérique. Présaje. Paris: Dalloz, 2009, p.7 : « Parménide et Héraclite s'interrogeaient déjà sur le lien entre changement et identité ».
[2] Kaufmann, Jean-Claude. L'invention de soi. Une théorie de l'identité, Armand Colin, Paris, 2004, p.352.
[3] Desgens-Pasanau, Guillaume. Freyssinet, Éric. L'identité à l'ère numérique. Présaje. Paris: Dalloz, 2009, pp.8-9

en vigueur le 21 mars 2010. Depuis le 31 décembre 2014, il compte dix-sept Etats membres ayant ratifié le traité[4]. L'article 1er du Traité, n'ayant pas subi de modification à l'occasion de la révision dispose que : « Le présent Traité a pour objet l'harmonisation du droit des affaires dans les Etats-Parties par l'élaboration et l'adoption de règles communes simples, modernes et adaptées à la situation de leurs économies, par la mise en œuvre de procédures judiciaires appropriées, et par l'encouragement au recours à l'arbitrage pour le règlement des différends contractuels ». L'OHADA a un champ d'application matériel très large et intervient dans une multitude de domaines tournant autour du droit des affaires comme le prévoit l'article 2 du Traité non modifié à l'occasion de la révision[5]. L'arsenal normatif de l'organisation porte une dénomination assez innovante. Il s'agit des « Actes Uniformes » prévus par le titre 2 du Traité. En effet, l'OHADA se veut une organisation qui apporte des changements concrets dans la vie des affaires. C'est pourquoi ces règles matérielles sont dotées d'un caractère obligatoire et une application directe dans tous les Etats membres[6] à l'instar des règlements européens.

Ainsi, l'objectif de l'organisation a toujours été de faire de ce vaste espace économique, une destination de choix en matière de sécurité, d'investissement, d'innovation et de concurrence. Ainsi, elle n'hésite pas à mobiliser les ressources nécessaires, mobiliser les partenaires adéquats et réunir les chercheurs dans le but de rendre concret cette volonté formulée depuis sa naissance et qui jusqu'à aujourd'hui demeure une priorité.

Elle n'est d'ailleurs pas la seule initiative sur le continent à promouvoir l'investissement. En effet, les Etats membres de l'Union Africaine ont récemment signé à Kigali un Accord portant création de la zone de libre-échange continentale africaine (ZLECAf) avec pour objectif la création d'un marché unique et la libéralisation du commerce des services en Afrique[7].

L'on assiste ainsi à un foisonnement d'initiatives sur tout le continent afin de mettre en avant le potentiel économique de l'Afrique. Ainsi, l'OHADA et ses institutions, dans le but de mettre en place des solutions innovantes, constituent ainsi un appui considérable pour le secteur privé

[4] Annexe 1, Carte coloriée de l'espace OHADA, Droit Afrique, http://www.droit-afrique.com/pays/ohada/
[5] Traité portant révision du Traité relatif à l'harmonisation du droit des affaires en Afrique, adopté le 17 octobre 2008 à Québec, publié au Journal Officiel n°20 du 01 novembre 2009, Art. 2 : « - Pour l'application du présent Traité, entrent dans le domaine du droit des affaires l'ensemble des règles relatives au droit des sociétés et au statut juridique des commerçants, au recouvrement des créances, aux sûretés et aux voies d'exécution, au régime du redressement des entreprises et de la liquidation judiciaire, au droit de l'arbitrage, au droit du travail, au droit comptable, au droit de la vente et des transports, (...) ».
[6] Ibid. Art. 10 : « Les actes uniformes sont directement applicables et obligatoires dans les Etats-Parties, nonobstant toute disposition contraire de droit interne, antérieure ou postérieure ».
[7] Union Africaine, Accord portant création de la zone de libre-échange continentale africaine, signé à Kigali, le 21 mars 2018, Art.3.

qui lui-même demeure un pilier de la croissance économique. En effet, l'OHADA et ses partenaires[8] dans leurs objectifs d'encourager les PME et les grands acteurs économiques privés à investir dans la zone, ont intérêt à instaurer un climat plus sécurisé et de confiance notamment dans la réglementation liée à l'utilisation des nouvelles technologies. L'institution n'est d'ailleurs pas hostile à un projet d'Acte Uniforme dans ce domaine[9].

La récente actualité en droit OHADA a tourné autour de la réforme de plusieurs Actes Uniforme notamment celui relatif au droit commercial général qui avait pour objectif de renforcer la sécurité judiciaire et juridique dans l'exécution des contrats commerciaux. L'une des innovations majeures a porté sur l'introduction de nouvelles notions liées au numérique et à la digitalisation des procédures dans la zone. Cette réforme a entraîné une accélération du processus d'informatisation du registre du commerce et du crédit mobilier (RCCM) de l'OHADA avec pour objectif de rendre possible « la réalisation des formalités légales, la conservation et la diffusion, en temps réel et sous forme électronique »[10].

La réforme ayant eu lieu entre 2010 et 2011, il convient aujourd'hui de faire un état des lieux post-réforme sur l'efficacité des nouvelles règles et pratiques introduites par celle-ci.

En effet, afin d'assurer un meilleur suivi et une amélioration de l'avancée majeure des pratiques des affaires dans l'espace OHADA, une étude est la bienvenue. D'autant plus que de nouveaux enjeux sont aujourd'hui à l'ordre du jour. Il s'agit des enjeux sécuritaires et de l'accroissement de la confiance dans les échanges économiques.

En effet, l'identité des différents acteurs ne saurait passer inaperçue dans ce contexte de digitalisation. Car pour garantir son efficacité, il faut que les acteurs soient identifiés voire clairement identifiés et que les outils mis à leur disposition soient des outils sûrs, infalsifiables afin d'éviter de nombreuses fausses opérations et surtout l'usurpation d'identité et la cyberdélinquance dans cet espace économique qui se veut attractif.

Si la notion de l'identité numérique revêt une importance capitale, son analyse démontre qu'elle n'est pas aisée à appréhender. Certains auteurs estiment à juste titre qu'elle se trouve « dans le

[8] Digital Africa. Fonds d'amorçage pour les start-up numériques africaines. https://www.afd.fr/fr/ressources/fonds-damorcage-pour-les-start-numeriques-africaines.
[9] CNUDCI. OHADA. OIF. Note de concept, Projet de réunion conjointe CNUDCI – OHADA – OIF sur les enjeux et défis de l'économie numérique en Afrique et dans la sphère francophone (en ligne, 11 mai 2021), p. 3.
[10] LexisNexis. L'ESSENTIEL Droits africains des affaires. RCCM informatisé de l'OHADA, LEDAF, juin 2017, n°06, p. 8.

paradigme de la complexité »[11] voire que sa technicité revêt un caractère v ésotérique »[12]. C'est ce qui a poussé les auteurs du Livre Blanc « blockchain et identité » initié par le Ministère de l'intérieur de la République française à affirmer que : « L'identité dite « numérique » (ou « électronique ») n'est que l'émanation de l'identité juridique inscrite sur un support numérique ou électronique et dont le contenu est supposé demeurer immuable. À proprement parler, il n'existe pas d'identité numérique, la numérisation n'étant qu'un processus qui permet de transcrire des éléments d'identité sur support numérique, lequel permet de remonter à l'identité juridique»[13]. À côté de cette vague doctrinale tendant à nier la capacité du droit à cerner ce concept[14], la Principauté de Monaco a pris l'initiative d'adopter une définition de la notion d'identité numérique. Ainsi, selon une loi de 2019 de la Principauté, « l'identité numérique d'une personne est constituée de données d'identification personnelle sous la forme d'un identifiant numérique représentant de manière univoque une personne physique ou une personne morale »[15].

En tout état de cause, la majorité des textes en la matière fait référence à la notion d' « identification électronique ». C'est notamment le cas du RÈGLEMENT (UE) N° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (Règlement eIDAS) , faisant l'objet d'un projet de révision actuellement. Ce Règlement auquel nous n'hésiterons pas à faire référence dans le cadre de cette étude, constitue une réglementation assez aboutie en termes d'identité numérique et de services de confiance. C'est d'ailleurs à bon droit que plusieurs Etats de l'OHADA s'en sont inspirés pour élaborer leurs propres législations en la matière[16]. Le Règlement eIDAS définit l'identification électronique comme « le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale »[17]. Plus concrètement, c'est un procédé électronique qui va permettre à une personne d'établir qui

[11] Caprioli, Éric A. Signature électronique et dématérialisation: droit et pratiques. Droit & professionnels. Communication et commerce électronique. Paris: LexisNexis, 2014.
[12] Desgens-Pasanau, Guillaume. Freyssinet, Éric. L'identité à l'ère numérique. Présaje. Paris: Dalloz, 2009, p. 13.
[13] Ministère de l'Intérieur. Livre blanc Blockchain et Identification Numérique : restitution des ateliers du groupe de travail « blockchain et identité (BCID) ». mai 2021, p. 31.
[14] Bardin, Michaël. « L'identité numérique et le droit : esquisse d'une conciliation difficile », Hermès, La Revue, vol. 80, no. 1, 2018, pp. 283-291.
[15] Loi n° 1.483 du 17 décembre 2019 relative à l'identité numérique, Art.2.
[16] CNUDCI. OHADA. OIF. Note de concept, Projet de réunion conjointe CNUDCI – OHADA – OIF sur les enjeux et défis de l'économie numérique en Afrique et dans la sphère francophone (en ligne, 11 mai 2021), p. 3.
[17] Règlement eIDAS, Art. 3.1.

elle est[18]. En général ce simple procédé ne suffit pas, il est accompagné d'une authentification[19]. En pratique, c'est l'étape qui va consister à « confirmer que la personne revendiquant une identité est bien la personne qu'elle prétend être »[20].

À côté de ces définitions, le Règlement eIDAS précise une série d'autres définitions qui ne sera utile pour la suite de cette étude. Ainsi, le Règlement eIDAS définit le moyen d'identification électronique comme « un élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne »[21]. Ensuite, les données d'identification personnelle doivent être analysées comme « un ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale »[22]. Enfin, l'expression schéma d'identification électronique doit être considéré comme « un système pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales, ou à des personnes physiques représentant des personnes morales »[23]. Afin de mieux cerner la notion et les concepts connexes qui gravitent autour. L'identité numérique est utilisée et constitue aujourd'hui un facteur important de la souveraineté.

L'autre concept important qui fera l'objet de notre étude est celui des services de confiance. S'il s'agit d'un concept qui a connu son essor avec la révolution numérique, il constitue aujourd'hui un concept incontournable pour le bon fonctionnement de l'économie numérique. En effet, les acteurs économiques, pour la sécurisation et l'authentification de leurs opérations, ne peuvent pas s'empêcher d'avoir recours à ces services. Le Règlement eIDAS définit le service de confiance comme « un service électronique normalement fourni contre rémunération qui consiste: - en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services; ou - en la création, en la vérification et en la validation de certificats pour l'authentification de site internet; ou - en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services ; »[24].

[18] Le Tourneau, Philippe. Contrat de commerce en ligne : données juridiques. Chapitre 412, Dalloz 2021/22
[19] Règlement eIDAS, Art. 3.5: « «authentification», un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique »
[20] Thibault Douville. « Enfin un cadre juridique général pour l'identification électronique ! ». Recueil Dalloz – D. 2018. 676
[21] Règlement eIDAS, Art. 3.2.
[22] Ibid., Art. 3.3.
[23] Ibid., Art. 3.4.
[24] Ibid., Art. 3.16.

Afin d'élever le niveau de qualité et assurer une bonne prestation aux acteurs économiques, le Règlement établit des critères pour l'octroi du titre de «service de confiance qualifié»[25]. Ainsi les services de confiance sont intrinsèquement liés à l'identité numérique car ce sont eux qui permettent de la vérifier et de garantir sa fiabilité.

Une revue des textes existant dans l'OHADA a permis de constater que ces notions restent moins méconnues par cette législation. Or dans la pratique, les prestataires privés ne cessent de s'installer et de proposer leurs services aux acteurs économiques de la zone et même aux institutions. Ce qui crée une certaine incertitude et insécurité juridique, allant dans le sens contraire aux objectifs de l'organisation[26]. Ainsi, il serait légitime de se demander, après plus de dix années de réforme, quel est l'état des lieux en matière d'utilisation de moyens électroniques, même si cette idée suscite de la réticence chez certains auteurs[27].

Au vu des observations évoquées, nous tenterons dans notre analyse de répondre à la question centrale suivante : quelle est l'état des moyens d'identification électronique et des services de confiance dans l'espace OHADA ?

Notre analyse consistera dans un premier temps à analyser comment est perçue la notion d'identité numérique dans l'OHADA **(Titre 1),** puis dans un second temps nous aborderons la question de l'encadrement des services de confiance **(Titre 2).**

Titre 1: L'identité numérique dans l'OHADA

L'OHADA compte aujourd'hui plusieurs Actes Uniformes qui mettent en relation des individus, des commerçants, des clients, des justiciables, des entreprises locales comme étrangères. Comment rendre efficace cette cohabitation si elle n'est pas sécurisée? Car l'un des enjeux majeurs de l'encadrement de l'identité numérique, c'est la lutte contre l'usurpation d'identité et la fraude[28]. Il est clair que la sécurisation des échanges passe indéniablement par une identification réussie et crédible des personnes et des entités.

[25] Règlement eIDAS, Art. 3.17
[26] Cissé, Abdoullah. « L'harmonisation du droit des affaires en Afrique :. L'expérience de l'Ohada à l'épreuve de sa première décennie ». *Revue internationale de droit économique*, vol. xviii,2, no. 2, 2004, p. 2.
[27] Ibid., p. 6.
[28] Alliance pour la Confiance Numérique. Identité numérique : enjeux et solutions. Dossier de presse, juin 2012, p.9.

Il convient donc de s'interroger dans un premier temps sur l'existence d'un régime juridique encadrant l'identité numérique **(Chapitre 1),** puis de poser les bases d'une réflexion allant dans le sens de la mise en œuvre d'un régime juridique propre à l'identité numérique dans l'OHADA **(Chapitre 2).**

Chapitre 1: Quel régime juridique pour l'identité numérique dans l'OHADA?

Il est de tradition de laisser aux soins des Etats la question de l'identité des individus, dans le sens où elle « permet un rattachement de l'individu à la société à laquelle il appartient »[29]. En effet, cela relève de leur devoir, établir une identité pour chaque citoyen[30]. L'actualité révèle d'ailleurs que plusieurs Etats n'ont pas attendu les organismes régionaux pour s'acquitter de ce devoir. Ainsi, plusieurs Etats se sont dotés de dispositifs biométriques pour identifier leurs citoyens[31]. Mais dans le contexte de l'OHADA, une nécessité s'impose, celle d'identifier non seulement les acteurs actifs, mais aussi tous les citoyens de l'OHADA[32]. La réforme de l'Acte Uniforme relatif au droit commercial général a d'ailleurs posé les premières pierres d'une identification des acteurs économiques en instaurant la dématérialisation du RCMM et la mise en place d'un numéro d'identification unique des entreprises[33]. Mais, l'identification des entreprises telle que prévue par l'acte uniforme suffit-elle à couvrir tout le périmètre et les exigences de l'identité numérique proprement dite? Car face à la croissance des échanges numériques entre les acteurs, une identification simple, classique ne saurait suffire, l'institution doit se doter d'un système d'identification numérique afin de sécuriser au mieux les échanges et protéger non seulement les acteurs, mais aussi les bénéficiaires des services proposés. Il s'agira donc dans notre analyse de montrer l'absence de régime juridique commun pour l'identité numérique dans l'OHADA **(Section 1)**, avant de présenter quelques initiatives élaborées dans ce sens sur le continent **(Section 2).**

[29] Deharo, Gaëlle. « L'identité numérique dans les procédures judiciaires », Les Cahiers du numérique, vol. 7, no. 1, 2011, pp. 87-102.
[30] Déclaration universelle des droits de l'homme, 10 décembre 1945, Art. 6.
[31] Awenengo Dalberto, Séverine. Banégas, Richard. Cutolo, Armando. « Biomaîtriser les identités ? État documentaire et citoyenneté au tournant biométrique ». Politique africaine, vol. 152, no. 4, 2018, pp. 5-29.
[32] Mercadal, Barthélemy. Séminaire international sur « le droit africain et le développement social », du 30 octobre au 2 novembre 2009-11-13 : « l'espace Ohada regorge plus de 170 millions de citoyens ».
[33] Acte Uniforme DCG, Art. 80 : « Dans chaque État Partie, le Registre du Commerce et du Crédit Mobilier et le Fichier National peuvent être tenus et exploités soit sur support papier, soit sous forme électronique. Le Fichier Régional est tenu et exploité soit sur support papier, soit sous forme électronique. ».

Section 1: L'absence de régime juridique commun

De tous les Actes Uniformes, aucune disposition n'évoque la question de l'identité numérique **(§1).** De plus, aucun Acte Uniforme n'a été consacré à une telle question importante comme c'est le cas dans d'autres institutions comme l'UE qui s'est dotée d'un règlement pour traiter de la question, le Règlement eIDAS. Il se pose une véritable nécessité pour l'OHADA de se doter d'un tel dispositif **(§2).**

§1: L'identité numérique, un concept important mais méconnu des Actes Uniformes

L'OHADA s' inscrit dans une vision de facilitation et de modernisation des échanges commerciaux dans les dix-sept pays membres. Pour se faire, une harmonisation de dix-sept législations différentes a dû avoir lieu. En procédant ainsi, ce sont plusieurs frontières commerciales qui sont tombées mettant en place une clientèle commune et des acteurs communs dans toute la zone. Dans un besoin de sécurisation des échanges commerciaux et divers dans l'OHADA, il est primordial de doter l'institution d'un corpus de règles encadrant l'identité numérique. À l'instar de l'Union européenne avec le Règlement eIDAS, il ne s'agit pas pour le législateur OHADA d'imposer aux Etats membres « la mise en place de dispositifs sécurisés des identités numériques »[34], mais dans son objectif constant d'harmonisation, établir des critères de fiabilité et une certaine opérabilité entre les solutions étatiques. Cela permettra ainsi de renforcer la vision des initiateurs de l'OHADA, créer un espace commun, uniforme en matière de droit des affaires.

Il convient donc de faire une revue générale des Actes Uniformes, analyser chacun, afin de constater d'une part l'état de l'identité numérique, mais aussi montrer l'utilité du concept de l'identité numérique pour le secteur d'activité couvert par cet Actes Uniformes. Nous analyserons d'une part les Actes Uniformes n'ayant pas été modifiés depuis leur entrée en vigueur **(A),** d'autre part nous nous intéresserons aux Actes Uniformes ayant subi une mise à jour de la part du législateur OHADA **(B).**

[34] Caprioli, Éric A. Agosti, Pascal. Cantero, Isabelle, Choukri, Ilène. L'identité numérique dans le droit et la pratique, Revue Banque Édition, Paris, 2021, p. 49.

A. L'identité numérique et les Actes Uniformes non révisés

De tous les Actes Uniformes pris pour l'application du Traité, seulement trois sont encore à leur état initial. Dans la conception de base des Actes Uniformes, la notion d'identité numérique n'a pas été prévue. En effet, cela peut s'expliquer par le fait que les rédacteurs des Actes Uniformes n'étaient pas encore conscients des enjeux juridiques et économiques que pourraient poser les questions liées à ce concept, le premier Acte Uniforme datant d'avant les années 2000. Il est ressorti de notre revue des Actes Uniformes que la notion n'y est pas évoquée. Or elle n'est pas sans importance pour chacune des matières couvertes par ces Actes Uniformes.

D'abord, l'identité numérique occupe une place importante pour la matière des recouvrements des créances et voies d'exécution. Car comment garantir l'efficacité des moyens de recouvrement des créances si le débiteur mais aussi le créancier ne sont pas clairement identifiés? D'autant plus que les problèmes liés à l'utilisation des moyens technologiques sont de plus en plus croissants[35]. Prendre en compte ce concept dans l'Acte Uniforme permettra de faciliter les procédures de recouvrement et l'identification des créanciers à travers tout l'espace OHADA.

Ensuite, le secteur du transport n'est pas en marge des bienfaits que peut apporter l'identité numérique dans les opérations de transports. En effet, l'identification des transporteurs et des clients occupe une place de choix dans la sécurisation des opérations de transport.

Enfin les sociétés coopératives encore dans le domaine rural gagneraient en efficacité si elles passaient toutes par un processus d'identification numérique.

À côté de ces Actes Uniformes qui ont gardé leur version initiale figurent d'autres qui ont fait l'objet d'une réforme.

B. L'identité numérique et les Actes Uniformes révisés

Le premier réflexe aurait été d'affirmer que le législateur OHADA dans le processus de réforme des Actes Uniformes a pris en compte la question de l'identité numérique qui n'avait pas été

[35] Ekani, Serge Christian. « Intégration, exequatur et sécurité juridique dans l'espace OHADA. Bilan et perspective d'une avancée contrastée », *Revue internationale de droit économique*, vol. xxxi, no. 3, 2017, (pp. 55-84.), p.4).

analysée dans la première version des Actes Uniformes. Mais le constat est que le concept demeure toujours absent.

Que ce soit dans l'Acte Uniforme relatif au droit commercial général, celui sur les sûretés révisées en 2010 ou les autres Actes Uniformes révisés après 2010, le constat est le même, l'absence de référence à d'identité numérique. Or l'identité numérique occupe une place de choix dans la mise en œuvre des règles d'encadrement de la vie de affaires

Dans la pratique commerciale, les commerçants, les clients, les utilisateurs doivent être convenablement identifiés. Cela permet de contrôler l'identité des cocontractants[36]. Dans la mesure où la condition tenant aux parties demeure une condition essentielle à la conclusion du contrat. En effet comment savoir si l'on contracte avec la bonne personne, ou est-ce que le consentement n'est pas donné par un mineur par exemple. Il en est de même dans le cas de la gestion des sociétés et dans tous les domaines touchant à la vie des sociétés commerciales, coopératives ou groupements d'intérêts économiques. Comment savoir qu'il s'agit bien du gérant de la SARL qui donne l'ordre? Notamment avec la vulgarisation de l'utilisation des outils de communications à distance et récemment la pandémie du COVID-19. Les entreprises ont été amenées à prendre des décisions comme la tenue d'assemblée générale à distance, ordre de virement par courriel ou par appel téléphonique, procédure de création de société dématérialisée. Afin de prévenir la croissance de l'usurpation d'identité en matière de droit des affaires donnant lieu à la pratique de la fraude au président par exemple[37], il convient de prendre en compte ces notions importantes.

Dans les Actes Uniformes qui concernent les procédures judiciaires et modes alternatifs de litiges, la question n'est pas réglée. L'identité numérique n'est pas évoquée. Or comment rendre efficacement la justice si les justiciables ne sont pas clairement identifiés? Dans un contexte où l'OHADA se tourne vers l'investissement extérieur, des litiges avec des entreprises étrangères ne sont pas exclus. Comment rendre efficace le dispositif de l'arbitrage si des critères d'identification solide ne sont pas mis en place afin d'encadrer l'identité des parties à l'instance arbitrale? Aussi, il existe la question de la forme de la sentence arbitrale qui peut être sous forme électronique. Toutes ces intrusions du numérique dans la vie des affaires dans la zone OHADA imposent au législateur une action afin que les institutions de l'organisme puissent être assez

[36] Piette-Coudol, Thierry. *Le numérique au service du droit de l'OHADA et des États parties*. Droits africains.Paris: EJA LGDJ, 2016, p. 34.

[37] https://www.cybermalveillance.gouv.fr : « L'escroquerie aux faux ordres de virement (FOVI) désigne un type d'arnaque qui, par persuasion, menaces ou pressions diverses, vise à amener la victime à réaliser un virement de fonds non planifié.

prêtes pour affronter les enjeux d'identification que va soulever l'usage et l'entrée du numérique dans la zone.

§2: La nécessité de la création d'un régime juridique commun

L'usage des services numériques n'a pas attendu l'édiction de règle en la matière. En effet, l'Afrique constitue aujourd'hui un grand consommateur de service numérique et se présente comme un futur pôle de développement de l'économie numérique mondiale comme l'atteste ce récent rapport effectué par Google et Société Financière Internationale (IFC) de la Banque Mondiale[38]. Pour faciliter l'utilisation des services numériques dans l'OHADA, les consommateurs ont recours aux moyens d'identification numérique. Ce qui caractérise ces moyens d'identification numérique, c'est leur diversité. Ainsi, il consistera à énumérer les différents types des moyens d'identification **(A)** avant d'analyser leur fonction **(B).**

A. Les éléments de l'identité numérique

Aujourd'hui, les services numériques sont présents à toutes les étapes de la vie de l'individu, tant dans la vie professionnelle que dans la vie non professionnelle. C'est une diversité de moyens d'identification auxquels l'individu doit faire face. Ces moyens peuvent être soit le fruit de la volonté de l'utilisateur, soit une contrainte imposée par les pouvoirs publics ou institutionnels. Ainsi, l'individu peut choisir un pseudonyme, un nom d'utilisateur, un login ou même un avatar sur internet dans ces rapports avec les autres. L'identité numérique ne laisse pas en marge les personnes morales. En effet, lorsqu'une personne morale choisit sa dénomination sociale ou encore un nom de domaine pour l'exercice de son activité commerciale, il s'agit d'élément d'identification.

De même, la possibilité qui est laissée à l'utilisateur de choisir librement les éléments qui vont permettre de l'identifier se justifient par l'essence même du web, « garantir l'anonymat » dans

[38] Google et la Société Financière Internationale (IFC) de la Banque Mondiale. Rapport e-Conomy Africa 2020. Lagos, Nairobi, Johannesburg, 11 novembre 2020 : « l'économie numérique en Afrique pourrait représenter 5,2 % du PIB du continent à l'horizon 2025, soit un peu plus de 180 milliards de dollars. Ce montant pourrait atteindre 712 milliards de dollars à l'horizon 2050 ».

l'utilisation des services numériques[39]. Il existe aussi des éléments beaucoup plus intrusifs que la personne peut communiquer à son insu ou en toute connaissance de cause pour constituer son identification. Ce sont les données de localisation géographique, données biométriques qui constituent des données sensibles.

Dans le but d'une meilleure administration des personnes, les autorités étatiques ou institutionnels peuvent avoir recours à des éléments d'identification qui changent de ceux que l'individu peut librement choisir. En effet, les éléments comme le nom d'état civil, la carte d'identité électronique ou biométrique, adresse IP ou même le numéro d'identification national attribué par les Etats à chaque individu peuvent être utilisés pour identifier numériquement la personne. Il s'agirait ici d'une identification identique tant dans l'utilisation des services numériques que dans la vie quotidienne. Dans ce cas de figure, « l'usage du nom d'état civil comme élément d'identification numérique est d'une efficacité redoutable à l'échelle internationale »[40].

L'objectif pour les Etats est d'avoir une maîtrise sur tous ces éléments d'identification évoqué afin de réguler au mieux les interactions entre les individus et à l'égard des prestataires de services. Mais ce n'est pas toujours le cas car une bonne partie de ces éléments est gérée par des opérateurs privés car elles constituent un potentiel énorme. C'est pourquoi, il est important pour l'OHADA de réguler ces aspects dans la zone afin d'établir des règles uniformes dans la gestion de l'identité numérique.

Si l'énumération des éléments d'identification de la personne est marquée par une grande diversité, il convient de lever le rideau sur l'utilité de ces éléments, quelle est leur fonction?

B. Les fonctions de l'identité numérique

L'identité numérique a une double fonction, celle d'identifier de manière électronique et d'authentifier les personnes dans leurs relations avec les autres ou avec l'administration. En quoi consiste concrètement la fonction d'identification de l'identité numérique? Comme la fonction de l'identité classique, elle permet à la société de pouvoir « individualiser »[41]

[39] Congrès des notaires de France, éd. Le numérique, l'homme et le droit: accompagner et sécuriser la révolution digitale. Paris: Association Congrès notaires de France, 2021, p. 96.
[40] Congrès des notaires de France, éd. Le numérique, l'homme et le droit: accompagner et sécuriser la révolution digitale. Paris: Association Congrès notaires de France, 2021, p. 96.
[41] Castets-Renard, Céline. « Personnalité juridique et identification numérique ». Bioy, Xavier. La personnalité juridique. Toulouse : Presses de l'Université Toulouse 1 Capitole, 2013. pp. 305-317.

l'individu. C'est-à-dire le désigner grâce à des signes qui le caractérisent. Ces signes dans ce cas seront des signes issus de procédés techniques. Le concept d'identification numérique a fait l'objet d'une définition dans le Règlement eIDAS[42].

Une question subsiste encore, celle de l'authentification. En quoi consiste-t-elle? Dans la masse de personne qui circulent dans une zone donnée, la fonction d'authentification permet à la société de pouvoir « retrouver l'individu » [43]. En effet, elle permet d'attester que la personne est vraiment celle qu'elle prétend être. La notion d'authentification a fait l'objet d'une définition dans le Règlement eIDAS. L'article 3.5 la définit comme le « processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique ».

Dans tous les cas, l'encadrement de l'identité numérique est important dans l'espace OHADA dans la mesure où elle permettra d'abord de faciliter les échanges entre les individus et l'administration[44], l'organisation des échanges privés entre entreprise et consommateurs, la sécurité des opérations juridiques et commerciales[45], la lutte contre la fraude, la cybercriminalité, la corruption, le détournement de fonds, le financement du terrorisme, etc.

La notion d'identité numérique revêt une importance assez significative pour que les instances de l'OHADA s'en saisissent et en pose le cadre juridique.

À côté de la situation dans l'OHADA, quel est l'état des lieux dans le reste de l'Afrique en matière d'identité numérique?

Section 2: Les initiatives isolées en matière d'identité numérique en Afrique

[42] Règlement eIDAS, Art. 3.1 : « le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale ».
[43] Castets-Renard, Céline. « Personnalité juridique et identification numérique ». Bioy, Xavier. La personnalité juridique. Toulouse : Presses de l'Université Toulouse 1 Capitole, 2013. pp. 305-317.
[44] Caprioli, Éric A. Agosti, Pascal. Cantero, Isabelle, Choukri, Ilène. L'identité numérique dans le droit et la pratique, Revue Banque Édition, Paris, 2021, p. 59.
[45] Ibid., p. 93.

L'Afrique n'est pas en marge des innovations numériques et de la sécurisation des échanges électroniques. En effet, il existe plusieurs initiatives tant au niveau des Etats **(§1),** que d'autres institutions régionales en matière d'identité numérique **(§2).**

§1: La diversité des initiatives nationales

L'OHADA compte aujourd'hui dix-sept pays[46] et une grande disparité se présente en matière de développement et d'innovation. Ainsi, il convient de préciser de prime abord que pour certains Etats, l'utilisation et la gestion de l'identité numérique demeure une réussite **(A).** Cependant d'autres Etats ne sont pas dotés d'un système d'identité numérique **(B).**

A. La présence de système de gestion de l'identité numérique

Au nombre des Etats qui se sont dotés d'un système de gestion de l'identité numérique figurent le Sénégal, la Côte d'Ivoire et plusieurs autres Etats à travers des lois instaurant le système de carte d'identité biométrique.

Le Sénégal est l'un des premiers pays dans la zone à s'être doté d'un tel système. En effet, c'est la Loi n° 2016-09 du 14 mars 2016 instituant une carte d'identité biométrique CEDEAO qui a enclenché le processus. Il s'agit d'une carte d'identité multifonction qui contient les données biométriques comme le nom, le prénom, le sexe, la date et lieu de naissance, l'adresse, la taille, la couleur des yeux, les empreintes digitales et la photographie. Le dispositif a pour objectif lointain d'y ajouter des données de santé. Ce dispositif multifonction a vocation à servir de carte d'identité nationale, de carte d'électeur, de permis de conduire, de carte bancaire. Ainsi, c'est la mobilité qui est rendue facile et surtout la sécurisation des échanges. Cependant le dispositif contient encore quelques limites. En effet, il n'existe pas encore d'interopérabilité entre les différents services étatiques sur l'identité numérique. Des efforts sont encore à faire pour que le Sénégal ait un système d'identité numérique autonome et sécurisé. C'est d'ailleurs ce qui est ressorti lors du Forum sur l'identité numérique et la gouvernance.

En Côte d'Ivoire, c'est la loi n°2019-566 du 26 juin 2019 instituant une carte nationale d'identité biométrique qui est à l'origine de ce premier pas vers l'identité numérique. La carte permet au détenteur de prouver son identité et sa nationalité ivoirienne dans toutes les opérations qui le requiert. Le dispositif est doté d'une puce électronique et a pour vocation d'assurer plusieurs

[46] Annexe 1, Carte coloriée de l'espace OHADA

fonctions comme celle de permis de conduire en plus de la fonction initiale de prouver l'identité. Elle va permettre d'accroître les dispositifs de sécurité déjà mis en place dans le pays. Mais le dispositif connaît quelques limites comme la rapidité de la délivrance du titre. En effet, la nouvelle carte arrivant en fin de validité de l'ancienne met du temps à être délivrée sur l'ensemble du territoire national. Cette situation place les ivoiriens dans une situation sans identité. De même, la question de l'interopérabilité entre les services pas encore d'interopérabilité entre les services de l'administration sur la base de la carte d'identité biométrique n'a pas encore été évoquée. Il serait important qu'elle puisse être prise en compte afin d'achever le processus d'identification qui a été engagé.

En plus de ces deux exemples, il existe des pays comme le Mali, le Burkina, le Bénin qui se sont aussi dotés d'une carte d'identité biométrique.

À côté de ces initiatives, il existe des États qui n'ont pas encore mis en place ce type de systèmes. Des projets sont annoncés mais leur mise en œuvre n'a pas encore suivi.

B. L'absence d'un système de gestion de l'identité numérique

Plusieurs Etats membres de l'OHADA n'ont pas encore mis en place un système de gestion de l'identité numérique. Mais des initiatives sont en vue. En effet, le Congo a annoncé l'adoption en février 2022 du projet de décret-loi portant création d'une carte d'identité nationale en République Démocratique du Congo, basé sur des données biométriques.

Le Congo a émis l'idée de mettre en place un système de carte d'identité numérique pour certifier et fixer l'identité. Il s'agit en effet d'une zone où tant les enjeux économiques que sécuritaires sont des plus importants. Les Congolais n'ont pas de carte d'identité. Ils font usage de la carte d'électeur pour se faire identifier[47].

Au Gabon, il existe une réelle difficulté pour la mise en œuvre d'une carte d'identité biométrique annoncée depuis 2012 à travers le projet le projet Iboga (Identité biométrique officielle du Gabon). Cependant, une annonce de la reprise en 2022 a été faite.

L'on note une disparité en termes de développement de l'identité numérique dans la zone OHADA. Certains Etats semblent réussir tandis que d'autres ont encore du mal. L'intervention de l'OHADA permettra à ces derniers de rejoindre les autres Etats afin d'avoir une identité

[47] Adoption du décret pour la création de la carte nationale d'identité nationale RDC

numérique commune dans tout l'espace OHADA. Il s'agit ici d'un facteur de développement important qui s'inscrit parfaitement dans la vision de l'OHADA.

Les Etats ne devraient pas ignorer certains systèmes assez réussis comme celui du Nigéria qui s'est doté depuis 2007 d'une base de données de l'identité nationale. Il faut noter que le Nigéria va vers la suppression de la carte et remplace ce dispositif par un numéro d'identification unique qui suffit à lui seul à assurer toutes les fonctions de l'identité numérique.

Si des avancées considérables se sont fait remarquer dans la zone Ouest de l'OHADA, c'est bien sous l'impulsion des organisations régionales qui jouent un rôle moteur dans la libre circulation des citoyens à travers leurs zones.

§2: Les initiatives régionales

Les institutions africaines jouent un rôle clé dans les différents processus de gestion de l'identité numérique. En effet, regroupant plusieurs Etats à la fois et doté de plus de moyens, ces institutions à vocation communautaire sont tournées vers une certaine fédération des efforts des Etats dans un but de libre circulation des personnes mais aussi des produits afin d'accroître le potentiel de l'Afrique. C'est le cas de l'instauration de la ZLECAf qui regorge de plusieurs opportunités. Cet accord dont l'un des objectifs est de « créer un marché unique pour les marchandises et les services facilité par la circulation des personnes afin d'approfondir l'intégration économique du continent africain »[48] demeure un projet significatif et doté de plusieurs opportunités. Mais pour que ce dispositif soit une réussite, l'Union Africaine devra s'appuyer sur des dispositifs organisant l'identité numérique afin de sécuriser la circulation des personnes.

Pour ce faire, plusieurs modèles se présentent aux institutions africaines dont « le modèle le mieux achevé à ce jour est celui de l'Union européenne »[49]. En effet, la question ne se pose plus au sein de l'Union européenne car l'organisme s'est doté du Règlement eIDAS ayant vocation à organiser l'interopérabilité des solutions nationales encadrant l'identité numérique. Les Etats membres de L'OHADA sont situés tant en Afrique de l'ouest, qu'en Afrique centrale. C'est

[48] Accord portant création de la zone de libre-échange continentale africaine (ZLECAf), Kigali, le 21 mars 2018, Art. 3 (a).
[49] Zogo Nkada, Simon-Pierre. « La libre circulation des personnes : réflexions sur l'expérience de la C.E.M.A.C. et de la C.E.D.E.A.O. », Revue internationale de droit économique, vol. xxv, no. 1, 2011, pp. 113-136.

pourquoi nous analyserons le dispositif mis en place au niveau de la CEDEAO **(A)**, avant d'étudier celui de la CEMAC **(B).**

A. Le passeport biométrique de la CEDEAO

Au titre des initiatives régionales en matière d'identité numérique, celui de la CEDEAO reste l'un des plus emblématiques avec l'instauration du passeport biométrique. Ce dispositif est l'un des premiers de ce type dans la région. Il a pour objectif de permettre la libre circulation des biens et des citoyens de la CEDEAO sur l'ensemble du territoire de la communauté[50].

Il faut noter que cette initiative est le propulseur de toutes les lois de la zone CEDEAO en matière d'identité numérique. En effet, l'organisation n'a pas simplement instauré une idée, elle a aussi formulé une intention en direction des Etats membres. Celle de rendre effective cette volonté de faire tomber les frontières. Cette invitation est prévue à l'article 59.2 du Traité révisé comme suit : « les Etats Membres s'engagent à prendre toutes les mesures appropriées en vue d'assurer aux citoyens de la Communauté la pleine jouissance des droits visés au paragraphe 1 du présent article ».

Il s'agit d'une réelle volonté de la communauté qui a été exprimée depuis 1979 avec le Protocole A/SP.1/5/79 de Dakar du 25 mai 1979 sur la libre circulation des personnes, le droit de résidence et d'établissement. Ce protocole a posé le principe de base qui a été entretenu par la législation postérieure de la Communauté. C'est notamment le cas le Protocole A/P/3/5/82 du 29 mai 1982, signé à Cotonou et portant code de la citoyenneté de la Communauté, suivi d'un autre Protocole A/SP.1/7/86 d'Abuja du 1er juillet 1986 relatif au droit de résidence. Puis à Banjul, les Etats Membres ont adopté le Protocole A/SP.2/5/90 de Banjul du 29 mai 1990 relatif au droit d'établissement, celui qui a précédé la de 2016 instaurant la carte d'identité biométrique de la CEDEAO entérinée par la 46ème conférence des chefs d'Etats et de gouvernements de la Communauté économique des Etats d'Afrique de l'ouest (CEDEAO), tenue à Accra en juillet 2014[51]. Si le passeport CEDEAO a été instauré depuis décembre 2000, il a fallu une Décision AIDEC du 01 décembre 2014 modifiant la décision MODIFIANT LA Décision AIDEC 2/7/85 portant institution d'un carnet de voyage des Etats Membres de la CEDEAO pour propulser les initiatives des Etats. Grâce à ce document, la libre circulation est garantie.

[50] Traité Révisé CEDEAO, Abuja, 14 Janvier 2006, Art. 59.1 : « Les citoyens de la Communauté ont le droit d'entrée, de résidence et d'établissement et les Etats Membres s'engagent à reconnaître ces droits aux citoyens de la Communauté sur leurs territoires respectifs, conformément aux dispositions des protocoles y afférents ».
[51] https://en.unesco.org/creativity/policy-monitoring-platform/traite-de-la-cedeao-pour-la-libre

Sur la base de tous ces textes, les Etats Membres sont invités à mettre sur le plan national toutes les mesures nécessaires pour garantir cette circulation. C'est dans cette optique que les projets de d'établissement de carte nationale d'identité ont vu le jour.

Quelle est la situation dans les Etats de l'Afrique centrale?

B. Le passeport biométrique de la CEMAC

En Afrique Centrale, la CEMAC n'est pas en marge de cet élan de développement de l'identité numérique. En effet, l'organisation s'est dotée de son dispositif en adoptant le Règlement n°01/08-UEAC-042-CM-17 du 20 juin 2008 portant institution et conditions de gestion et de délivrance du passeport CEMAC. Ce document a vocation à établir la libre circulation des ressortissants de la Communauté[52]. Mais ce texte n'est pas isolé en matière de libre circulation des personnes dans la zone[53]. Il a été précédé de plusieurs textes notamment le Règlement n° 1/100 - CEMAC-042-CM-04 du 21 juillet 2000 portant institution et conditions d'attribution du passeport CEMAC, puis l'Acte additionnel n° 08/CEMAC-CEE-SE du 29 juin 2005 relatif à la libre circulation des personnes en zone CEMAC. Par la suite a été adoptée une première décision n° 02/08-UEAC-CM-17 du 20 juin 2008 portant liste des personnes admises à titre transitoire à circuler sans visa en zone CEMAC. Il a fallu attendre plusieurs années plus tard pour que la libre circulation de tous les citoyens de la communauté soit effective. C'est l'Acte additionnel n° 01/13-CEMAC-070 U-CCE S.E du 25 juin 2013 portant suppression du visa pour tous les ressortissants de la CEMAC circulant dans l'espace communautaire définitivement instauré cette possibilité. L'article 1er de cet Acte additionnel dispose que : « la circulation des ressortissants des Etats membres de la CEMAC est libre sur l'ensemble de l'espace communautaire à partir du 1er janvier 2014, sous réserve de la présentation d'une carte nationale d'identité ou d'un passeport délivré par un Etat Membre et en cours de validité ». Cependant cette libre circulation connaît une limite posée à l'article 2 de l'Acte additionnel, elle ne peut pas excéder 90 jours[54].

[52] Règlement CEMAC, Yaoundé, 20 juin 2008, Art. 2 : « le passeport CEMAC confère à son titulaire, le droit de circuler librement, sans visa au sein de l'espace CEMAC. A cet effet, il tient lieu également de pièce d'identité ».
[53] BIPELE KEMFOUEDIO, Jacques. « La libre circulation des personnes comme droit fondamental en zone CEMAC». La Revue du Centre Michel de L'Hospital.
[54] Acte additionnel CEMAC, n° 01/13-CEMAC-070 U-CCE S.E du 25 juin 2013, Art. 2 : « la libre circulation prévue à l'article 1er du présent Acte Additionnel comporte le droit de se déplacer sans visa et de séjourner dans tout autre Etat de la Communauté pour une durée de quatre-vingt-dix (90) jours au plus ».

Il faut noter enfin que le passeport CEMAC n'avait pas été adopté par l'ensemble des Etats de la zone. En effet, le Gabon n'avait pas encore procédé à l'homologation de cet instrument d'expression de la libre circulation de tous les ressortissants de la zone dans les Etats frères de leurs choix. Aujourd'hui c'est chose faite depuis le mois de mai 2022[55].

Il ressort de notre analyse qu'il n'existe pas de régime établi pour l'identité numérique dans l'OHADA bien que cette notion regorge de nombreux enjeux tant économiques que sécuritaires. Néanmoins, les États parties et certaines organisations régionales ont montré l'exemple.

Mais, il faut noter qu'il existe encore des insuffisances. Car les dispositifs mis en place restent encore des collectes de données biométriques ne faisant pas encore l'objet d'un fichier numérisé, sécurisé et accessible dans toute la zone. Il serait judicieux d'avancer dans ce sens en posant les bases d'une interopérabilité des systèmes d'identification numérique pour garantir l'efficacité de ces moyens isolés déjà mis en place.

C'est pourquoi, nous essayerons de mettre en lumière les exigences qu'un système de gestion de l'identité numérique dans l'OHADA peut soulever afin de faire de cette organisation centrale le pilier de l'interopérabilité des systèmes d'identification numérique en Afrique.

Chapitre 2: La proposition d'un cadre normatif harmonisé pour l'identité numérique dans l'OHADA

Au vu de ce qui précède, il n'existe pas encore de système normatif harmonisé au sein de l'OHADA pour encadrer l'identité numérique des ressortissants de cette zone. C'est pourquoi pour asseoir notre proposition, nous nous orienterons vers d'autres systèmes communautaires assez reconnus en la matière pour en tirer les éléments clés qu'il faudra adapter au cadre de l'OHADA. Dans le cadre de cette étude, c'est le Règlement eIDAS qui fera l'objet de notre support de proposition. Néanmoins, il faut noter que ledit Règlement fait l'objet actuellement d'un projet de révision qui pourra entraîner des changements dans le système actuel[56].

[55] Le Gabon homologue le passeport biométrique de la CEMAC.
[56] Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL, modifiant le règlement (UE) n°910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique

La question centrale qui se pose dans notre analyse est celle de l'interopérabilité. En effet, nous avons vu récemment que plusieurs Etats disposaient d'une carte d'identité numérique ou même biométrique. Mais ces instruments d'identification ne faisaient pas encore l'objet d'un fichier central permettant l'interopérabilité avec les dispositifs présents dans d'autres Etats. Ce qui freine la volonté de certaines organisations communautaires à veiller à la libre circulation sécurisée et efficace des ressortissants de ces communautés. Il s'agit d'une question qui a été résolue avec l'adoption du Règlement eIDAS qui a eu pour effet de « supprimer l'obstacle que représente pour la libre prestation de services, que les citoyens-consommateurs ne peuvent pas utiliser leur identification électronique pour s'authentifier dans un autre État membre parce que les schémas nationaux d'identification électronique de leur pays n'y sont pas reconnus »[57]. Alors, doter l'OHADA d'un système d'identification numérique passera par deux points importants. La création de schémas d'identification d'une part **(Section 1)** et la mobilisation de règles relatives à la sécurisation de ces schémas d'autre part **(section 2).**

Section 1: Les propositions relatives à la création des schémas d'identification électronique

Les schémas d'identification électronique constituent la clé de voûte de la mise en œuvre de l'identité numérique. En effet, c'est grâce à ces schémas que sont délivrés les moyens d'identification à une entité[58]. Pour les rendre plus efficaces, les schémas d'identification doivent obéir à certains critères qu'il va falloir établir **(§1),** et par la suite organiser une reconnaissance mutuelle entre les États de ces schémas afin de garantir leur interopérabilité **(§2).**

§1: L'établissement de critères encadrant les schémas d'identification

Avant d'analyser la finalité de l'établissement de ces critères **(B),** il convient de dresser la liste des différents requis pour l'établissement de ces critères **(A)**.

[57] Rev . crit. DIP, Création du marché unique numérique, 2014. 975.
[58] Opt. Cit. 20

A. La nature des critères d'établissement des schémas d'identification électronique

L'article 7 du Règlement eIDAS pose une série de conditions cumulatives nécessaires pour l'établissement des schémas d'identification. D'abord, la première série de conditions tient à l'entité qui délivre le schéma. Il doit émaner soit d'un Etat Membre, soit d'un réalisé par un autre organisme mais dans le cadre d'un mandat délivré par un Etat Membre, soit en dehors de toutes ces cas mais reconnu tout de même par un Etat Membre[59]. En l'espèce, avec un tel système, les Etats Membres de l'OHADA pour garder le contrôle de la production de schémas d'identification électronique sur leur territoire. Ensuite, une autre condition tient à la fonction du schéma en question. En effet, les moyens d'identification électronique relevant du schéma d'identification électronique doivent pouvoir être utilisés pour accéder au moins à un service qui est fourni par un organisme du secteur public et qui exige l'identification électronique dans l'État membre notifiant[60]. Dans ce cas, des mesures supplémentaires accompagnent la mise en œuvre de ce schéma. Il doit respecter des normes de qualité mises en place pour assurer son intégrité[61].

Ensuite la deuxième série de conditions tient au processus d'attribution de données personnelles d'identification de la personne dans le cadre de la mise en œuvre du schéma. Cette attribution devra se faire en fonction du niveau de garantie qui aura été requis[62]. L'obligation pèse aussi bien sur l'entité qui délivre les moyens d'identification que sur l'Etat en question[63]. En l'espèce, l'OHADA devra veiller à ce que le respect des exigences de garantie soit effectif.

Par ailleurs, la troisième série de conditions est relative à la disponibilité de l'authentification en ligne nécessaire pour l'utilisation du schéma d'identification. Elle doit être effective pour les utilisateurs[64]. En effet, pour que toute personne présente sur le territoire puisse avoir accès au service, sa disponibilité doit être effective. L'OHADA devra veiller au respect de cette condition de disponibilité. Enfin les dernières conditions tiennent à la procédure de communication des schémas aux autres Etats membres, avant un certain délai, conformément à l'obligation posée par l'article 12 du même Règlement qui concernent l'interopérabilité des schémas. En l'espèce, l'OHADA devra veiller à mettre en place un mécanisme de

[59] Règlement eIDAS, Art. 7.a).
[60] Ibid., Art. 7.b).
[61] Ibid., Art. 7.c & Art. 8.3.
[62] Ibid., Art. 7.d.
[63] Ibid., Art. 7.e.
[64] Ibid., Art. 7.f.

communication des schémas entre Etats afin d'assurer l'effectivité de l'interopérabilité des schémas d'identification.

En France, ces services seront assurés par la complémentarité FranceConnect[65] et le service de garantie de l'identité numérique (SGIN)[66], remplaçant le dispositif Alicem[67].

FranceConnect est « un système d'identification et d'authentification mis en place par l'Etat, offrant gratuitement la possibilité aux usagers d'utiliser un compte, un identifiant et un mot de passe uniques pour un accès sécurisé à l'ensemble des services publics et privés référencé chez FranceConnect »[68]. Grâce à ce système, tous les comptes publics du citoyen sont liés. Il peut accéder à ses espaces publics de déclaration d'impôts, de sécurité sociale en passant par l'interface FranceConnect. Pour assurer un service complet et de qualité, le dispositif FranceConnect est complété par le dispositif SGIN. Ce dispositif a pour « finalité de mettre à disposition des titulaires d'une carte nationale d'identité comportant le composant électronique mentionné à l'article 1-1 du décret du 22 octobre 1955 susvisé un moyen d'identification électronique leur permettant de s'identifier et de s'authentifier auprès d'organismes publics ou privés grâce à une application qu'ils installent sur leur équipement terminal de communications électroniques permettant la lecture sans contact de ce composant L'application permet à l'usager, notamment, de générer des attestations électroniques comportant les seuls attributs d'identité dont il estime la transmission nécessaire aux tiers de son choix »[69]. Ainsi FranceConnect assure l'interface et le dispositif assure la création et la sécurisation de l'identité numérique des utilisateurs.

[65] Arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect », Journal officiel électronique authentifié n° 0180 du 06/08/2015.
[66] Décret n° 2022-676 du 26 avril 2022 autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (SGIN) et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », Journal officiel électronique authentifié n° 0098 du 27/04/2022.
[67] Décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », abrogé, Journal officiel électronique authentifié n° 0113 du 16/05/2019.
[68] Caprioli, Éric A. Agosti, Pascal. Cantero, Isabelle, Choukri, Ilène. L'identité numérique dans le droit et la pratique, Revue Banque Édition, Paris, 2021. p. 63.
[69] Décret n° 2022-676 du 26 avril 2022 autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (SGIN) et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », Journal officiel électronique authentifié n° 0098 du 27/04/2022, Art. 1.

L'OHADA ainsi que les Etats membres pourraient s'inspirer de ces systèmes de gestion de l'identité numérique assez avancés. A présent, il convient d'analyser quelle est la finalité de la mise en place de critères d'établissement de l'identité numérique.

B. La finalité des critères d'établissement des schémas d'identification électronique

L'article 8 du Règlement eIDAS pose trois niveaux de garantie des schémas d'identification. Ainsi, il faut distinguer les niveaux de garantie faible, substantiel et élevé.

D'abord, le niveau de garantie faible concerne le « moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un degré limité de fiabilité à l'identité revendiquée ou prétendue d'une personne, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire le risque d'utilisation abusive ou d'altération de l'identité »[70]. Il s'agit du premier niveau de garantie qui ne présente pas une fiabilité assez complète. Ensuite, le niveau de garantie substantiel renvoie à « un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un degré substantiel de fiabilité à l'identité revendiquée ou prétendue d'une personne, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité »[71]. C'est le niveau intermédiaire qui offre un niveau de sécurité assez moyen. Enfin, le niveau de garantie élevé qui renvoie à « un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un niveau de fiabilité à l'identité revendiquée ou prétendue d'une personne plus élevé qu'un moyen d'identification électronique ayant le niveau de garantie substantiel, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est d'empêcher l'utilisation abusive ou l'altération de l'identité »[72]. C'est le dernier niveau qui offre le degré de sécurité maximal. La Commission autorise la notification des schémas en fonction du niveau de sécurité. Ainsi,

[70] Règlement eIDAS, Art. 8.2,a).
[71] Ibid., Art. 8.2,b).
[72] Ibid., Art. 8.2,c).

« seuls les deux derniers niveaux sont à notifier à la Commission »[73]. La finalité de ces exigences est bien de garantir un niveau de sécurité le plus inaltérable possible afin d'éviter les risques d'usurpation d'identité ou de compromission des moyens d'identification par les cyberattaques. Ainsi dans sa mise en œuvre des niveaux de garantie, l'OHADA devra veiller à ce que les critères choisis aient pour finalité de garantir la solidité et la crédibilité des moyens d'identification.

Il ressort de notre analyse que la mise en place de critères encadrant l'établissement de schémas d'identification est l'un des piliers de l'intégrité du système d'identification numérique. Ainsi ils doivent faire l'objet de la plus grande attention. L'étape suivante du processus est la reconnaissance des schémas dans tous les Etats membres de l'OHADA. Pour ce faire, un processus particulier doit être mis en place.

§2: La nécessité de la reconnaissance mutuelle des schémas d'identification entre Etats

Quels sont les enjeux de la reconnaissance mutuelle des schémas entre les Etats et par quel processus doit-elle passer? **(A)**. La réponse à cette importante question nous permettra de comprendre plus aisément la fonction essentielle de la reconnaissance qui n'est autre que d'assurer l'interopérabilité des schémas d'identification électronique **(B).**

A. Les enjeux et le processus de reconnaissance mutuelle des schémas d'identification

Pour mieux comprendre les enjeux de la reconnaissance mutuelle des schémas d'identification entre les Etats-Parties de l'OHADA, il faut revenir à la volonté initiale de l'organisation, celle d'œuvrer à « l'harmonisation du droit des affaires dans les Etats-Parties par l'élaboration et l'adoption de règles communes simples, modernes et adaptées à la situation de leurs économies »[74]. Ainsi, la reconnaissance mutuelle des schémas s'inscrit parfaitement dans la vision de l'OHADA d'établir un cadre normatif commun, cette fois-ci en matière d'identification numérique, garant de la sécurisation des échanges commerciaux.

[73] Caprioli, Éric A. Agosti, Pascal. Cantero, Isabelle, Choukri, Ilène. L'identité numérique dans le droit et la pratique, Revue Banque Édition, Paris, 2021. p. 52.
[74] Traité OHADA révisé, Art.1.

Pour comprendre le fonctionnement de la reconnaissance mutuelle, il faut s'orienter vers l'article 6 du Règlement eIDAS. Selon cet article, la reconnaissance mutuelle joue « lorsqu'une identification électronique à l'aide d'un moyen d'identification électronique et d'une authentification est exigée en vertu du droit national ou de pratiques administratives nationales pour accéder à un service en ligne fourni par un organisme du secteur public dans un État membre ». Dans ce cas, lorsque certaines conditions sont réunies « le moyen d'identification électronique délivré dans un autre État membre est reconnu dans le premier État membre aux fins de l'authentification transfrontalière pour ce service en ligne »[75].

Après cette reconnaissance mutuelle, le schéma doit être notifié à la commission. Cette notification est organisée par l'article 9 du Règlement. Elle passe d'abord par la description du schéma d'identification électronique, y compris ses niveaux de garantie et l'entité ou les entités qui délivrent les moyens d'identification électronique relevant de ce schéma. Ensuite, le régime de contrôle applicable et le régime de responsabilité dans la gestion du schéma, l'autorité ou les autorités responsables du schéma, les informations sur l'entité ou les entités qui gèrent l'enregistrement des données d'identification personnelle uniques. Enfin, la reconnaissance mutuelle dépend de plusieurs autres conditions relatives à la description plus détaillée du schéma d'identification électronique et aux dispositions concernant la suspension ou la révocation du schéma d'identification électronique notifié[76].

Dans le cadre de l'instauration des schémas d'identification numérique dans l'OHADA, il s'agit d'étapes qu'il faudra encadrer et détailler avec la plus grande attention de sorte que le processus de reconnaissance ne rencontre pas d'obstacle. Il faudra ainsi veiller à la mise en place d'un organe pour faciliter la gestion de l'identité numérique dans la zone. Cet organe aura vocation à assurer un rôle central et conciliateur entre les Etats. À ce titre, l'organe assurera également la bonne mise en œuvre de l'interopérabilité des schémas d'identification entre les Etats qui constitue l'étape suivante à présenter.

B. L'interopérabilité des schémas d'identification

Le principe de l'interopérabilité des schémas d'identification électronique nationaux est posé par le premier alinéa de l'article 12 du Règlement eIDAS. L'interopérabilité consiste à « échanger des informations, des expériences, des bonnes pratiques concernant tous les aspects

[75] Règlement eIDAS, Art. 6.1.
[76] Ibid.

des schémas d'identification électronique des Etats, en une évaluation des pairs des schémas d'identification électronique relevant du règlement et en un examen des évolutions pertinentes en matière d'identité électronique »[77]. Afin de faciliter l'interopérabilité des schémas d'identification électronique, certaines conditions sont requises[78].

Ainsi, c'est la coopération entre les États qui est facilitée. En droit OHADA, cette coopération sur les schémas d'identification électronique aura un impact significatif sur le monde des affaires. En effet, il sera aisé pour un commerçant béninois de proposer ses produits en Côte d'Ivoire ou au Tchad sans se déplacer et sans que son identité ne soit rendue douteuse par les autorités locales de ces Etats membres. Il en est de même pour une société camerounaise qui souhaite candidater à un appel d'offre public aux Comores.

Dans tous les cas, si l'organisation parvient à réaliser cette connexion entre les Etats, c'est le monde des affaires dans la zone qui sera bénéficiaire. Dans la mesure où il existera une confiance entre les différents opérateurs exerçants dans les Etats, ce qui facilitera les échanges économiques et augmentera la croissance économique de la zone. L'OHADA deviendra ainsi un véritable marché ouvert et communautaire, facilitant ainsi les efforts et la vision de ZLECAF.

D'un point de vue sécuritaire, l'interopérabilité facilitera la coopération des Etats dans la lutte contre la fraude et l'usurpation d'identité. En effet, il faut noter que plusieurs Etats membres de l'OHADA souffrent de la cybercriminalité qui connaît une forte croissance avec la vulgarisation des moyens de communication électroniques. C'est donc une lutte commune qui sera engagée par les Etats.

D'un point de vue pratique, plusieurs Etats ont déjà mis en place ou ont pour projet de mettre en place des systèmes d'identification numérique. Il s'agira pour l'OHADA de leur proposer un accompagnement et une invitation à la mise en conformité de leurs outils nationaux, vis-à-vis des exigences communautaires qui seront adoptées afin de garantir une meilleure efficacité de ces systèmes d'identification.

Après avoir proposé un cadre normatif dans l'optique d'encadrer l'émission de schémas d'identification électronique, il convient à présent de nous intéresser à la sécurisation de ces schémas.

[77] Caprioli, Éric A. Agosti, Pascal. Cantero, Isabelle, Choukri, Ilène. L'identité numérique dans le droit et la pratique, Revue Banque Édition, Paris, 2021, p. 55.
[78] Règlement eIDAS, Art. 3.

Section 2: Les propositions de règles relatives à la sécurisation des schémas d'identification

La question de l'identité des personnes constitue un point essentiel au cœur de l'attention des Etats. En effet, il s'agit d'une question qui touche à la vie privée des personnes. Car il ne faut pas négliger le fait que les données des individus constituent des données à caractère personnel reconnues par plusieurs textes nationaux et internationaux[79].

Les données d'identification des individus sont au cœur de ce mécanisme, c'est pourquoi un point d'honneur doit être mis sur la sécurisation de l'ensemble du processus dans un contexte où l'Afrique est la proie de plusieurs cyberattaques. Il est donc primordial, dans le cadre de la mise en place des moyens d'identification d'encadrer la procédure par suite d'une atteinte à la sécurité des moyens d'identification **(§1),** afin d'établir ensuite la responsabilité des acteurs impliqués dans le processus **(§2).**

§1: L'encadrement de l'atteinte à la sécurité des moyens d'identification

Il conviendra de présenter dans un premier temps les différentes atteintes à la sécurité et les enjeux de la sécurité des données **(A)**, puis dans un second temps, proposer des solutions pour établir un système de sécurité solide **(B).**

A. La présentation des différentes atteintes à la sécurité et leurs enjeux

L'atteinte à la sécurité ne fait pas l'objet d'une définition dans le Règlement eIDAS. Cependant, à la lecture de l'alinéa 1er de l'article 10 du Règlement, il ressort que l'atteinte à la sécurité concerne une altération partielle ou totale de la fiabilité du schéma d'identification notifié selon les modalités prévues par ledit Règlement. Pour qu'il y ait atteinte à la sécurité, il faut que la fiabilité du schéma ait été compromise. Car c'est sur elle que repose l'ensemble du système de

[79] Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel, Art. 1 : « Données à caractère personnel : toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité ».

l'identité numérique. Si elle est atteinte, c'est tout le système qui est atteint. Le système se voit alors dépourvu de toute intégrité. Or l'une des raisons d'être de ce système d'identification est son intégrité en raison des données particulières qu'elle traite.

Il existe une pluralité d'atteinte à la sécurité d'un système informatique. La Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel propose plusieurs cas. Ainsi l'article 29 prévoit comme infraction, le fait d'accéder ou de tenter d'accéder frauduleusement dans tout ou partie d'un système informatique ou de dépasser un accès autorisé, d'accéder ou de tenter d'accéder frauduleusement dans tout ou partie d'un système informatique ou de dépasser un accès autorisé avec l'intention de commettre une nouvelle infraction ou faciliter une telle infraction, de se maintenir ou de tenter de se maintenir frauduleusement dans tout ou partie d'un système informatique, d'entraver, fausser ou tenter d'entraver ou de fausser le fonctionnement d'un système informatique, d'introduire ou tenter d'introduire frauduleusement des données dans un système informatique, d'endommager ou de tenter d'endommager, d'effacer ou tenter d'effacer, de détériorer ou tenter de détériorer, d'altérer ou tenter d'altérer, de modifier ou tenter de modifier frauduleusement des données informatiques. En effet, les schémas d'identification à mettre sur place dans le cadre de l'identité numérique dans l'OHADA peuvent être confrontés à toutes ces atteintes. C'est pourquoi la sécurité des schémas d'identification électronique doit être un point de vigilance pour l'organe qui souhaite le mettre en place.

Quelle est la procédure à suivre en cas d'atteinte à la sécurité du schéma d'identification?

B.la procédure à suivre en cas d'atteinte à sécurité des moyens d'identification

Dans l'article 10 du Règlement eIDAS, l'accent est mis sur les conséquences de l'atteinte à la sécurité des schémas d'identification.

A cet effet, la conséquence immédiate est la révocation ou la suspension des schémas d'identification électronique compromis. Puis après avoir mis hors fonction ces schémas altérés, l'État qui a vu ses schémas altérés doit procéder à la notification de l'incident à l'organe de contrôle et aux Etats membres. Il s'agit d'une procédure assez logique qui s'inscrit clairement dans le processus normal établi dès la création du schéma.

En effet, tout comme la mise en circulation du schéma d'identification électronique a requis l'information de l'organe de contrôle et des Etats membres, son altération doit suivre la même

procédure. En plus de cette mesure, l'article 10 du Règlement prévoit le processus à suivre après la notification car il s'agit d'une suspension temporaire.

Ainsi, la suite sera tributaire de la correction qui aura été apportée après l'atteinte au schéma. Deux situations se présentent donc. D'une part, si l'atteinte a été résolue, l'État membre notifiant rétablit l'authentification transfrontalière et procède à l'information des autres États membres et la Commission[80]. Cependant, si l'atteinte n'a pas été résolue, « dans un délai de trois mois à compter de la suspension ou de la révocation, l'État membre notifiant notifie le retrait du schéma d'identification électronique aux autres États membres et à la Commission »[81].

Nous pensons que l'OHADA pourrait s'inspirer de cette politique de gestion de l'atteinte à la sécurité prévue dans le cadre européen.

Qu'en est-il du régime de responsabilité?

§2: L'établissement d'un régime de responsabilité applicable aux acteurs

Pour achever l'encadrement des schémas d'identification électronique, il convient de s'intéresser au régime de responsabilité applicable aux acteurs impliqués dans la mise en œuvre de ces schémas. Le Règlement eIDAS propose trois régimes de responsabilité qui peuvent être traités en deux étapes. Ainsi, nous présenterons d'une part la responsabilité des Etats membres **(A)**, d'autre part, nous analyserons la responsabilité des prestataires d'identité numérique **(B).**

A. La responsabilité des Etats membres

La responsabilité de l'Etat membre sera engagée chaque fois qu'un dommage aura été causé intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement à ses obligations dans deux cas qui concernent les transactions transfrontalières[82].

[80] Règlement eIDAS, Art. 10.2.
[81] Ibid., Art. 10.3.
[82] Ibid., Art. 11.1.

D'une part, le manquement de l'État membre à son obligation de veiller à ce que les données d'identification personnelle représentant de manière univoque la personne soient attribuées conformément aux spécifications techniques, aux normes et aux procédures pour le niveau de garantie concerné prévues dans l'acte d'exécution visé à l'article 8, paragraphe 3, à la personne physique ou morale visée à l'article 3, point 1), au moment de la délivrance du moyen d'identification électronique relevant de ce schéma[83]; D'autre part, l'obligation de l'Etat de membre notifiant veille à ce qu'une authentification en ligne soit disponible afin de permettre à toute partie utilisatrice établie sur le territoire d'un autre État membre de confirmer les données d'identification personnelle reçues sous forme électronique[84].

Il est important de retenir la responsabilité des Etats en cas de manquement à leurs obligations, afin de garantir une certaine efficacité au processus d'identification. Ce régime de responsabilité amènera les États à plus d'implication dans la gestion de l'identité numérique. L'OHADA doit veiller à prévoir un régime de responsabilité applicable aux Etats pour la même finalité.

A côté de la responsabilité des Etats membres, il existe un autre régime de responsabilité applicable aux prestataires. Qu'en est-il de la responsabilité de ces derniers?

B. La responsabilité des prestataires d'identité numérique

Il convient d'ores et déjà de faire une distinction entre les prestataires qui délivrent des moyens d'identification électronique et ceux qui gèrent des procédures d'authentification. En effet, ils n'obéissent pas au même régime de responsabilité.

Dans le premier cas, le prestataire qui « délivre le moyen d'identification électronique est responsable du dommage causé intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations qui lui incombent en vertu de l'article 7, point e) »[85]. Il s'agit de l'obligation de veiller à ce que le moyen d'identification électronique soit attribué à la personne conformément aux exigences prévues dans le cadre du Règlement pour garantir l'intégrité des moyens d'identification[86].

Dans le deuxième cas, le prestataire qui « gère la procédure d'authentification est responsable du dommage causé intentionnellement ou par négligence à toute personne physique ou morale

[83] Règlement eIDAS, Art. 7,d).
[84] Ibid., Art. 7,f).
[85] Ibid., Art. 11.2.
[86] Ibid., Art. 7,e).

pour ne pas avoir assuré la gestion correcte de l'authentification visée à l'article 7, point f) »[87]. L'obligation de ce dernier consiste à procéder à la confirmation des données d'identification personnelle reçues sous forme électronique[88] par un Etat.

Dans tous les cas, le Règlement eIDAS précise que l'application de ces cas de responsabilité se fait « conformément aux dispositions nationales en matière de responsabilité »[89].

Dans la mise en œuvre des régimes de responsabilité, l'OHADA doit veiller à ne pas piétiner la souveraineté des Etats parties, mais plutôt trouver un compromis afin que la législation de chaque Etat soit respectée et en parfaite adéquation avec le dispositif qui sera mis en œuvre dans le cadre de l'encadrement de l'identité numérique dans l'espace OHADA.

Il ressort de notre analyse que l'OHADA reste attachée à son ambition première, celle de faire de la zone OHADA, une zone de confiance propice à la croissance économique, aux affaires et aux investissements. Face aux nouveaux enjeux du numérique, établir un cadre de l'identité numérique dans la zone n'est plus une option mais un impératif qui contribuera à la consolidation des efforts déjà engagés mais aussi à la sécurisation des échanges économiques et des opérations commerciales.

Nous gardons bon espoir que ces règles verront bientôt le jour en droit OHADA. « L'Acte Uniforme OHADA relatif aux transactions électroniques devra aborder les questions telles que la publicité et le démarchage électronique, la protection du consentement et la conclusion de contrats par voie électronique, la signature électronique ou encore la preuve électronique, y compris les éléments probants introduits par les techniques numériques comme l'horodatage ou les certifications etc. De même, le droit OHADA des transactions électroniques fixera les règles de responsabilité des fournisseurs de biens et services en ligne, la sécurité des échanges électroniques, la protection du consommateur et des données à caractère personnel, ou encore la coexistence des documents électroniques et papiers et l'application des techniques électroniques aux actes commerciaux et administratifs»[90].

[87] Règlement eIDAS, Art. 11.3.
[88] Ibid., Art. 7, f).
[89] Ibid., Art. 11.4.
[90] Zogo, Willy Stéphane, https://www.ohada.com/actualite/5170/article-un-acte-uniforme-ohada-relatif-aux-transactions-electroniques-se-prepare.html.

Titre 2: Les services de confiance dans l'OHADA

Jusqu'en 2010, le droit OHADA était étranger aux normes techniques liées à l'utilisation des nouvelles technologies. Il a fallu attendre la réforme de 2010 pour voir entrer dans l'Acte Uniforme tout un livre sur la dématérialisation et l'utilisation des moyens technologiques. Ces innovations sont prévues dans l'Acte Uniforme OHADA relatif au droit du commerce général dans le livre VI portant sur l'informatisation du Registre du commerce, du Registre national des sûretés et du crédit, du fichier national du commerce et du crédit et du fichier régional du commerce et du crédit.

Ainsi, il ne serait pas juste d'affirmer qu'il n'existe pas de cadre juridique pour l'encadrement des services de confiance dans l'OHADA, cependant, ces règles ne couvrent pas tout le champ d'application de l'OHADA. Ainsi dans notre analyse, nous présenterons l'insuffisance de l'encadrement des services de confiance dans l'OHADA **(chapitre 1),** avant d' identifier le cadre institutionnel relatif aux services de confiance **(chapitre 2).**

Chapitre 1: L'insuffisance des règles encadrant les services de confiance

Dans un premier temps, nous verrons que l'OHADA détient des acquis en matière de règle sur les services de confiance **(Section 1)**, puis dans un second temps, nous présenterons les limites de ces acquis **(Section 2).**

Section 1: Les acquis de l'OHADA en matière de transformation numérique

Dans le cadre de la réforme de 2010, l'OHADA a consacré plusieurs nouvelles notions dans son corpus normatif. C'est ainsi que la notion de signature électronique a fait l'objet d'un encadrement **(§1),** mais aussi la reconnaissance de certains documents électroniques **(§2).**

§1: Les efforts d'encadrement de la signature électronique

L'Acte Uniforme ne propose pas une définition de la notion de signature électronique **(A)**, il présente ses caractéristiques et sa fonction **(B).**

A. L'absence de définition de la signature électronique

C'est à l'article 83 de l'AUDCG qu'apparaît pour la première fois la notion de signature électronique même s'il aurait été bien que le législateur OHADA l'accompagne d'une claire définition. Mais aucune définition n'est proposée. Il faut donc aller chercher dans d'autres corps de règles afin de mieux cerner cette notion importante pour le monde des affaires. Déjà sur le continent africain, une définition existait déjà dans le cadre du droit UEMOA. En effet, l'article 1er du Règlement n°15/2002/CM/UEMOA du 19 septembre 2002 relatif aux systèmes de paiement dans les Etats membres de l'UEMOA définissait la signature électronique de manière assez flou avec un renvoie à un autre article[91]. Il a fallu attendre l'Acte additionnel A/SA.2/01/10 du 16 février 2010 sur les transactions électroniques pour apporter une définition claire à la notion. Ainsi, l'article 1er de l'Acte additionnel, reprise à l'article 34 de l'Acte, définit la signature électronique comme « toute donnée qui résulte de l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ». Mais il s'agit d'une définition similaire à celle de l'article 23 du Règlement UEMOA.

Une autre approche proposée par le Règlement eIDAS considère la signature électronique comme « des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer »[92]. Le Règlement profite pour faire une distinction entre différents types de signatures électroniques. Ainsi, il fait une distinction entre la signature électronique simple[93], la signature électronique avancée[94] et la signature électronique qualifiée[95].

[91] « Signature électronique : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à l'article 23 du présent Règlement ».
[92] Règlement eIDAS, Art. 3.10.
[93] Ibid., Art. 3.10.
[94] Ibid., Art. 3.11: « une signature électronique qui satisfait aux exigences énoncées à l'article 26 ».
[95] Ibid., Art. 3.12; « une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique ».

Dans le cadre de l'OHADA, cette distinction n'est pas encore opérée. En effet, l'article 83 de l'AUCG traite directement de la signature électronique qualifiée qu'il ne prend pas le soin de définir. Néanmoins, si l'Acte Uniforme ne définit pas la notion, elle donne quand même ses caractéristiques. Ainsi, pour être admis au titre de signature électronique OHADA, le dispositif mis en place doit être lié uniquement au signataire, permettre d'identifier dûment le signataire, être créée par des moyens que le signataire peut garder sous son contrôle exclusif, être liée au document auquel elle se rapporte de telle sorte que toute modification ultérieure du document soit détectable[96]. De plus, la signature électronique qualifiée requiert la réunion de certains composants techniques. Elle comprend ainsi, un logiciel de création de signature et un logiciel de vérification de signature et un certificat électronique, authentifiant le signataire, produit par un prestataire de services de certification électronique[97].

Il est clair qu'il n'existe pas un seul type de signature électronique comme le présente l'AUDCG. Il serait dans l'intérêt de l'organisation de mieux préciser le cadre des différentes spécifications de cet outil afin de lui garantir une meilleure efficacité.

Qu'en est-il de ses fonctions?

B. Les fonctions de la signature électronique

Les auteurs sont unanimes sur le fait que la signature électronique doit être mise en place selon des critères techniques particuliers. Dans le cadre de l'OHADA, ces critères sont élaborés par un organe spécial créé à l'occasion de la réforme de l'AUDCG[98].

Ainsi, la signature électronique ne doit pas être confondue avec certains procédés classiques comme « la signature graphique ou la signature biométrique »[99]. Il s'agit plutôt d'un mécanisme qui « repose sur la « cryptographie asymétrique », ou « cryptographie à clé publique », qui se matérialise par la création de « bi-clés », à savoir une clé privée et une clé publique propres à chaque émetteur, les clés privées restant secrètes »[100]. D'ailleurs, il a déjà été jugé qu' « une signature scannée ou imprimée ne vaut pas signature électronique »[101]

[96] AUDCG, Art. 83.
[97] Ibid., Art. 83.
[98] Ibid., Art. 81.
[99] Piette-Coudol, Thierry. Le numérique au service du droit de l'OHADA et des États parties. Droits africains. Paris: EJA LGDJ, 2016, p. 226.
[100] Caprioli, Éric A. Agosti, Pascal. Cantero, Isabelle, Choukri, Ilène. L'identité numérique dans le droit et la pratique, Revue Banque Édition, Paris, 2021, p. 86.
[101] Cass. 2e civ. 30 avril. 2003, n° 00-46.467: JurisData n° 2003-018798.

Tout ce mécanisme est requis en raison de la fonction importante reconnue à la signature électronique.

L'AUCG lui reconnaît deux fonctions essentielles. Celle d'identifier son signataire d'une part, et d'autre part, celle de lui permettre de manifester son consentement[102].

Cette double fonction est un élément clé dans la vie des affaires. En effet, il s'agit de deux éléments essentiels nécessaires à la formation du contrat[103].

En plus de cette fonction, il est couramment reconnu une fonction essentielle à la signature électronique, celle de garantir l'intégrité du document auquel elle est apposée[104]. L'article 82 de l'AUCG n'hésite pas à le rappeler in fine.

Lorsqu'elle remplit les critères qui lui sont imposés, la signature électronique a force probante. En effet, elle a la même valeur que la signature manuscrite dans la mesure où elle permet de garantir « à tout moment, l'origine des documents sous forme électronique, leur intégrité au cours de leurs traitements et de leurs transmissions électroniques »[105].

Les usages de la signature électronique sont diversifiés dans la vie des affaires. Mais le plus important c'est qu'elle demeure incontournable, dans un monde en pleine mutation technologique.

A côté de la signature, il s'agira d'étudier comment le droit OHADA encadre le certificat électronique, moyen technique destiné à garantir la l'efficacité de la signature électronique.

§2: Les efforts d'encadrement du certificat électronique

Dans sa version révisée, l'article 84 de l'AUCG dispose que : « le certificat électronique employé en support de la signature électronique qualifiée est une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne. Il présente au minimum les mentions suivantes : le nom du titulaire du certificat, la clé cryptographique publique du titulaire, la période de validité du certificat, un numéro de série unique, la signature électronique du prestataire de services de certification électronique ».

[102] AUDCG, art. 83.
[103] Ibid., Art. 241 et suivants.
[104] Art. 1367 Code civil français.
[105] AUDCG, Art. 82.

Ainsi, sur la base de cette disposition nous étudierons d'une part les caractéristiques du certificat électronique **(A)**, avant d'analyser la fonction **(B).**

A. Les caractéristiques du certificat électronique

Le certificat électronique est un service intrinsèquement lié à la signature électronique. C'est lui qui confirme sa technicité. En effet, « le certificat est un instrument de sécurité, bien connu des techniciens, sur lequel s'appuie la garantie d'authentification de la signature électronique »[106]. Même si ce n'est pas le cas dans l'AUDCG, le Règlement eIDAS fait une distinction entre le « certificat de signature électronique »[107] et le « certificat qualifié de signature électronique »[108].

De son côté, l'Acte Uniforme pose une condition minimale de données devant figurer sur le certificat électronique. Il s'agit d'abord des données d'identification du titulaire du certificat. Ensuite, doivent figurer des données techniques relatives à l'intégrité du certificat comme la clé cryptographique publique du titulaire, la période de validité du certificat et un numéro de série unique. Enfin, l'autre type de données devant figurant est relatif à la raison d'être du certificat, celle d'authentifier la signature électronique. Ainsi, le certificat électronique doit comporter la signature électronique du prestataire de services de certification électronique.

Il s'agit de procédés qui n'existaient pas encore avant la réforme de l'AUDCG. Ces règles doivent connaître une amélioration au vu de l'avancée des pratiques technologiques.

Qu'en est-il de la fonction de ce certificat électronique?

B. La fonction du certificat électronique

L'article 84 de l'AUCG reconnaît une double fonction essentielle au certificat électronique. En effet, il s'agit de celle de lier les données afférentes à la vérification de signature à une personne; d'une part et, d'autre part celle de confirmer l'identité de cette personne.

Pour réaliser cette double fonction, il faut que l'établissement de certificat électronique soit encadré par des normes techniques élevées. Dans la pratique, ces certificats sont délivrés par

[106] Piette-Coudol, Thierry. *Le numérique au service du droit de l'OHADA et des États parties*. Droits africains. Paris: EJA LGDJ, 2016, p. 56.
[107] Règlement eIDAS, Art. 3.14: « une attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne »
[108] Règlement eIDAS Art. 3.15 : « un certificat de signature électronique, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe I ».

des prestataires spécialisés reconnus pour leur expertise. Le terme pour désigner ces spécialistes varient en fonction du langage juridique et du langage technique.

Ainsi, pour les techniciens, il s'agit d'une « autorité de certification »[109], tandis que pour les juristes, on utilise le terme de « prestataire de service de certification »[110]. La fonction de ce prestataire technique et commercial est de certifier pour son client l'identité de l'auteur de la signature électronique qu'il reçoit et la garantie de l'intégrité de cette signature. Plus concrètement, la mission de ces certificateurs va consister à « vérifier l'identité du demandeur, puis tirer sa biclé cryptographique composée d'une clé privée et d'une clé publique, placer la clé publique du demandeur dans le certificat électronique qu'il crée pour le demandeur et transmettre le certificat (contenant la clé publique) et la clé privée au titulaire d'une façon sécurisée »[111].

Il ressort de notre analyse que la signature électronique et le certificat électronique sont à mi-chemin entre la qualification de moyens d'identification électronique et de service de confiance. Si la question continue de diviser la doctrine, certains auteurs préconisent de garder la classification opérée par le Règlement eIDAS pour qui la signature électronique et le certificat électronique demeurent des services de confiance[112].

Qu'en est-il de l'encadrement des autres services de confiance?

Section 2: L'encadrement des autres services de confiance

Dans sa volonté de légiférer sur les notions du numériques, l'OHADA pourrait inclure dans les services de confiance, les questions d'écrit électronique **(A)** et d'archivage électronique **(B)** car en réalité, il ne s'agit pas de véritable services de confiance. Cependant dans un but de facilitation de l'organisation législative, cette inclusion pourrait être bénéfique.

[109] Piette-Coudol, Thierry. *Le numérique au service du droit de l'OHADA et des États parties*. Droits africains. Paris: EJA LGDJ, 2016, p. 57.
[110] Ibid., p. 57.
[111] Ibid., p 57.
[112] Caprioli, Éric A. Agosti, Pascal. Cantero, Isabelle, Choukri, Ilène. L'identité numérique dans le droit et la pratique, Revue Banque Édition, Paris, 2021, p. 114.

§1: L'écrit sous forme électronique

L'article 86 de l'AUDCG dispose que : « la demande ou la déclaration ainsi que les pièces justificatives peuvent se présenter, totalement ou partiellement, sous forme électronique, sous réserve du respect des dispositions de l'article 79 du présent Acte Uniforme en ce qui concerne le destinataire et du respect des dispositions des articles 82 à 85 du présent Acte Uniforme en ce qui concerne la conformité des documents ». En consacrant une telle disposition, le législateur établit une équivalence entre les documents sous forme classique et ceux sous forme électronique.

L'écrit électronique fait l'objet d'un point d'attention sur le continent. En effet, l'Acte Uniforme sur le transport de marchandises par route avait déjà consacré l'écrit sous forme électronique quand il a défini l'écrit 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 »[113].

La valeur de l'écrit électronique n'est plus à contester. En effet, l'Union Africaine a tranché la question en consacrant de manière définitive l'écrit électronique à titre de preuve. Dans son instrument sur les transactions électroniques, il est possible de lire que « l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier et a la même force probante que celui-ci, 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 »[114].

L'écrit ayant été consacré, qu'en est-il de l'archivage électronique?

§2: L'archivage électronique

Il n'est pas aisé de trouver une définition légale de l'archivage électronique. L'AUDCG l'évoque sans toutefois en donner une définition. L'archivage électronique peut se définir comme « l'ensemble des actions, outils et méthodes mises en œuvre pour conserver à moyen ou long terme des informations dans le but de les exploiter »[115]. Mais « au-delà du stockage, de

[113] Acte uniforme relatif aux contrats de transport de marchandises par route (AUTMR), Art. 2.c.
[114] Convention de l'union africaine sur la cybersécurité et la protection des données à caractère personnel, Art.6.6.
[115] Notaise, Jacques. Barda, Jean. Dusanter, Olivier. Dictionnaire du multimédia. Audiovisuel. Informatique. Télécommunications, AFNOR, 1995.

la sauvegarde et de la gestion électronique des documents, l'archivage électronique peut être défini comme l'ensemble des actions visant à identifier, recueillir, classer et conserver des informations, en vue de consultation ultérieure, sur un support adapté et sécurisé, pour la durée nécessaire à la satisfaction des obligations légales ou des besoins d'information »[116].

Dans le droit OHADA, plusieurs références sont faites à l'archivage électronique. Dans le cadre de la mise en œuvre du RCCM dématérialisé, l'article 91 de l'AUDCG met l'accent sur la capacité de l'archivage électronique à conserver le caractère durable, intègre et lisible de la déclaration ou de la demande d'inscription au RCCM établies sur support électronique.

Fondamentalement, l'archivage électronique à une fonction de stockage et de conservation des documents électroniques. En droit, l'archivage électronique joue un rôle en matière de conservation de la preuve. L'OHADA doit donc encadrer les normes relatives à ce procédé technique.

Il ressort de notre analyse que l'élan vers la dématérialisation des procédures dans l'OHADA est remarquable. Cependant, elle n'est pas allée jusqu'au bout. En effet, plusieurs services de confiance ne font pas encore l'objet d'une réglementation. Ils n'ont pas été pris en compte alors qu'ils ont une importance dans la digitalisation du monde des affaires. C'est le cas du cachet électronique**.** Ce service de confiance est constitué de « données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières »[117]. Les auteurs considèrent qu'il s'agit d'un nouveau service de confiance qui permet de « certifier le lien entre les données électroniques « cachetées » et une personne morale »[118]. C'est d'ailleurs un aspect essentiel qui le distingue de la signature électronique[119]. A côté de ce service de confiance, il y aussi l'horodatage électronique et l'authentification sur internet qui doivent être pris en compte pour un encadrement complet des services de confiance dans la zone OHADA.

[116] Direction des archives de France, Stage technique international des archives, 2009.
[117] Règlement eIDAS, Art. 3.25.
[118] Caprioli, Éric A. Agosti, Pascal. Cantero, Isabelle, Choukri, Ilène. L'identité numérique dans le droit et la pratique, Revue Banque Édition, Paris, 2021, p. 89
[119] Ibid. p.89 : « la signature électronique concerne les personnes physiques et le cachet électronique les personnes morales ».

Chapitre 2: L'analyse du cadre institutionnel de régulation des services de confiance

Pour garantir une efficacité des services de confiance, leur établissement et leur fonctionnement doivent être assurés par un cadre institutionnel structuré. Cependant, il est noté une certaine ineffectivité du rôle des organes de contrôle des services de confiance **(Section 1)** et il se pose une réelle nécessité d'encadrer l'activité des tiers de confiance **(Section 2).**

Section 1: Le rôle des organes de contrôle des services de confiance

Avant d'analyser la nécessité de renforcer le rôle des organes de contrôle étatiques (§2), il convient d'étudier les rôles et missions de l'organe central de contrôle (§1).

§1: L'analyse des rôles et missions de l'organe central de contrôle

A la lecture de la version révisée de l'article 81 de l'AUDCG, il ressort qu'il sera créé un Comité technique de normalisation des procédures électroniques institué au sein de l'OHADA. A la suite de cette annonce, le Règlement n° 02/2010/CM/OHADA du 15 décembre 2010 Portant création, attributions, organisation et fonctionnement du comité technique de normalisation des procédures électroniques de l'OHADA a été adopté afin de rendre effectif la volonté de l'OHADA d'encadrer et de contrôler l'usage des moyens techniques et électroniques dans le monde des affaires.

Ce Comité a pour mission essentielle de veiller à la normalisation des procédures effectuées au moyen de documents et de transmissions électroniques[120]. Cependant, les attributions du Comité technique ne se limitent pas à cette prescription de l'article 81 de l'AUDCG. En effet, il lui attribue un certain nombre de missions. Ainsi, l'article 82 de l'AUDCG lui confie le rôle

[120] AUDCG, Art. 81.

de vérifier et reconnaître « la fiabilité technique des documents électroniques »[121]. C'est lui qui doit établir les critères encadrant l'émission de la signature électronique et du certificat électronique. Par ailleurs, c'est le Comité technique qui a la charge d'organiser l'activité des prestataires de certificat électronique[122]. Enfin, le Comité technique aura pour rôle plus globalement d'assurer la validité des documents électroniques dans le cadre de la gestion du RCCM[123] et organiser la transmission des documents individuelles par le biais de moyens électroniques[124].

Ainsi, le Comité technique dispose d'une mission transversale en ce qui concerne les services de confiance. Cependant, certains auteurs estiment que la mise en place d'un simple régional ne suffit pas. En effet, il faudrait penser à un Comité plus étendue, voire continental[125] qui pourra concilier tous les efforts sur le continent dans le but de rendre effective l'ambition de sécuriser et d'organiser les échanges électroniques dans le monde des affaires et dans les relations ordinaires.

Qu'en est-il du rôle des organes étatiques?

§2: Le besoin de renforcement du rôle des organes de contrôle étatique

L'article 85 de l'AUDCG est très clair, « la réglementation de l'Organisation pour l'Harmonisation en Afrique du Droit des Affaires, et à défaut, le droit interne des États parties, énonce les contraintes techniques appliquées aux composants de la signature électronique pour que celle-ci soit réputée qualifiée »[126]. Les Etats ont leur rôle à jouer dans cet encadrement des services de confiance et cette normalisation de l'utilisation des moyens de communication électronique. Ainsi il est de leur devoir de mettre en place des Comités nationaux pour assurer l'application des normes mises en place par le Comité central et lorsque le droit OHADA ne

[121] Piette-Coudol, Thierry. *Le numérique au service du droit de l'OHADA et des États parties*. Droits africains. Paris: EJA LGDJ, 2016, p. 80.
[122] AUDCG, Art. 83 « Le Comité technique de normalisation des procédures électroniques prévu à l'article 81 du présent Acte uniforme détermine les critères à remplir pour être un prestataire de services de certification électronique ».
[123] AUDCG, Art. 87.
[124] AUDCG, Art. 96.
[125] Piette-Coudol, Thierry. Le numérique au service du droit de l'OHADA et des États parties. Droits africains. Paris: EJA LGDJ, 2016, p. 80: « l'application des normes techniques communes doit concerner le plus grand nombre d'acteurs possibles, c'est-à-dire, à terme, le continent africain lui-même ».
[126] AUDCG, Art. 85.

prévoit pas de règles pour régir certaines situations, ils ont la possibilité de légiférer dans le sens.

En pratique, plusieurs Etats africains membres de l'OHADA se sont dotés de lois spécifiques avec l'objectif de répondre à l'invitation de l'OHADA. C'est le cas de la Côte d'Ivoire, avec la loi n° 2013-546 du 30 Juillet 2013 relative aux transactions électroniques. De son côté, le Sénégal avait déjà une loi sur les transactions électroniques avant l'invitation de l'OHADA[127]. La loi du Sénégal a été mise en place en 2008 avant la réforme du droit des affaires dans l'OHADA.

Qu'en est-il de l'encadrement de l'activité des prestataires de services de confiance?

Section 2: La nécessité d'encadrer l'activité des prestataires de services de confiance

Pour la mise en œuvre des services de confiance prévue dans le cadre de la modernisation du droit des affaires, il faut recourir à des prestataires de services de confiance. Or, l'AUDCG n'a dédié aucune partie de la réforme du droit des affaires à l'encadrement de l'activité des prestataires de services de confiance **(§1).** De ce fait, il est plus qu'important de proposer des règles qui auront vocation à régir l'activité de ces acteurs importants **(§2).**

§1: L'inexistence d'un encadrement propre à leurs activités

En l'absence de définition en droit OHADA, nous nous inspirerons de celle proposée par le Règlement eIDAS. Le règlement définit le prestataire de service de confiance comme « une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié »[128]. Une distinction est d'ailleurs faite entre les prestataires de services de confiance. Dans la mesure où certains prestataires sont dits « qualifiés » et d'autres non. Ainsi, un prestataire de services de confiance qualifié est « un

[127] LOI n° 2008-08 du 25 janvier 2008 sur les transactions électroniques.
[128] Règlement eIDAS, Art. 3.19.

prestataire de services de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut qualifié »[129].

Dans la pratique, on distingue les prestataires de services de confiance en fonction du service fourni. Ainsi, il existe des prestataires de services de certification électronique, pour les certificats électroniques (identités numériques) et de fourniture des services en matière de signature électronique (PSCE), les prestataires d'Audit de Sécurité des Systèmes d'Informations, chargé de veiller à la sécurité et à l'audit de sécurité des systèmes d'informations et réseaux (PASSI), les prestataires des services d'archivage électronique, chargé d'assurer la dématérialisation et la conservation des archivages électroniques (PSAE)[130].

Comment l'OHADA peut-elle encadrer l'activité de ces prestataires?

§2: La proposition de règles pour l'encadrement de leurs activités

Dans le cadre de la réforme de l'AUDCG, de nouveaux concepts et services ont été introduits dans le monde des affaires. Ainsi, pour la mise en œuvre effective de la modernisation de la vie des affaires dans l'OHADA, tout un livre a été consacré à la dématérialisation. Ce livre contient des règles dispersées faisant référence aux prestataires de services de confiance. Il serait judicieux pour l'OHADA de veiller à rassembler ces règles afin d'en constituer une partie distincte et autonome. Ainsi cette distinction permettra d'établir un régime avec pour vocation l'encadrement des activités des prestataires de service de confiance.

Cette démarche doit s'inscrire dans la volonté de doter le Comité technique de normalisation mis en place de plus de moyens pour mieux assurer ses missions. Grâce à ce cadre, le Comité technique pourra aisément élaborer et mettre en place des normes techniques de qualité et des niveaux de services élevés.

[129] Règlement eIDAS, Art. 3.20.
[130] William KADIO, Enjeux de la Confiance Numérique pour les pays africains SG 13 RG- AFR, Session 5 : Trust and Technology Convergence, ARTCI.

Conclusion

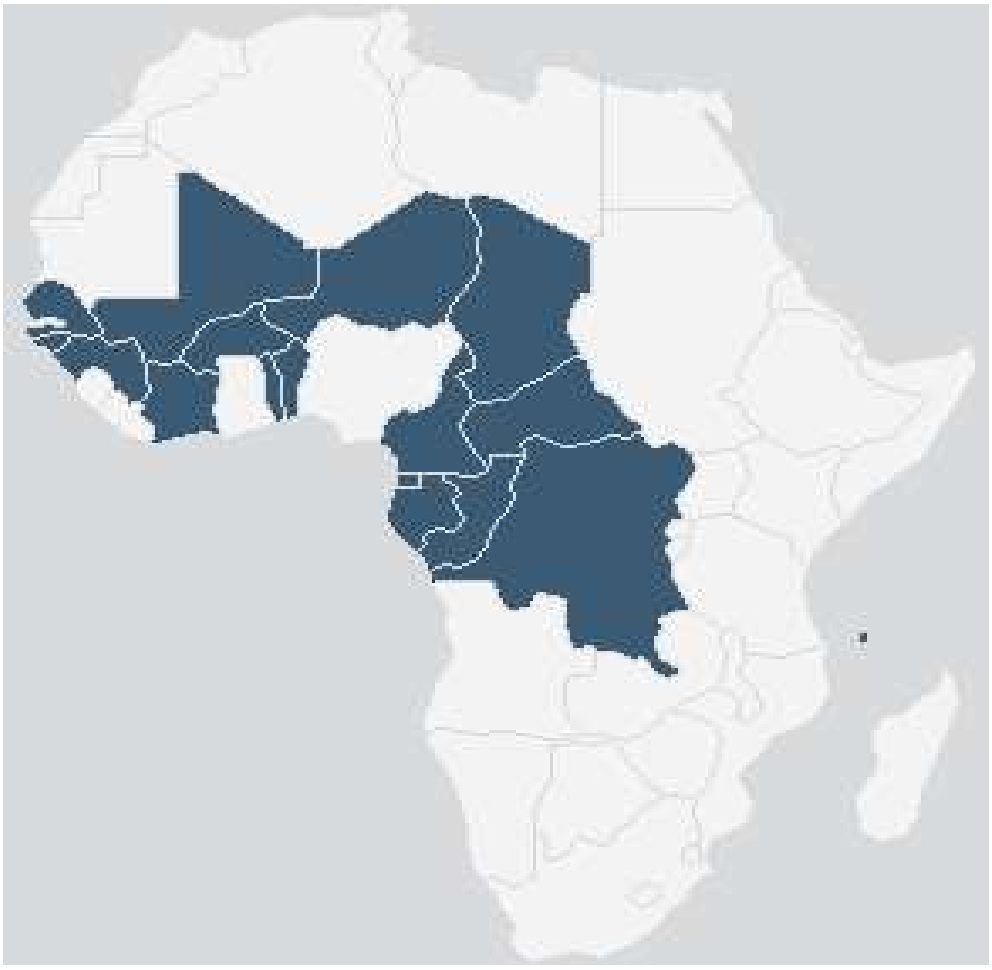
Il ressort en définitive de notre étude que la réforme du droit des affaires dans la zone OHADA a apporté des changements importants. En effet, cette réforme constitue l'acte qui matérialise la volonté profonde de l'organisation, celle de moderniser le droit des affaires dans l'espace OHADA. Ainsi de nombreux moyens ont été mis en place pour accroître la sécurité des opérations et faciliter les échanges entre acteurs commerciaux, mais aussi entre les entreprises et les individus.

Cependant, des efforts restent encore à être accomplis afin d'atteindre les buts visés par l'organisation. En effet, plusieurs zones d'ombres persistent encore dans cet élan de modernisation de la vie des affaires comme la question de l'identité numérique ou encore l'encadrement de plusieurs services de confiance, dans un contexte où l'utilisation des nouvelles technologies dans la vie de tous les jours ne fait croître, notamment la mise en place des transactions mobiles.

En tout état de cause, le droit OHADA a le mérite de ne pas être un droit statique, mais ouvert aux innovations en fonction des mutations sociales. Ainsi plusieurs projets de réformes sont en cours comme le Projet d'Acte Uniforme sur le droit des contrats. Plus précisément, les innovations en matière d'identité numérique et de services de confiance peuvent venir d'un éventuel Acte Uniforme relatif aux transactions électroniques[131], tel qu'annoncé en 2019 par le Secrétaire permanent de l'Organisation.

[131] https://www.ohada.com/actualite/5170/article-un-acte-uniforme-ohada-relatif-aux-transactions-electroniques-se-prepare.html.

Annexe 1 : Carte coloriée de l'OHADA



Source : http://www.droit-afrique.com/pays/ohada/

Commentaire: L'OHADA compte 17 pays de 4 langues différentes

Bibliographie

Ouvrages

Bardin, Michaël. « L'identité numérique et le droit : esquisse d'une conciliation difficile ». *Hermès, La Revue* 80, nº 1 (2018): 283-91. https://doi.org/10.3917/herm.080.0283.

Campion, D. R., J. C. Olson, D. G. Topel, L. L. Christian, et D. L. Kuhlers. « Mitochondrial Traits of Muscle from Stress-Susceptible Pigs ». *Journal of Animal Science* 41, nº 5 (novembre 1975): 1314-17. https://doi.org/10.2527/jas1975.4151314x.

Caprioli, Éric A., *Signature électronique et dématérialisation: droit et pratiques*. Droit & professionnels. Communication et commerce électronique. Paris: LexisNexis, 2014.

Caprioli, Éric A. Agosti, Pascal. Cantero, Isabelle, Choukri, Ilène. L'identité numérique dans le droit et la pratique, Revue Banque Édition, Paris, 2021.

Castets-Renard, Céline. « Personnalité juridique et identification numérique ». In *La personnalité juridique*, édité par Xavier Bioy, 305-17. Travaux de l'IFR. Toulouse: Presses de l'Université Toulouse 1 Capitole, 2018. http://books.openedition.org/putc/3053.

Cissé, Abdoullah. « L'harmonisation du droit des affaires en Afrique : L'expérience de l'OHADA à l'épreuve de sa première décennie ». *Revue internationale de droit économique* t. XVIII, 2, nº 2 (2004): 197-225. https://doi.org/10.3917/ride.182.0197.

Congrès des notaires de France, éd. *Le numérique, l'homme et le droit: accompagner et sécuriser la révolution digitale*. Paris: Association Congrès notaires de France, 2021.

Dalberto, Séverine Awenengo, Richard Banégas, et Armando Cutolo. « Biomaîtriser les identités ? État documentaire et citoyenneté au tournant biométrique ». *Politique africaine* 152, nº 4 (2018): 5-29.

Deharo, Gaëlle. « L'identité numérique dans les procédures judiciaires ». *Les Cahiers du numérique* 7, nº 1 (2011): 87-102.

Desgens-Pasanau, Guillaume. Freyssinet, Éric. L'identité à l'ère numérique. Présaje. Paris: Dalloz, 2009.

Piette-Coudol, Thierry. *Le numérique au service du droit de l'OHADA et des États parties*. Droits africains. Paris: EJA LGDJ, 2016.

William, KADIO KASSY Uriel. « Enjeux de la Confiance Numérique pour les pays africains », s. d., 13.

CNUDCI. OHADA. OIF. Note de concept, Projet de réunion conjointe CNUDCI – OHADA – OIF sur les enjeux et défis de l'économie numérique en Afrique et dans la sphère francophone (en ligne, 11 mai 2021), p. 3.

Ministère de l'Intérieur, Livre blanc Blockchain et Identification Numérique : restitution des ateliers du groupe de travail « blockchain et identité (BCID) », mai 2021.

Le Tourneau, Philippe. Contrat de commerce en ligne : données juridiques. Chapitre 412, Dalloz 2021/22.

Mercadal, Barthélemy. Séminaire international sur « le droit africain et le développement social ». du 30 octobre au 2 novembre 2009.

Notaise, Jacques. Barda, Jean. Dusanter, Olivier. Dictionnaire du multimédia. Audiovisuel. Informatique. Télécommunications, AFNOR, 1995.
Direction des archives de France, Stage technique international des archives, 2009.

Législatifs

Code civil français 2022 annoté, Dalloz, juillet 2020.
Acte uniforme relatif aux contrats de transport de marchandises par route, Yaoundé, Juillet 2003, le 22 mars 2003, Journal Officiel de l'OHADA N° 13 – 31.

RÈGLEMENT (UE) N° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

Loi n° 1.483 du 17 décembre 2019 relative à l'identité numérique, principauté de Monaco.

Arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect », Journal officiel électronique authentifié n° 0180 du 06/08/2015.

Décret n° 2022-676 du 26 avril 2022 autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (SGIN) et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », Journal officiel électronique authentifié n° 0098 du 27/04/2022.
Décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé «Authentification en ligne certifiée sur mobile », abrogé, Journal officiel électronique authentifié n° 0113 du 16/05/2019.
Traité OHADA révisé, Québec, 17 octobre 2008.
Acte Uniforme sur le droit commercial général (AUDCG), 15 décembre 2010, Lomé (Togo).

Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel, Malabo, le 27 juin 2014.
Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL, modifiant le règlement (UE) nº910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique.

Traité CEDEAO révisé, Abuja, 14 Janvier 2006.

Règlement CEMAC, Yaoundé, 20 juin 2008.

Acte additionnel CEMAC, n° 01/13-CEMAC-070 U-CCE S.E du 25 juin 2013.

Revues

Revue critique de droit international privé, Création du marché unique numérique – Rev. crit. DIP 2014. 975.

« Dalloz référence Contrats du numérique | Dalloz ». Consulté le 11 juin 2022. Revue Dalloz.

BIPELE KEMFOUEDIO, Jacques. « La libre circulation des personnes comme droit fondamental en zone CEMAC». La Revue du Centre Michel de L'Hospital [En ligne], 21 | 2020, mis en ligne le 20 septembre 2021, consulté le 10 juin 2022, http://revues-msh.uca.fr/revue-cmh/index.php?id=72.
« Numerical identity in judicial proceedings ». *Les Cahiers du numerique* 7, nº 1 (27 juillet 2011): 87-102.

Ekani, Serge Christian. « Intégration, exequatur et sécurité juridique dans l'espace OHADA. Bilan et perspective d'une avancée contrastée ». *Revue internationale de droit économique* t. XXXI, nº 3 (2017): 55-84. https://doi.org/10.3917/ride.313.0055.

« Revue critique de droit international privé | Dalloz ». Consulté le 11 juin 2022. https://www dalloz-fr.docelec-u paris2.idm.oclc.org/documentation/Document?ctxt=0_YSR0MD1zaGPDqW1hcyBkJ2lkZW50aWZpY2F0aW9uIMOpbGVjdHJvbmlxdWXCp3gkc2Y9c2ltcGxlLXNlYXJjaA%3D%3D&ctxtl=0_cyRwYWdlTnVtPTHCp3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BlPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RlPUZhbHNlwqdzJGJxPcKncyRzZWFyY2hMYWJlbD3Cp3Mkc2VhcmNoQ2xhc3M9wqdzJHo9MERCRkM4REIvNkIxMjFGQ0I%3D&id=REVDIP%2FCHRON%2F2014%2F0098.
Zogo Nkada, Simon-Pierre. « La libre circulation des personnes : réflexions sur l'expérience de la C.E.M.A.C. et de la C.E.D.E.A.O. », Revue internationale de droit économique, vol. xxv, no. 1, 2011.

Thibault Douville. « Enfin un cadre juridique général pour l'identification électronique ! ». Recueil Dalloz, 2018.

LexisNexis. L'ESSENTIEL Droits africains des affaires. RCCM informatisé de l'OHADA, LEDAF, juin 2017, n°06, p. 8.

Cass. 2e civ. 30 avril 2003, n° 00-46.467: JurisData n° 2003-018798.

Articles en ligne

« Le Gabon homologue le passeport biométrique de la Cemac – Le Librevillois – Site d'information ». Consulté le 11 juin 2022. https://www.lelibrevillois.com/2022/05/17/le-gabon-homologue-le-passeport-biometrique-de-la-cemac/.

Www.ohada.com. « Article : Un Acte uniforme OHADA relatif aux transactions électroniques se prépare ». OHADA.com. Consulté le 12 juin 2022.

https://www.ohada.com/actualite/5170/article-un-acte-uniforme-ohada-relatif-aux transactions-electroniques-se-prepare.html.

https://www.cybermalveillance.gouv.fr

Google et la Société Financière Internationale (IFC) de la Banque Mondiale. Rapport e-Conomy Africa 2020. Lagos, Nairobi, Johannesburg, 11 novembre 2020, https://www.ifc.org/wps/wcm/connect/e358c23f-afe3-49c5-a509-034257688580/e-Conomy-Africa-2020.pdf?MOD=AJPERES&CVID=nmuGYF2

Digital Africa. Fonds d'amorçage pour les start-up numériques africaines. https://www.afd.fr/fr/ressources/fonds-damorcage-pour-les-start-numeriques-africaines.

https://www.dgdi.ga/actualites/homologation-du-passeportcemac/#:~:text=Le%20pr%C3%A9sident%20de%20la%20Commission,Guin%C3%A9e%2DEquatoriale%2C%20le%20Thad.