Les mutations du cadre juridique africain de protection des droits de l'homme face aux TIC : L'avènement de la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel du 27 juin 2014

Martial JEUGUE DOUNGUE
Docteur en droit international

Citation de l'article : M. Jeugue Doungue « Les mutations du cadre juridique africain de protection des droits de l'homme face aux TIC : L'avènement de la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel du 27 juin 2014 », Ouvrage Commun, Droits en mutation 2017, Collection Doc Publication, Les Editions de l'Immatériel, 2017, pp. xx-xx.

Chapeau

Les Etats africains souhaitent mettre en place des politiques d'innovation pour rénover leur cadre juridique et institutionnel, notamment en matière de lutte contre la cybercriminalité, avec comme objectif l'émergence d'un environnement juridique favorisant la confiance et le respect mutuel. La Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel de juin 2014 s'inscrit dans cette stratégie encourageant un usage des nouvelles technologies de l'information et de la communication compatible avec la protection des droits de l'homme.

Abstract

African states have the will to introduce innovative policies to renovate their legal and institutional framework, particularly to tackle cybercrime, with the aim of creating a legal environment that fosters both confidence and mutual respect. The African Union Convention on Cybersecurity and Personal Data Protection of June 2014 is a key element of this strategy encouraging the use of new technologies compatible with the protection of human rights.

Article

Dans un monde marqué par la globalisation des risques, des crimes et des menaces sur la cybersécurité[i], une fracture menace l'Afrique dans ce domaine, puisque l'absence de maîtrise du risque sécuritaire accroit la dépendance technologique des individus, des organisations et des États aux systèmes d'information et aux réseaux. Or, ces infrastructures sont de nature à permettre le contrôle de leurs besoins et des moyens de sécurité des technologies de l'information ou de communication (TIC)[ii]. Force est donc de constater que la plupart des Etats ne disposent pas des outils intégrant des moyens suffisants et nécessaires à la réalisation ou à la garantie d'un niveau minimal de sécurité, comme ils ne disposent pas des ressources humaines aptes à concevoir et à créer un cadre juridique de confiance.

Les systèmes informatiques mis en réseau sont des ressources accessibles à distance. Ils deviennent à ce titre des cibles potentielles des cyber attaques qui portent atteintes à la capacité à traiter, sauvegarder, communiquer le capital informationnel, aux valeurs immatérielles et aux symboles, aux processus de production ou de décision de ceux qui les possèdent. De tels agissements ont des conséquences sur la sécurité et la pérennité des États et des organisations non gouvernementales. Ces risques par leur gravité impliquent la mise en place d'une stratégie de défense active en profondeur, combinant protection intrinsèque des systèmes, surveillance permanente, réaction rapide et action offensive, imposant une

forte impulsion gouvernementale, associé à un changement des mentalités encore appelée cybersécurité[iii].

Dans cette perspective, la cybersécurité pourrait être définie comme l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations ou des utilisateurs[iv]. Ces actifs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement[v].

Les États africains soucieux d'acquérir de stratégies innovantes de politique criminelle combinant les réponses étatiques, sociétales et techniques, susceptibles de créer un environnement juridique de confiance[vi] pour la cybersécurité envisagent de se doter d'instruments juridiques répondant à ces critères. La Convention de l'Union Africaine (UA) sur la cybersécurité et la protection des données à caractère personnel du 27 juin 2014 représente l'un des axes structurants de cette politique menée conjointement par les États africains. Conscients des menaces engendrées par le phénomène de la cybercriminalité[vii], les Chefs d'État et de gouvernement de l'UA, réunis en juin 2014 à Malabo en Guinée Équatoriale, pour la 23ème session ordinaire du Sommet de l'UA, ont adopté, à l'instar du Conseil de l'Europe, ce texte fondateur.

Quels sont les objectifs de cette Convention ? Comment participe-t-elle à l'appropriation des valeurs universelles au rythme des réalités « culturelles » africaines en matière de TICs, et de l'émergence de nouvelles formes de criminalités ?

Ces questions revêtent aujourd'hui un intérêt tout particulier. En Afrique, sans doute plus que partout ailleurs, il devient impératif de doter les individus, les organisations, et les Etats de mesures, de procédures et d'outils qui autorisent une meilleure gestion des risques technologiques, informationnels et juridiques. Les enjeux de la maîtrise de ces risques sont si importants, qu'ils se doivent d'être appréhendés de manière globale, c'est-à-dire au niveau international, régional et national[viii], en intégrant dans la démarche sécuritaire l'ensemble des États membres de l'UA et ce, dans le respect des droits fondamentaux des personnes et des États.

Aborder l'essence de cette problématique supposerait, d'abord, de considérer la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel comme un moyen de construction d'un cadre normatif africain de protection des droits de l'homme face aux TIC. Ensuite et surtout, il serait nécessaire d'envisager cet accord structurant comme une garantie de protection spécifique des données personnelles et de la vie privée, objectif majeur de protection des droits de l'homme et des peuples.

Une telle analyse est ici hors de propos. Néanmoins, quelques idées peuvent être esquissées comme autant d'invitations à poursuivre à la fois la réflexion mais aussi l'action, dans une matière encore en devenir.

Commençons par un constat. L'édification d'une société de l'information inclusive et au service du développement requiert l'existence d'un environnement propice. La confiance et la sécurité comptent parmi l'un des principaux piliers de cet environnement, et sont notamment indispensables à la nouvelle économie du savoir.

Pour l'instauration de cet écosystème, il a été demandé aux pouvoirs publics et au secteur privé de coopérer, afin de prévenir et détecter la cybercriminalité et l'utilisation abusive des technologies de l'information et de la communication et y remédier. De cette coopération a émergé la définition de lignes directrices qui tiennent compte des efforts en cours dans ces domaines, en envisageant une législation qui autorise des investigations efficaces et des poursuites en cas d'utilisation illicite. Ce processus a été instauré en encourageant les efforts d'assistance mutuelle et en renforçant l'appui institutionnel sur le

plan international, toujours avec comme objectif de prévenir et de détecter d'éventuels incidents technologiques et d'y remédier, tout en encourageant l'éducation et la sensibilisation en matière de TICs.

Dans ce contexte, la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel consacre la volonté des États africains de protéger les droits de l'homme dans le cadre de l'usage et de la promotion[ix] des TIC. Il s'agit indéniablement d'une avancée majeure, mais aussi nécessaire, tant les applications qui en sont faites très souvent échappent aux différents acteurs de cet usage[x]. Cependant, une question importante demeure, celle de l'intégration des dispositions qu'elle contient au sein des États et de la large communication sur les enjeux de l'opérationnalisation de la cybersécurité[xi].

---

[i] L. COSTES, « Vers une nouvelle société de l'information », Lamy droit de l'informatique et des réseaux, Bull. actualité, J. Février 1996, n°78, p. 1.

[ii] Voir C. ANTONELLI, « Economie des réseaux : variété et complémentarité », in *Economie industrielle et économie spatiale*, Paris : Economica, 1995, p. 38 et s.

[iii] Voir A. BA, *Internet, cyberespace et usages en Afrique, l'Harmattan*, 2003, p. 11 et s.

[iv] Myriam QUEMENER, Jean-Paul PINTE, Cybersécurité des acteurs économiques : Risques, réponses stratégiques et juridiques, Hermès Science Publications, coll. « Cyberconflits et cybercriminalité », 13 décembre 2012, 274 p ; Myriam QUEMENER et J. FERRY, *Cybercriminalité*. Défi mondial, 2e édition, *Economica*, 2009.

[v] A. DUFOUR, *Internet, « Que sais-je ? »*, 8e édition, Paris, 2000.

[vi] Une récente étude menée par le Centre de Recherches pour le Développement International (CRDI) sous la coordination de M. le professeur Abdoullah CISSE montre l'existence réelle de la cybercriminalité en Afrique.

[vii] En ce sens, M. QUEMENER et Y. CHERPENEL, C*ybercriminalit*é, Droit pénal appliqué, Economica, Paris, 2010, n° 27, p. 7 ; J. J. BOGUI, « La cybercriminalité, menace pour le développement. Les escroqueries internet en Côte d'Ivoire », *Afrique Contemporaine*, 2010/2 n°234, p. 155 – 170 ; 5. Mohamed CHAWKI, *Combattre la cybercriminalité*, Editions de Saint-Amans, 15 mai 2009, 458 p ; Myriam QUEMENER, Joël FERRY, *Cybercriminalité : Défi mondial et réponses,* 2ème éd., Perpignan : Economica, 9 mars 2009, 308 p.

[viii] E. FREYSSINET, *La cybercriminalité en mouvement*, Hermes Science Publications, coll. « Management et informatique », 27 septembre 2012, 240 p.

[ix] Voir Martial Sylvain Marie ABEGA ELOUNDOU, Intégration des technologies de l'information et de la communication dans le secteur artisanal au Cameroun, Mémoire de Master II professionnel, mention Sciences de l'Information et de la Communication, 2007, Université Paris X Nanterre, 164 p.

[x] Les perspectives ouvertes par la généralisation et le perfectionnement des techniques informatiques sont également dangereuses. Le fichage, même manuel des données, est ainsi à l'origine de ce danger. Cette inquiétude est en particulier liée à une possible utilisation abusive de certaines informations personnelles à caractère confidentiel enregistrées électroniquement. Ces informations, qui en elles-mêmes peuvent apparaître inoffensives, peuvent être mises en corrélation avec d'autres informations moins anodines et en définitive nuire aux intérêts des personnes concernées ; le danger pouvant venir aussi bien des collectivités publiques que des groupes privés. Qu'il soit question d'écoutes téléphoniques ou encore de l'informatisation de données personnelles de tous types (administratives, fiscales, financières, mais aussi médicales et incluant les données génétiques), la question du respect des libertés de la personne se pose. Le danger principal provient en fait de la centralisation et du recoupement de données nominatives concernant l'individu. Ils aboutissent à un véritable « encerclement » mettant en cause la liberté de l'individu sous tous ses aspects. En 1950, les possibilités technologiques qui aujourd'hui sont communément utilisées n'étaient pas connues. Toutefois, les enjeux et risques liées aux NTIC ne doivent pas faire oublier les perspectives qu'elles présentent notamment en termes de développement des pays du sud.

[xi] Notons également la question de la preuve électronique et de l'adaptation de la Convention à la rapidité de l'évolution des TIC et autres formes de violations dans le cyberespace. Avec la transition de la téléphonie traditionnelle vers la téléphonie sur Internet, les services de répression seront aussi confrontés à de nouveaux problèmes. Par ailleurs, de nouveaux appareils mettant en jeu des technologies réseaux voient régulièrement le jour et sont rapidement adoptés.