CONVENTION DE L'UNION AFRICIANE SUR LA CYBERSÉCURITÉ ET LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Résumé

Le projet de convention est la traduction d'une résolution de la dernière Conférence des Chefs d'États et de gouvernement de l'UA et vise l'harmonisation des cyber législations africaines dans les domaines de l'organisation du commerce électronique, la protection des données à caractère personnel, la promotion de la cybersécurité et la lutte contre la cybercriminalité. Dans le respect des principes de l'Initiative Africaine de la Société de l'Information [AISI] et du Plan d'Action Régional Africain pour l'Économie du Savoir (PARAESJ, le projet de convention vise à la fois à définir les objectifs et les grandes orientations de la société de l'Information en Afrique et à renforcer les législations actuelles des États membres et des Communautés Économiques Régionales (CER] en matière de Technologies de l'information et de la Communication. Le projet de convention détermine les règles de sécurité essentielles à la mise en place d'un espace numérique de confiance en réponse aux principaux obstacles au développement des transactions numériques en Afrique qui sont liés à des problèmes de sécurité. Il pose les bases d'une cyberéthique à l'échelle de l'Union Africaine en énonçant des principes fondamentaux dans les principaux domaines de la cybersécurité. Il détermine également les bases du commerce électronique, met en place un dispositif permettant de lutter contre les atteintes à la vie privée susceptibles d'être engendrées par la collecte, le traitement, la transmission, le stockage et l'usage des données à caractère personnel et fixe les grandes orientations de l'incrimination et de la répression de la cybercriminalité.

Son adoption va permettre, en capitalisant les expériences africaines et internationales en matière de cyber législation, d'accélérer les réformes dans les États et les CERs africains.

Cadre conceptuel

Partant d'une relecture de l'environnement juridique et institutionnel des régions de l'Union Africaine, l'objectif de la présente convention est de proposer l'adoption à l'échelle de l'Union Africaine, d'une convention sur la mise en place d'un cadre de confiance pour la cybersécurité en Afrique à travers l'organisation des transactions électroniques, la protection des données à caractère personnel, la promotion de la cybersécurité, la gouvernance électronique et la lutte contre la cybercriminalité.

1. **Contexte**

Dans un monde marqué par la globalisation des risques, des crimes et des atteintes à la cybersécurité, l'Afrique est menacée par la fracture sécuritaire qui, en raison du risque sécuritaire non maîtrisé, accroit la dépendance technologique des individus, des organisations et des États aux systèmes informatiques et aux réseaux qui contrôleraient leurs besoins et moyens de sécurité des technologies de l'information.

Les États africains ont un réel besoin de stratégies innovantes de politique criminelle combinant les réponses étatiques, sociétales et techniques pour créer un environnement juridique de confiance pour la cybersécurité.

Toutefois force est de constater que la plupart des États ne disposent pas des outils de communication intégrant des moyens suffisants et nécessaires à la réalisation ou à la garantie d'un niveau minimal de sécurité ni les 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 et deviennent des cibles potentielles des cyberattaques 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 avec des conséquences sur la sécurité et la pérennité des États et des organisations.

Aujourd'hui il devient urgent en Afrique plus que partout ailleurs de mettre à la disposition des individus, des organisations, ainsi que des États des mesures, procédures et outils qui autorisent une meilleure gestion des risques technologique, informationnel et juridique. Les enjeux de la maîtrise des risques technologiques sont importants et sont à appréhender de manière globale au niveau international en intégrant dans la démarche sécuritaire l'ensemble des États membres de l'Union et ce, dans le respect des droits fondamentaux des personnes et des États.

Des efforts certains de protection juridique (nationale, communautaire et internationale) sont notés. Ainsi la CEA a initié un important projet d'harmonisation en coopération avec les autorités de l'UEMOA et de la CEDEAO. Les autres Communautés Économiques Régionales s'inscrivent dans la même dynamique au moment où des États adoptent de plus en plus des législations sur la cybersécurité et les TIC en général. L'UIT a également produit un guide sur la cybersécurité à l'attention des pays en développement.

La présente convention prolonge et renforce cette dynamique et permet un saut qualitatif important en donnant corps à la volonté politique.

2. Enjeux et défis

La cybersécurité soulève des enjeux à la fois multiples et complexes à l'aune desquels se mesure l'ampleur des défis.

La pluralité des enjeux est telle qu'elle dicte la prise en compte de ses multiples dimensions, scientifique, technologique, économique et financière, politique et socioculturelle.

L'interaction entre ces dimensions renforce la complexité de la cybersécurité qui se manifeste à plusieurs niveaux :

- La sécurité informationnelle touche à la sécurité du **patrimoine numérique et culturel** des individus, des organisations et des nations ;
- La vulnérabilité dans le fonctionnement normal des Institutions peut compromettre la **pérennité et la souveraineté des États** ;
- La prise en charge de la cybersécurité requiert une **volonté politique** clairvoyante pour définir et réaliser une stratégie de développement des infrastructures et services du numérique (e-services), et de l'articuler avec une stratégie pluridisciplinaire de la cybersécurité cohérente, efficace et contrôlable.

Les principaux défis qui interpellent les États de l'Union Africaine consistent principalement dans la nécessité :

- D'obtenir un niveau de **sécurité technologique** suffisant pour prévenir et maîtriser les risques technologique et informationnel ;
- D'édifier une société de l'information respectueuse des **valeurs**, protectrice des **droits et libertés**, garantissant la sécurité des biens des personnes, des organisations et des nations ;
- De contribuer à l'économie du savoir en garantissant un accès égal à l'information, en stimulant la création de **savoirs conformes** ;
- De créer un environnement de confiance qui soit :
    - **Prévisible** en termes de prévention et règlements des différends et évolutif parce que tenant compte de l'évolution technologique continue ;
    - **Organisé** en couvrant tous les secteurs pertinents ;

- **Protecteur** des consommateurs et de la propriété intellectuelle (civile et pénale), des citoyens, des organisations, des nations ;
- **Sécurisé** en réalisant une parfaite adéquation sécurité juridique et sécurité technologique ;
- **Intégré** à l'ordre international en assurant une bonne articulation entre les échelons national, régional et mondial.

3. Objet et finalité

L'objet de la convention sur la cybersécurité vise à contribuer à préserver les forces et les moyens organisationnels, humains, financiers, technologiques et informationnels, dont disposent les institutions, pour réaliser leurs objectifs. Elle englobe le traitement de la cybercriminalité et de la cybersécurité au sens strict mais ne se limite pas uniquement à cet aspect ; elle concerne des éléments importants des transactions électroniques et de la protection des données à caractère personnel.

Elle a une finalité éminemment protectrice en ce qu'elle vise à protéger :

- ☞ les institutions contre les **menaces** et les **préjudices** pouvant mettre en péril leur pérennité et leur efficacité ;
- ☞ les droits des **personnes** lors de la collecte, le traitement des données contre les menaces et les préjudices pouvant les affecter.

Elle vise également à :

- ☞ limiter les **atteintes ou dysfonctionnements** institutionnels induits, en cas de sinistre ;
- ☞ autoriser le retour à un **fonctionnement normal** à des coûts et des délais raisonnables ;

- ☞ mettre en place des mécanismes juridiques et institutionnels susceptibles de garantir **l'exercice normal** des droits humains dans le cyberespace.

4. Orientations stratégiques

La présente convention pose un dispositif juridique basé sur cinq orientations stratégiques suivantes :

- ☞ elle exprime les options d'une politique de cybersécurité à l'échelle de l'Union Africaine ;
- ☞ elle pose les bases d'une cyberéthique à l'échelle de l'Union Africaine en énonçant des principes fondamentaux dans les principaux domaines de la cybersécurité ;
- ☞ Elle organise les transactions électroniques, la signature électronique et la publicité par voie électronique ;
- ☞ Elle organise le cadre juridique et institutionnel de la protection des données à caractère personnel ;
- ☞ Elle consacre les bases d'un cyberdroit pénal et d'une procédure pénale adaptée au traitement de la cybercriminalité.