Laboratoire Africain de
Recherches en Cyberstratégie

Enjeux et évolutions du droit dans le cyberespace : Quelle stratégie pour l'Afrique ?

Par DJIMGOU NGAMENI

Avril 2021

Résumé :

Pourtant devenu un outil stratégique pour les Etats et les organisations, le droit relatif au cyberespace est traité de façon partielle et incomplète par les acteurs africains du numérique. Le RGPD en Europe, le Cloud Act des Etats-Unis, ou encore le Manuel de Tallinn, sont des exemples éloquents qui renseignent sur les évolutions et la puissance du droit dans le cyberespace au service de divers intérêts. Afin de faire face à cette nouvelle donne et combler son retard abyssal en la matière, l'Afrique doit s'appuyer sur des sources et référentiels endogènes pour initier une réflexion sur *les fondements d'une théorie africaine du droit dans le cyberespace*, ainsi que sur l'usage des technologies numérique dans la pratique du droit sur le continent.

Introduction

« Numérique et Droit : stratégies de puissance ITIA et Droit dans la cyberguerre » : tel est le titre d'une conférence organisée en Mai 2020 par l'école de guerre économique de Paris, qui résume bien le cœur du sujet dont nous allons traiter ici. Il s'agira d'explorer le rapport dialectique qui existe entre le droit et le cyberespace, et d'en tirer les conséquences pour l'Afrique. Dans ce contexte nous emprunterons la définition du cyberespace proposée par Pierre Lévy, qui selon lui « *désigne l'univers des réseaux numériques comme lieu de rencontres et d'aventures, enjeu de conflits mondiaux, nouvelle frontière économique et culturelle. […] Le cyberespace désigne moins les nouveaux supports de l'information que les modes originaux de création, de navigation dans la connaissance et de relation sociale qu'ils permettent* »[1].

Quant à la notion de droit, nous l'entendons ici comme « *l'ensemble des règles qui régissent la conduite de l'homme en société, les rapports sociaux* »[2]. C'est l'élément régulateur de toute société moderne, et bien souvent le produit d'une vision du monde. Hors comme nous pouvons tous le constater aujourd'hui, le cyberespace à travers les technologies numériques transforme continuellement à peu près tous les secteurs d'activités et tous les aspects de notre vie quotidienne, lesquels sont régis par des règles de droit. On voit ainsi changer nos façons de consommer, de produire, de commercer, d'apprendre, de se défendre, d'accéder à la culture, de socialiser, etc.

Au cours de la conférence évoquée *supra*, le panel d'experts multidisciplinaires (juristes, entrepreneurs, etc.) a constaté et confirmé cette forme d'intrication entre droit et cyberespace, en essayant d'évaluer quelques-unes des implications pour différents acteurs de leur écosystème. Il était question par exemple de voir dans quelle mesure accompagner les startups européennes pour mieux les protéger contre l'extraterritorialité du droit américain dans le cyberespace, ou encore d'aider les pouvoirs publics à construire des propositions pour l'adaptation des normes juridiques européennes et internationales existantes (droit international humanitaire, droit des conflits armés, etc.) dans le cyberespace.

N'ayant moi-même aucune expertise juridique, je ne vais pas ici vous donner des arguments techniques de droit. Je laisse le soin aux juristes africains de prendre la balle au rebond sur ce point. Mon propos sera de relever les différents enjeux observés à partir d'une perspective stratégique, afin de stimuler la conception d'un point de vue africain sur ce sujet capital.

[1] Pierre Lévy, *L'intelligence collective. Pour une anthropologie du cyberespace*, Paris, La Découverte, 1997
[2] Émile Littré, *Dictionnaire de la langue française*, 1863

Les enjeux juridiques du cyberespace pour l'Afrique

Il n'est pourtant pas rare d'entendre parler de cyber-droit ou de droit du cyberespace en Afrique. Certains juristes et universitaires du continent ont d'ailleurs écrit et travaillé sur le sujet, à l'instar du congolais Dr *Kodjo Ndukuma Adjayi* qui en est un spécialiste reconnu (auteur du livre *Cyberdroit, Télécoms, Internet, e-commerce : une contribution au droit congolais*, 2009). De plus, ces dernières années, on voit émerger dans plusieurs universités et grandes écoles des masters en droit du cyberespace africain ou encore en droit du numérique en Afrique (cas de Université Gaston BERGER de Saint-Louis au Sénégal).

Au niveau des Etats africains et organisations régionales ou continentales les regroupant, on assiste là aussi une mise à jour un peu poussive mais progressive du cadre législatif et réglementaire pour prendre en compte les évolutions du numérique et s'arrimer à la société de l'information. Selon l'Indice Mondial de Cybersécurité[3] (rapport de 2018), plusieurs pays mettent en place un ensemble de lois sur la cybersécurité et la lutte contre la cybercriminalité, la protection des données personnelles et la protection de l'enfance en ligne, l'encadrement du commerce en ligne, etc. La convention de l'Union africaine en la matière[4], adoptée à Malabo en 2014, marque aussi une étape importante dans cette démarche (même si elle n'est pas encore signée et ratifiée par la plupart des Etats).

Cependant, à l'analyse, cette question de droit relatif au cyberespace est traitée de façon partielle et incomplète aussi bien par nos universitaires, dans les programmes d'enseignement, que par le gouvernement eux-mêmes, et ce à mon avis pour une raison très précise : c'est qu'en Afrique, nous n'avons mené aucune étude rigoureuse sur le cyberespace, entendu ici comme objet scientifique en soit. Nous focalisons complètement notre attention sur l'étude, la compréhension et la tentative de régulation des technologies numériques et leurs usages. Et ce faisant, nous ne considérons pas le cyberespace dans sa globalité et dans toute sa complexité, créant ainsi des angles morts dans le raisonnement qui nous empêche d'appréhender tous les enjeux et par conséquent, toutes les implications du droit.

Ainsi, les notions de souveraineté numérique, de conflictualité et rapports de force dans le cyberespace, de territorialité et de frontière, de représentation symbolique et idéologique etc., ne font malheureusement pas partie de notre grille de lecture lorsque nous abordons cette question. Pourtant, vu sous cet angle, on pourrait aisément deviner les implications juridiques et stratégiques qui en découlent. Ce manque de rigueur dans le traitement des questions relatives au cyberespace a de mon point de vue d'énormes conséquences, dont on ne commencera à mesurer l'étendu qu'une fois qu'on s'y mettra vraiment.

A la différence du reste du monde, l'Afrique ne considère pas encore le cyberespace comme un « milieu stratégique » au même titre que le ciel, l'air, la mer et l'espace extra-atmosphérique,

[3] Le GCI (*Global Cybersecurity Index*) est un baromètre de l'Union Internationale des Télécommunications (UIT), qui évalue régulièrement les avancements dans la mise en place des dispositifs de cybersécurité par chaque pays.

[4] Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, adoptée à Malabo en 2014.

avec toutes les considérations que cela suppose. La particularité de ce nouveau milieu est qu'il est anthropogène (créée de toute pièce par l'Homme), alors même que les autres sont des milieux naturels, et donc fondamentalement soumis aux lois de la nature. Le fonctionnement du cyberespace n'est donc régi que par des lois de son créateur, l'Homme. Ce qui pose plusieurs problèmes ! Par exemple, qui exactement a créé les lois actuelles ? Comment se déclinent-elles concrètement ? Comment évoluent-elles ? Qui décident de quand elles doivent évoluer ? De plus, si c'est un milieu stratégique cela suppose que chaque pays puisse en contrôler une partie ? Dans ce cas, comment se défini et se matérialise ses frontières et sa souveraineté ? Autant de questions qu'à défaut d'avoir trouvé les réponses, les africains ne se posent même pas !

La production des normes technologiques (évolution de l'architecture du réseau, protocoles de communication, etc.), la gouvernance mondiale de l'Internet, l'adaptation et l'application du droit international humanitaire au cyberespace, la classification et la régulation internationale des cyberarmes, les conditions générales d'utilisation des applications et des algorithmes, voilà autant de questions auxquelles des nouvelles filières comme l'intelligence juridique[5] ou encore le droit du numérique tentent d'apporter des réponses, en s'appuyant sur le paradigme occidental, donc au service de ses intérêts. L'irruption des technologies numériques dans la pratique du droit (*LegalTech*[6]) est en train de produire tout un écosystème, avec de plus en plus de startups qui conçoivent des algorithmes agissant comme assistant juridique, et même permettant l'automatisation de certaines procédures grâce à l'intelligence artificielle (au point où commence à émerger des notions telles que le « droit prédictif »).

Le RGPD (*Règlement Général pour la Protection des Données*) en Europe, le *Cloud Act*[7] des Etats-Unis, ou encore le Manuel de Tallinn,[8]sont des exemples éloquents qui renseignent sur la puissance du droit dans le cyberespace au service de divers intérêts des états (économiques, géopolitique, social, etc.). Ce sont des dispositifs qui font émerger la notion « *d'extraterritorialité du droit* » dans le cyberespace, avec des modes opératoires différents, créant de fait des rapports de force entre puissances.

En effet, pendant que le *Cloud Act* s'inscrit dans une logique de conquête (imposé aux acteurs par la puissance américaine), le RGDP est plutôt présenté et perçu comme un outil de protection. C'est une approche qui rend cette réglementation européenne attractive au point d'être copiée par plusieurs pays en dehors de l'Europe, y compris par environ 25 pays africains. Le travail d'encerclement cognitif autour de ce règlement a été si efficace qu'il devient même suspect

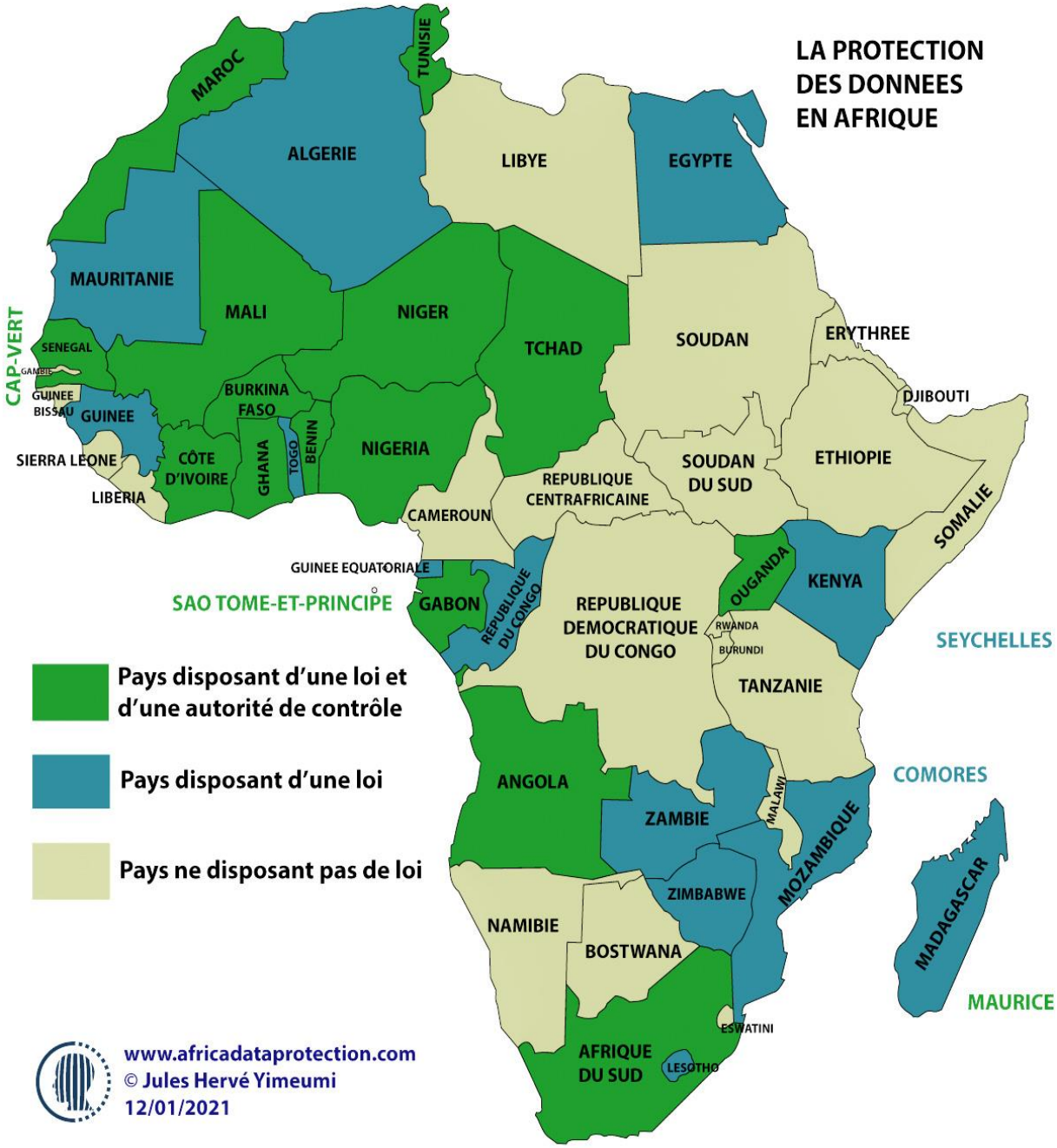
[5] « *L'Intelligence Juridique est définie, à partir de la définition proposée par le professeur Bertrand Warusfel, comme l'ensemble des méthodes, des moyens et des techniques permettant à un acteur - privé ou public - de connaître l'environnement juridique dont il est tributaire pour l'intégrer dans sa stratégie, d'en identifier et d'en anticiper les opportunités et les risques, d'agir sur son évolution et de disposer des informations nécessaires pour pouvoir mettre en œuvre les instruments juridiques et les solutions opérationnelles aptes à réaliser ses objectifs stratégiques et à se préserver* ». Véronique Chapuis

[6] Une *LegalTech* est une expression issue de l'union entre "Légal" et "Technology". D'après l'observatoire français des *LegalTech*, c'est défini comme une entreprise proposant des services juridiques à l'aide des nouvelles technologies.

[7] Le *Clarifying Lawful Overseas Use of Data Act* ou *CLOUD Act* (H.R. 4943) est une loi fédérale des États-Unis adoptée en 2018 sur la surveillance des données personnelles, notamment dans le Cloud.

[8] Le *Manuel de Tallinn* est un guide rédigé par un groupe d'experts mandatés par l'OTAN, qui propose une transposition du droit international aux cyberconflits.

pour un pays de ne pas avoir une loi similaire. On est quand même en droit de se poser la question si c'est ce dont nous avons besoin dans le contexte africain, quand on sait que les données représentent la matière première de l'économie du 21ème siècle, et qu'un règlement qui tend à limiter la collecte et l'exploitation de ces données peut avoir un impact plutôt négatif sur la croissance qu'on est en droit d'attendre de l'économie numérique en Afrique. C'est un sujet à examiner de près.



Source: Africa Data Protection

Les évolutions du droit international dans le cyberespace

Afin de mettre en perspective concrètement les enjeux évoqués *supra* avec les évolutions du droit international dans le cyberespace, je vous renvoie à la lecture du document "Trends in international law for cyberspace". Il s'agit d'une étude menée par plusieurs experts en droit, du centre de recherche en cyberdéfense affilié à l'OTAN (*CCDCOE : Cooperative Cyber Defence Centre of Excellence*), qui répertorie en sept points les dernières tendances du droit international relatif au cyberespace, et envisage leurs évolutions au cours des prochaines années. Explorons quelques-unes des observations parmi les sept relevées par ces chercheurs dans leur étude. D'après eux :

- Un consensus sur l'application du droit international dans le cyberespace se développe progressivement, mais le débat sur la manière dont certaines règles doivent s'appliquer se poursuit, notamment avec un "front de résistance" constitué par les Etats tels que l'Iran, la Russie, ou encore la Chine (qui ont une différence conceptuelle avec l'occident autour des notions de *cybersécurité* et de *sécurité de l'information*). En l'occurrence, certaines règles telles que l'interdiction d'intervention (règles 66 à 67 du *MT 2.0*[9]) et le droit de légitime défense (règles 71 à 75 du *MT 2.0*) sont généralement acceptées. D'autres, en particulier l'exercice de la souveraineté territoriale (règles 1 à 5 du *MT 2.0*) et le devoir de diligence (règles 6 à 7 du MT 2.0) dans le cyberespace continuent de susciter des réactions mitigées quant à leur portée et à leur contenu.

- Les États affichent leur volonté de riposter en cas de cyberagressions en se donnant les moyens techniques de les attribuer aux commanditaires, afin d'y apporter la réponse la plus adaptée. Ainsi, les normes juridiques en matière d'attribution deviennent plus claires, l'attribution étant comprise comme une décision politique étayée par des faits établis (par des moyens techniques et de renseignement) dans leur ensemble. Bien qu'il n'y ait pas d'obligation légale de publier des preuves à l'appui de l'attribution, les États le font avec des niveaux de détail de plus en plus élevés. Étant donné que les cyber-opérations parrainées par les États restent généralement sous le seuil des attaques armées bien que considérées comme une violation du droit international, les États continuent de chercher les contre-mesures efficaces (dénonciation publique et sanctions financières, riposte collective, etc.). Cependant, il existe un consensus sur le fait qu'une cyber-opération d'une gravité et de conséquences données peut constituer une attaque armée déclenchant le droit à la légitime défense (*jus ad*). Dans une telle situation, les États sont libres de choisir les moyens appropriés pour réagir, dans les limites du droit international, en ne se limitant pas aux moyens électroniques.

[9] *MT 2.0* fait référence à la version 2 du Manuel de Tallinn parue en 2017.

- Plusieurs entités (États, organisations internationales, secteur privé) développent aujourd'hui une série d'initiatives visant à promouvoir des normes internationales non contraignantes en matière de comportement responsable, en vue de maintenir la sécurité et la stabilité dans le cyberespace. On peut citer par exemple *l'appel de Paris pour la confiance et la sécurité dans le cyberespace* porté par la France depuis 2018, ou encore la « *Convention de Genève numérique* » proposée par le géant Microsoft. Cependant, l'impact concret reste à démontrer, notamment au regard de la disparité de contenu entre les propositions des acteurs qui, bien que partageant la nécessité de créer les normes pour le cyberespace, ont des idées très différentes quant à l'état final souhaité et les moyens d'y parvenir.

- La plupart des pays considèrent désormais que l'outil cyber fait partie intégrante de leur arsenal militaire, et exigent des réponses opérationnelles pratiques pour la conduite licite d'activités spécifiques (dans le cas des conflits armés ou des opérations de maintien de la paix, par exemple). Cependant, considérer le cyberespace comme théâtre d'opération militaire soulève des questions juridiques concernant par exemple la conduite des activités de cyber-renseignement, les limites de la souveraineté des États, les doctrines des pays pour les cyber-opérations offensives, le seuil d'attaque armée déclenchant le droit à la légitime défense et la manière d'appliquer les règles du *droit international humanitaire*.

En résumé, dans une démarche prospective, cette étude prévoit des évolutions importantes quant à l'application du droit et des normes juridiques dans le cyberespace dans un horizon de cinq ans. D'après les auteurs, la tendance est à la clarification et à l'acceptabilité progressive par les Etats de la manière dont le droit international va s'appliquer dans le cyberespace (même s'ils ne prévoient pas un traité mondial avec des normes contraignantes à l'horizon choisi). La tendance est également à la montée en puissance de certaines technologies qu'il faudra réguler (Intelligence Artificielle, réalité augmentée, Internet des Objets, etc.).

De plus, l'opposition entre deux modèles conceptuelles (*cybersécurité* vs *sécurité de l'information)* se poursuivra vraisemblablement, car les pays tels que la Russie, la Chine ou encore l'Iran vont continuer à considérer « l'espace informationnel » comme un moyen d'exercer un contrôle sur l'usage et le contenu, alors que les démocraties occidentales se concentrent sur la sécurité technique et le libre exercice des droits fondamentaux en ligne de la même manière que hors ligne.

Les conséquences sont, d'après l'étude, qu'on aura de plus en plus de cyber-opérations parrainées par les États, une évolution dans les réponses des Etats face à ces cyber-opérations jugées hostiles, une tendance à la balkanisation du cyberespace par les Etats qui souhaitent en contrôler leur petit bout sur lequel transposer et exercer leur souveraineté, etc. Vous l'aurez compris, les chantiers du droit et des normes juridiques dans le cyberespace sont nombreux et

le resteront pour les années à venir. De plus, les centres de recherches dans la plupart des pays sont à pied d'œuvre pour être les architectes des évolutions à venir (ou au moins les influencer).

Quelles Leçons pour l'Afrique ?

Du propre aveu des auteurs de cette étude, il ne s'agit pas d'un catalogue complet des tendances, et les thèmes traités ne sont pas présentés dans un ordre particulier. Cependant, ces derniers ont fait une mise en garde qu'il me semble pertinent de relever ici. *« (…) bien que nous ayons déployé tous les efforts possibles pour décrire les évolutions juridiques pertinentes au niveau mondial,* disent-ils, *nous reconnaissons que la liste découle d'une perspective géopolitique euro-atlantique et que la division entre évolutions politiques et tendances du droit n'est pas toujours nette ».*

Cette précision est tout à fait fondamentale si nous souhaitons engager une réflexion sur le regard et la contribution africaine en matière de droit du cyberespace, car elle rappelle le caractère engagé du droit qui aujourd'hui se met au service des intérêts idéologique, économique, et même géopolitique. La Chine et la Russie par exemple, qui militent au niveau international pour que chaque pays puisse appliquer des restrictions de liberté dans son espace informationnel si nécessaire, ont réussi par ailleurs à bloquer en 2017 le projet d'un groupe d'experts gouvernementaux de l'ONU, qui portait sur la transposition du droit international humanitaire dans le cyberespace. D'après ces deux cyberpuissance, cela aurait conduit à perpétuer l'hégémonie de la culture occidentale du droit dans l'univers numérique (ce qui est déjà le cas aujourd'hui avec la prédominance étatsunienne). Et l'Afrique dans tout ça ?

A la lumière de ces enjeux hautement stratégiques et des implications juridiques évidentes, j'invite les experts africains du droit à se pencher sérieusement sur le sujet. Car comme le montre l'étude ci-dessus, la bataille juridique pour le contrôle de l'espace cybernétique bat son plein en ce moment même, et chaque puissance essaye de manier avec habileté sa propre conception du droit pour améliorer son positionnement. A l'heure actuelle, les pays africains sont malheureusement absents de ce champ de bataille alors même que cette étude laisse transparaître à quel point le droit est un instrument majeur dans la définition d'une souveraineté numérique, et que les tendances indiquent que le champ est encore ouvert pour proposer de nouvelle façon d'approcher cette question.

Les africains devront donc être en mesure de formuler leurs propres réponses aux questions que nous venons d'explorer. N'existe-t-il pas des sources africaines de droit à partir desquelles nous pouvons articuler nos propres normes et règlements qui traduisent notre vision du monde dans le cyberespace ? Des livres tels que *Les Origines Égyptiennes Du Droit Civil Romain* d'Eugène Revillout [2013] ou encore *La théorie du droit en Afrique* de Mbog Bassong [2016] par exemple ne pourraient-ils pas servir de référentiel en la matière ? J'ai la conviction que nous avons de quoi faire !

Prenons le cas de l'introduction des solutions numériques dans la pratique actuelle du droit en Afrique. Au regard du potentiel économique que représente ce marché (ne serait-ce que par la digitalisation et l'automatisation des pratiques les plus courantes du droit OHADA), des acteurs commencent à se positionner pour structurer le secteur. On a par exemple vu naître des initiatives telles que *Legal Tech Africa* (qui se positionne comme « *programme d'accompagnement juridique des écosystèmes entrepreneuriaux en Afrique* »), ou encore *The African Law & Tech Network* (positionné comme « *une communauté en ligne à l'intersection de la technologie et des services juridiques en Afrique* »). Aussi louables qu'elles puissent sembler aujourd'hui, ces initiatives sont en réalité des excroissances des projets occidentaux qui souhaitent investir et contrôler ce marché en Afrique, bien entendu sur la base de leurs propres normes juridiques (droit continental et *common law*) qui sont de toute façon actuellement dominantes sur le continent. C'est notamment le cas de l'initiative *The African Law & Tech Network*, qui est le démembrement du projet anglais Hook Tangaza visant à couvrir toute l'Afrique anglophone.

A ce titre, afin de planter le décor de cette réflexion à laquelle je convie les juristes du continent et portant sur *les fondements d'une théorie africaine du droit dans le cyberespace* ainsi que sur l'usage des technologies numérique dans la pratique du droit en Afrique, je vous laisse avec cette assertion inspirante du savant Mbog Bassong :

« *Nous sommes persuadés de la pertinence de Maât, la norme juridique africaine inférée de l'ordre de l'Univers et confrontée, depuis près de cinq siècles, à un droit positif qui ignore l'histoire et la culture des nations de Kemet. Si dans la pensée occidentale, le législateur, le juriste et le prince sont garants de la production du sens, du contrôle et de l'application du droit, il n'en va pas de même pour le droit africain qui nie ce point de départ pour s'en tenir à l'Ordre de l'Univers, Maât (Egypte), ...saisi comme l'objet (l'objectif) de droit, le référent extérieur au droit lui-même et à la réalité sociale, du moins dès le départ. Le droit africain fonde ainsi une autre manière de faire la science qui dépasse le cadre de la pensée complexe d'Edgar Morin. Aussi n'est-il pas exagéré de dire que le droit positif n'est rien d'autre qu'une forme de droit et non la science du droit, en raison de l'identité opérée entre l'objet (l'objectif, la science) et le sujet (le subjectif, le juriste) qui produit le droit sur la base du paradigme juridique cartésien, sans référence à un objet qui lui est extérieur* »[10].

[10] Extrait de *La théorie du droit en Afrique,* Mbog Bassong [2016]

A propos de l'Auteur :

DJIMGOU NAGMENI est Entrepreneur, Conférencier, Consultant international en cybersécurité / cyberdéfense, Enseignant à l'École Politique Africaine de Paris, Spécialiste de cyberstratégie et Fondateur du LARC.

A propos du LARC :

Le LARC (Laboratoire Africain de Recherches en Cyberstratégie) est un cadre de réflexion créé par votre serviteur et regroupant des chercheurs pluridisciplinaires, avec pour mission de décrypter, d'analyser et d'anticiper les enjeux de demain dans le cyberespace africain.

Pour soutenir les activités du LARC ou y contribuer par vos propres publications, visitez notre site web : https://www.larc.africa

Pour citer cet article :

DJIMGOU NGAMENI, « Enjeux et évolutions du droit dans le cyberespace : Quelle stratégie pour l'Afrique ? », Note N°04 - LARC, Avril 2021.