PROJET DE CONVENTION DE L'UNION AFRICAINE

SUR LA MISE EN PLACE D'UN CADRE JURIDIQUE DE CONFIANCE POUR LA CYBERSECURITE EN AFRIQUE

Cadre conceptuel

Partant d'une relecture de l'environnement juridique et institutionnel des régions de l'Union Africaine, le rapport propose 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 du commerce électronique, la protection des données à caractère personnel et la lutte contre la cybercriminalité.

1. **Contexte**

Dans un monde marqué par la globalisation des risques, des crimes et des menaces sur 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 Etats aux systèmes d'information et aux réseaux qui contrôleraient leurs besoins et moyens de sécurité des technologies de l'information.

Les Etats 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 Etats 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 Etats et des organisations.

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

Des efforts certains de protection juridique (nationale, communautaire et international) 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 Economiques Régionales s'inscrivent dans la même dynamique au moment des Etats 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 approfondit 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 socioculturelles.

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 Etats**.
- ☞ 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 articuler avec une stratégie pluridisciplinaire de la cybersécurité cohérente, efficace et contrôlable.

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

- ☞ Obtenir un niveau de **sécurité technologique** suffisant pour prévenir et maîtriser les risques technologique et informationnel
- ☞ Edifier d'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
- ☞ Contribuer à l'économie du savoir en garantissant un accès égal à l'information, en stimulant la création de **savoirs conformes**.
- ☞ créer un environnement de confiance c'est-à-dire un environnement qui soit :
    - o **Prévisible** en termes de prévention et règlements des différends et évolutif parce que tenant compte de l'évolution technologique continue
    - o **Organisé** : en couvrant tous les secteurs pertinents
    - o **Protecteur** : des consommateurs et de la propriété intellectuelle (civile et pénale), des citoyens, des organisations, des nations
    - o **Sécurisé** : en réalisant une parfaite adéquation sécurité juridique et technologique
    - o **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 se sont dotées les Institutions, pour réaliser leurs objectifs. Elle englobe le traitement de la cybercriminalité et à la cybersécurité au sens strict mais ne se limite pas uniquement à cet aspect ; elle concerne des éléments importants du commerce électronique 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 es préjudices pouvant les affecter.

Dans le même ordre d'idées, elle vise 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 les 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 le commerce électronique, 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.

PROJET DE CONVENTION DE L'UNION AFRICAINE

SUR LA MISE EN PLACE D'UN CADRE JURIDIQUE DE CONFIANCE POUR LA CYBERSECURITE EN AFRIQUE

PREAMBULE

Les Etats membres de l'Union africaine :

VISAS

Considérant que le présent projet de convention sur la ma mise en place d'un cadre juridique de confiance pour la cybersécurité prend en charge les engagements actuels des Etats membres de l'Union Africaine aux plans sous-régional, régional et international en vue de l'édification de la Société de l'Information ; qu'il 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 Etats membres et des Communautés Economiques Régionales (CER) en matière de Technologies de l'Information et de la Communication.

Considérant que la nécessité de mobiliser l'ensemble des acteurs publics et privés (Etat, collectivités locales, entreprises du secteur privé, organisations de la société civile, médias, institutions de formation et de recherche etc.) en faveur de la cybersécurité.

Forts des principes de l'Initiative Africaine de la Société de l'Information (AISI) et du Plan d'Action Régional Africain pour l'Economie du Savoir (PARAES) ;

Conscients qu'elle est destinée à régir un domaine technologique particulièrement évolutif et en vue répondre aux attentes exigeantes des nombreux acteurs aux intérêts souvent divergents, **la présente convention** détermine les règles de sécurité essentielles à la mise en place d'un espace numérique de confiance à travers l'organisation du commerce électronique, la protection des données à caractère personnel et la lutte contre la cybercriminalité

Considérant que les principaux obstacles au développement du commerce électronique en Afrique sont liés à des problèmes de sécurité dont notamment :

- les insuffisances qui affectent la réglementation en matière de reconnaissance juridique des messages de données ; de reconnaissance de la signature électronique ;

- l’absence de règles juridiques spécifiques protectrices des consommateurs, de la propriété intellectuelle, des données personnelles et des systèmes d’informations ;
- l’absence de législation propre aux téléservices et au télétravail ;
- l’application des techniques électroniques aux actes commerciaux et administratifs ;
- les éléments probants introduits par les techniques numériques (horodatage, certification, etc.).
- les règles applicables aux moyens et prestations de cryptologie.
- l’encadrement de la publicité en ligne ;
- l’absence de législations fiscale et douanière appropriées au commerce électronique.

Considérant que ce constat justifie l’appel à la mise en place d’un cadre normatif approprié correspondant à l’environnement juridique, culturel, économique et social africain ; que l’objet de cette convention vise donc à assurer la sécurité et le cadre juridique nécessaires à l’émergence d’un commerce électronique fiable en Afrique.

Considérant que sur un autre plan, la protection des données à caractère personnel ainsi que de la vie privée se présente donc comme un enjeu majeur de la société de l’information, tant pour les pouvoirs publics que pour les autres acteurs ; que de cette protection dépend naturellement la pérennité de cette nouvelle technologie qui devra allier protection de l’intimité des citoyens dans leur vie quotidienne ou professionnelle et garantie de la libre circulation des informations.

Considérant qu’il urge donc de mettre en place un dispositif permettant de faire face aux dangers et risques nés de l’utilisation de l'informatique et des fichiers sur les individus dans le souci de respecter la vie privée et les libertés tout en favorisant la promotion et le développement des TIC dans les pays membres de l’Union Africaine.

Considérant que l'ambition de la présente convention est de combler ce « vide juridique » ; qu’elle vise à mettre en place, dans chaque pays membres de l’union Africaine, 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 personnelles. ; qu’elle garantit, en proposant un type d’ancrage institutionnel, que tout traitement, sous quelque forme que ce soit, respecte les libertés et droits fondamentaux des personnes physiques tout en prenant également en compte les prérogatives des Etats, les droits des collectivités locales, les intérêts des entreprises ; qu’en prenant en compte les meilleures

pratiques reconnues au niveau international en matière de protection des données personnelles, elle propose un certain nombre de leviers réglementaires ainsi que les modalités permettant d'assurer la protection.

Considérant que la protection pénale du système de valeurs de la société de l'information s'impose comme une nécessité dictée par des considérations de sécurité ; qu'elle se manifeste essentiellement par le besoin d'une législation pénale appropriée à la lutte contre la cybercriminalité en général et au blanchiment de capitaux en particulier.

Conscients qu'il est nécessaire, face à l'actualité de la cybercriminalité qui constitue une véritable menace pour la sécurité des réseaux informatiques et le développement de la société de l'information en Afrique, de fixer les grandes orientations de la stratégie de répression de la cybercriminalité, dans les pays membres de l'Union Africaine, en prenant en charge leurs engagements actuels aux plans sous-régional, régional et international.

Considérant que la présente convention vise en droit pénal substantiel à moderniser les instruments de répression de la cybercriminalité, par l'élaboration d'une politique d'adoption d'incriminations nouvelles spécifiques aux TIC, d'adaptation de certaines incriminations, des sanctions et du régime de responsabilité pénale en vigueur dans les Etats Membres à l'environnement technologique.

Considérant qu'en outre, en droit pénal procédural, elle fixe d'une part le cadre de l'aménagement de la procédure classique par rapport aux TIC et précise d'autre part les conditions de l'institution de procédures spécifiques à la cybercriminalité.

Rappelant les décisions : (à compléter)

SONT CONVENUS DE CE QUI SUIT :

PARTIE I - L'ORGANISATION DU COMMERCE ELECTRONIQUE

Titre Premier : Terminologie

Article 1 :

Au sens de la présente convention, les différentes expressions suivantes seront définies comme suit :

1) **Activité de cryptologie** : vise toute activité ayant pour but la production, l'utilisation, l'importation, l'exportation ou la commercialisation des moyens de cryptologie ;
2) **Agrément :** consiste à la reconnaissance formelle que le produit ou le système évalué peut protéger jusqu'à un niveau spécifié par un organisme agréé ;
3) **Chiffrement** : vise toute technique qui consiste à transformer des données numériques en un format inintelligible en employant des moyens de cryptologie ;
4) **Commerce électronique** : vise comme l'activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens et la prestation de services ;
5) **Communication au public par voie électronique** : vise toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée ;
6) **Conventions secrètes** : visent les clés non publiées nécessaires à la mise en œuvre d'un moyen ou d'une prestation de cryptologie pour les opérations de chiffrement ou de déchiffrement ;
7) **Courrier électronique** : vise tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère ;
8) **Cryptologie** : vise la science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation ;
9) **Information** : vise tout élément de connaissance susceptible d'être représenté à l'aide de conventions pour être utilisé, conservé, traité ou communiqué. L'information peut être exprimée sous forme écrite, visuelle, sonore, numérique, etc. ;

10) **Moyens de cryptologie** : visent l'ensemble des outils scientifiques et techniques (matériel ou logiciel) qui permettent de chiffrer et/ou de déchiffrer ;
11) **Prestation de cryptologie** : vise toute opération visant à la mise en œuvre, pour le compte de soi ou d'autrui, des moyens de cryptologie ;
12) **Prestataire de services de cryptologie** : vise toute personne, physique ou morale, qui fournit une prestation de cryptologie ;
13) **Prospection directe** : vise tout envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services.

Titre II : Du commerce électronique

Chapitre Premier : Champ d'application du commerce électronique

Article 2 :

Le commerce électronique est l'activité économique par laquelle une personne propose ou assure par voie électronique la fourniture de biens ou la prestation de services.

Entrent également dans le champ du commerce électronique les services tels que ceux consistant à fournir des informations en ligne, des communications commerciales, des outils de recherche, d'accès, de récupération de données, d'accès à un réseau de communication ou d'hébergement d'informations, même s'ils ne sont pas rémunérés par ceux qui les reçoivent.

Article 3 :

L'activité définie à l'Article 1 de la présente Convention s'exerce librement dans l'espace de l'Union Africaine à l'exclusion des domaines suivants :

1) les jeux d'argent, mêmes sous forme de paris et de loteries, légalement autorisés ;
2) les activités de représentation et d'assistance en justice ;
3) les activités exercées par les notaires en application des textes en vigueur.

Article 4 :

Sans préjudice des autres obligations d'information prévues par les textes législatifs et réglementaires en vigueur dans les pays membres de l'Union Africaine, toute personne qui exerce l'activité définie à l'Article 1 de la présente Convention est tenue d'assurer à ceux à qui est destinée la fourniture de biens ou la prestation de services un accès facile, direct et permanent utilisant un standard ouvert aux informations suivantes :

1) s'il s'agit d'une personne physique, ses nom et prénom et, s'il s'agit d'une personne morale, sa raison sociale ;

2) l'adresse complète de l'endroit où elle est établie, son adresse de courrier électronique, ainsi que son numéro de téléphone ;
3) si elle est assujettie aux formalités d'inscription des entreprises ou au répertoire national des entreprises et associations, le numéro de son inscription, son capital social et l'adresse de son siège social ;
4) si elle est assujettie à la taxe sur la valeur ajoutée ;
5) si son activité est soumise à un régime d'autorisation, le nom et l'adresse de l'autorité ayant délivré celle-ci ;
6) si elle est membre d'une profession réglementée, la référence aux règles professionnelles applicables, son titre professionnel, le pays membre de l'Union Africaine dans lequel il a été octroyé ainsi que le nom de l'ordre ou de l'organisme professionnel auprès duquel elle est inscrite.

Article 5 :

Toute personne qui exerce l'activité définie à l'Article 1 par la présente Convention doit, même en l'absence d'offre de contrat, dès lors qu'elle mentionne un prix, indiquer celui-ci de manière claire et non ambiguë, et notamment si les taxes et les frais de livraison sont inclus.

Chapitre II : La responsabilité contractuelle du fournisseur électronique de biens ou de services

Article 6 :

Toute personne physique ou morale exerçant l'activité définie au premier alinéa de l'Article 1 de la présente Convention est responsable de plein droit à l'égard de son cocontractant de la bonne exécution des obligations résultant du contrat, que ces obligations soient à exécuter par elle-même ou par d'autres prestataires de services, sans préjudice de son droit de recours contre ceux-ci.

Toutefois, elle peut s'exonérer de tout ou partie de sa responsabilité en apportant la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable, soit au cocontractant, soit à un cas de force majeure.

Article 7 :

L'activité définie à l'Article 1 de la présente Convention est soumise à la loi du pays membre de l'Union Africaine sur le territoire duquel la personne qui l'exerce est établie, sous réserve de la commune intention de cette personne et de celle à qui sont destinés les biens ou services.

Titre III : Publicité par voie électronique

Article 8 :

Toute publicité, sous quelque forme que ce soit, accessible par un service de communication en ligne, doit pouvoir être clairement identifiée comme telle. Elle doit rendre clairement identifiable la personne physique ou morale pour le compte de laquelle elle est réalisée.

Article 9 :

Les publicités, et notamment les offres promotionnelles, telles que les rabais, les primes ou les cadeaux, ainsi que les concours ou les jeux promotionnels, adressés par courrier électronique, doivent pouvoir être identifiés de manière claire et non équivoque sur l'objet du courrier dès leur réception par leur destinataire, ou en cas d'impossibilité technique, dans le corps du message.

Article 10 :

Les conditions auxquelles sont soumises la possibilité de bénéficier d'offres promotionnelles ainsi que celle de participer à des concours ou à des jeux promotionnels, lorsque ces offres, concours ou jeux sont proposés par voie électronique, doivent être clairement précisées et aisément accessibles.

Article 11 :

Dans l'Union Africaine, il est interdit la prospection directe par envoi de message au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen.

Article 12 :

Nonobstant, les dispositions de l'Article 11, la prospection directe par courrier électronique est autorisée si :

1) les coordonnées du destinataire ont été recueillies directement auprès de lui ;
2) la prospection directe concerne des produits ou services analogues fournis par la même personne physique ou morale.

Article 13 :

Dans l'Union Africaine, il est interdit d'émettre, à des fins de prospection directe, des messages au moyen d'automates d'appel, télécopieurs et courriers électroniques, sans indiquer de coordonnées valables auxquelles le destinataire puisse utilement transmettre une demande tendant à obtenir que ces communications cessent sans frais autres que ceux liés à la transmission de celle-ci.

Article 14 :

Dans l'Union Africaine, il est également interdit de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise et de mentionner un objet sans rapport avec la prestation ou le service proposé.

Article 15 :

Le consentement des personnes dont les coordonnées ont été recueillies avant la publication de la présente Convention peut être sollicité par voie de courrier électronique.

Titre IV : Les obligations conventionnelles sous forme électronique

Chapitre Premier : Les contrats sous forme électronique

Article 16 :

La voie électronique peut être utilisée pour mettre à disposition des conditions contractuelles ou des informations sur des biens ou services.

Article 17 :

Les informations qui sont demandées en vue de la conclusion d'un contrat ou celles qui sont adressées au cours de son exécution peuvent être transmises par moyen électronique si leur destinataire a accepté l'usage de ce moyen.

Article 18 :

Les informations destinées à un professionnel peuvent lui être adressées par courrier électronique, dès lors qu'il a communiqué son adresse professionnelle électronique.

Article 19 :

Le fournisseur qui propose, à titre professionnel, par voie électronique, la fourniture de biens ou la prestation de services, met à disposition les conditions contractuelles applicables d'une manière qui permette leur conservation et leur reproduction. L'offre doit comprendre :

1) les différentes étapes à suivre pour conclure le contrat par voie électronique ;
2) les moyens techniques permettant à l'utilisateur, avant la conclusion du contrat, d'identifier les erreurs commises dans la saisie des données et de les corriger ;
3) les langues proposées pour la conclusion du contrat ;

4) en cas d'archivage du contrat, les modalités de cet archivage par l'auteur de l'offre et les conditions d'accès au contrat archivé ;
5) les moyens de consulter par voie électronique les règles professionnelles et commerciales auxquelles l'auteur de l'offre entend, le cas échéant, se soumettre.

Article 20 :

Pour que le contrat soit valablement conclu, le destinataire de l'offre doit avoir eu la possibilité de vérifier le détail de sa commande notamment du prix avant de confirmer celle-ci pour exprimer son acceptation.

Article 21 :

L'auteur de l'offre doit accuser réception sans délai injustifié et par voie électronique de la commande qui lui a été ainsi adressée.

La commande, la confirmation de l'acceptation de l'offre et l'accusé de réception sont considérés comme reçus lorsque les parties auxquelles ils sont adressés peuvent y avoir accès.

Article 22 :

Il peut être dérogé aux dispositions des Articles 20 et 21 de la présente Convention dans les conventions conclues entre professionnels.

Chapitre II : L'écrit sous forme électronique

Article 23 :

A défaut de dispositions légales contraires, nul ne peut être contraint de poser un acte juridique par voie électronique.

Article 24 :

Lorsqu'un écrit est exigé pour la validité d'un acte juridique, il peut être établi et conservé sous forme électronique dans les conditions définies par les textes juridiques pris en vue de son application.

Article 25 :

Il est fait exception aux dispositions de l'Article 24 de la présente Convention pour :

1) les actes sous seing privé relatifs au droit de la famille et des successions ;
2) les actes sous seing privé relatifs à des sûretés personnelles ou réelles, de nature civile ou commerciale, sauf s'ils sont passés par une personne pour les besoins de sa profession

Article 26 :

L'écrit résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission.

Article 27 :

Une lettre recommandée peut être envoyée par voie électronique à condition que ce courrier soit acheminé par un tiers selon un procédé permettant d'identifier le tiers, de désigner l'expéditeur, de garantir l'identité du destinataire et d'établir si la lettre a été remise ou non au destinataire.

Article 28 :

La remise d'un écrit sous forme électronique est effective lorsque le destinataire, après en avoir pris connaissance, en a accusé réception.

Article 29 :

Lorsque l'écrit sur papier est soumis à des conditions particulières de lisibilité ou de présentation, l'écrit sous forme électronique doit répondre à des exigences équivalentes.

Article 30 :

L'exigence d'un envoi en plusieurs exemplaires est réputée satisfaite sous forme électronique si l'écrit peut être imprimé par le destinataire.

Article 31 :

La facture sous forme électronique est admise en facturation au même titre que la facture sur support papier, pour autant que l'origine des données qu'elle contient et l'intégrité de son contenu soient garanties pendant la transmission.

Titre V : La sécurisation des transactions électroniques

Article 32 :

Aux fins de la présente convention, on entend par : "Signature électronique", une donnée sous forme électronique, qui est jointe ou liée logiquement à un message de données, qui peut être utilisé pour identifier le signataire du message de données et pour indiquer le consentement sur l'information contenu dans ce message[1] ;

Article 33 :

La preuve par écrit est établie conformément aux dispositions de l'Article 26 de la présente Convention.

Article 34 :

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.

Article 35 :

Le fournisseur de biens ou prestataire de services par voie électronique qui réclame l'exécution d'une obligation doit en prouver l'existence et, lorsqu'il se prétend libérer, doit prouver que l'obligation est inexistante ou éteinte.

[1] Prendre la définition officielle, art.1
(a) "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message;

Article 36 :

Lorsque les dispositions légales des pays membres n'ont pas fixées d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support.

Article 37 :

La copie ou toute autre reproduction d'actes passés par voie électronique a la même force probante que l'acte lui-même lorsqu'elle est certifiée conforme par des organismes agréés par une autorité étatique.

La certification donne lieu, le cas échéant, à la délivrance d'un certificat de conformité.

Article 38 :

La signature électronique est admise dans les écrits sous forme électronique au même titre que la signature manuscrite dans les écrits sur support papier.

Elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.

La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée par un dispositif sécurisé de création de signature, qu'elle garantit l'intégrité de l'acte et que l'identification du signataire en est assurée.

Article 39 :

Une signature électronique créée par un dispositif sécurisé que le signataire puisse garder sous son contrôle exclusif et qui repose sur un certificat numérique est admise comme signature au même titre que la signature manuscrite.

Article 40 :

A défaut de dispositions légales contraires, nul ne peut être contraint de poser un acte juridique par voie électronique.

PARTIE II- LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Titre Premier : Terminologie

Article 41 :

Au sens de la présente convention, les expressions ci-dessous sont définies comme suit :

1) **Code de conduite** : vise les chartes d'utilisation élaborées par le responsable du traitement afin d'instaurer un usage correct des ressources informatiques, de l'Internet et des communications électroniques de la structure concernée et homologué par l'Autorité de protection.

2) **Consentement de la personne concernée** : toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel accepte que ses données à caractère personnel fassent l'objet d'un traitement manuel ou électronique.

3) **Destinataire d'un traitement des données à caractère personnel** : vise toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargés de traiter les données.

4) **Données à caractère personnel :** visent 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 physique, physiologique, génétique, psychique, culturelle, sociale ou économique.

5) **Données sensibles** : visent toutes les données à caractère personnel relatives aux opinions ou activités religieuse, philosophique, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives.

6) **Données dans le domaine de la santé** : visent toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques précitées.

7) **Fichier de données à caractère personnel** : vise tout ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

8) **Interconnexion des données à caractère personnel** : vise tout mécanisme de connexion consistant en la mise en relation de données traitées pour une finalité déterminée avec d'autres données traitées pour des finalités identiques ou non, ou liées par un ou plusieurs responsables de traitement.

9) **Personne concernée** : vise toute personne physique qui fait l'objet d'un traitement des données à caractère personnel.

10) **Prospection directe** : vise toute sollicitation effectuée au moyen de l'envoi de message, quel qu'en soit le support ou la nature notamment commerciale, politique ou caritative, destinée à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services.

11) **Responsable du traitement** : vise la personne physique ou morale, publique ou privée, tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités.

12) **Sous-traitant** : vise toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données pour le compte du responsable du traitement.

13) **Tiers :** vise toute personne physique ou morale, publique ou privée, tout autre organisme ou association autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placés sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilités à traiter les données.

14) **Traitement des données à caractère personnel** : vise toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés ou non, et appliquées à des données, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le

verrouillage, le cryptage, l'effacement ou la destruction des données à caractère personnel.

Titre II : Le cadre juridique de la protection des données à caractère personnel

Chapitre Premier : Les objets de la présente convention sur les données à caractère personnel

Article 42 :

Dans l'Union Africaine, chaque pays membre doit disposer d'un cadre juridique ayant pour objet de mettre 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.

Ce dispositif doit garantir que tout traitement, sous quelque forme que ce soit, respecte les libertés et droits fondamentaux des personnes physiques tout en prenant en compte les prérogatives de l'Etat, les droits des collectivités locales et les intérêts des entreprises.

Chapitre II : Le champ d'application de la Convention

Article 43 :

Sont soumises à la présente convention :

1) Toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données à caractère personnel par une personne physique, par l'Etat, les collectivités locales, les personnes morales de droit public ou de droit privé ;
2) Tout traitement automatisé ou non de données contenues ou appelées à figurer dans un fichier, à l'exception des traitements mentionnés à l'Article 44 de la présente Convention ;
3) Tout traitement mis en œuvre sur le territoire d'un pays membre de l'Union Africaine ;
4) Tout traitement des données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, sous réserve des dérogations définies par des dispositions spécifiques fixées par d'autres textes de loi en vigueur.

Article 44 :

La présente convention ne s'applique pas :

1) aux traitements de données mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, à condition toutefois que les données ne soient pas destinées à une communication systématique à des tiers ou à la diffusion ;
2) aux copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises.

Chapitre III : Les formalités préalables à la mise en œuvre des traitements des données à caractère personnel

Article 45 :

Sont dispensés des formalités préalables :

1) les traitements mentionnés à l'Article 44 de la présente Convention ;
2) les traitements ayant pour seul objet la tenue d'un registre qui est destiné à un usage exclusivement privé ;
3) les traitements mis en œuvre par une association ou tout organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical dès lors que ces données correspondent à l'objet de cette association ou de cet organisme, qu'elles ne concernent que leurs membres et qu'elles ne doivent pas être communiquées à des tiers.

Article 46 :

En dehors des cas prévus à l'Article 45 ci-dessus et aux Article 48 et 49 de la présente Convention, les traitements de données à caractère personnel font l'objet d'une déclaration auprès de l'autorité de protection.

Article 47 :

Pour les catégories les plus courantes de traitement des données à caractère personnel dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, l'autorité de protection peut établir et publier des normes destinées à simplifier ou à exonérer l'obligation de déclaration.

Article 48 :

Sont mis en œuvre après autorisation de l'autorité de protection :

1) les traitements des données à caractère personnel portant sur des données génétiques et sur la recherche dans le domaine de la santé ;
2) les traitements des données à caractère personnel portant sur des données relatives aux infractions, condamnations ou mesures de sûreté ;
3) les traitements des données à caractère personnel ayant pour objet une interconnexion de fichiers, telle que définie à l'Article 92 de la présente Convention les traitements portant sur un numéro national d'identification ou tout autre identifiant de la même nature ;
4) les traitements des données à caractère personnel comportant des données biométriques ;
5) les traitements des données à caractère personnel ayant un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques.

Article 49 :

Les traitements des données à caractère personnel opérés pour le compte de l'Etat, d'un établissement public ou d'une collectivité locale ou d'une personne morale de droit privé gérant un service public sont décidés par acte législatif ou réglementaire pris après avis motivé de l'autorité de protection.

Ces traitements portent sur :

1) la sûreté de l'Etat, la défense ou la sécurité publique ;
2) la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;
3) le recensement de la population ;
4) les données à caractère personnel faisant apparaître, directement ou indirectement, les origines raciales, ethniques ou régionales, la filiation, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle ;
5) le traitement de salaires, pensions, impôts, taxes et autres liquidations.

Article 60 :

Les demandes d'avis, les déclarations et les demandes d'autorisations doivent préciser :

1) l'identité et l'adresse du responsable du traitement ou, si celui-ci n'est pas établi sur le territoire d'un pays membre de l'Union Africaine, celles de son représentant dûment mandaté ;
2) la ou les finalités du traitement ainsi que la description générale de ses fonctions ;
3) les interconnexions envisagées ou toutes autres formes de mise en relation avec d'autres traitements ;
4) les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;
5) la durée de conservation des données traitées ;
6) le ou les services chargés de mettre en œuvre le traitement ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;
7) les destinataires habilités à recevoir communication des données ;
8) la fonction de la personne ou le service auprès duquel s'exerce le droit d'accès ;
9) les dispositions prises pour assurer la sécurité des traitements et des données ;
10) l'indication du recours à un sous-traitant ;
11) les transferts de données à caractère personnel envisagés à destination d'un pays tiers non membre de l'Union Africaine, sous réserve de réciprocité.

Article 61 :

L'autorité de protection se prononce dans un délai fixe à compter de la réception de la demande d'avis ou d'autorisation. Toutefois, ce délai peut être prorogé ou non sur décision motivée de l'autorité de protection.

Article 62 :

L'avis ou la déclaration ou la demande d'autorisation peut être adressé à l'autorité de protection par voie électronique ou par voie postale.

Article 63 :

L’autorité de protection peut être saisie par toute personne, agissant par elle-même, par l’entremise de son avocat ou par toute autre personne physique ou morale dûment mandatée.

Titre III : Le cadre institutionnel de la protection des données à caractère personnel

Chapitre Premier : Statut, composition et organisation

Article 64 :

Dans l'Union Africaine, chaque Etat membre doit disposer d'une autorité chargée de la protection des données à caractère personnel.

L'autorité de protection est une autorité administrative indépendante chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente Convention.

Article 65 :

L'autorité de protection informe les personnes concernées et les responsables de traitement de leurs droits et obligations.

Article 66 :

L'autorité de protection doit comprendre des parlementaires, des députés, des sénateurs, des hauts magistrats de la Cour des comptes, du Conseil d'Etat, de la Cour de cassation, des personnalités qualifiées pour leur connaissance de l'informatique, des réseaux ou des secteurs professionnels.

Article 67 :

Des agents assermentés, conformément aux dispositions en vigueur dans les pays membres de l'Union Africaine, peuvent être appelés à participer à la mise en œuvre des missions de vérification. .

Article 68 :

Les membres de l'autorité de protection sont soumis au secret professionnel conformément aux textes en vigueur dans chaque pays membre.

Chaque autorité de protection établit un règlement intérieur qui précise, notamment, les règles relatives aux délibérations, à l'instruction et à la présentation des dossiers.

Article 69 :

La qualité de membre d'une autorité de protection est incompatible avec la qualité de membre du Gouvernement**,** de l'exercice des fonctions de dirigeants d'entreprise, de la détention de participation dans les entreprises du secteur de l'informatique ou des télécommunications.

Article 70 :

Les membres d'une autorité de protection jouissent d'une immunité totale pour les opinions émises dans l'exercice ou à l'occasion de l'exercice de leur fonction.

Dans l'exercice de leur attribution, ils ne reçoivent d'instruction d'aucune autorité.

Article 71 :

Pour l'accomplissement de ses missions, l'autorité de protection reçoit une dotation budgétaire de l'Etat.

Chapitre II : Attributions de l'autorité de protection

Article 72 :

L'autorité de protection est chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente Convention.

Article 73 :

L'autorité de protection s'assure que les TIC ne comportent pas de menace au regard des libertés publiques et de la vie privée. A ce titre, elle doit :

1) répondre à toute demande d'avis portant sur un traitement de données à caractère personnel ;
2) informer les personnes concernées et les responsables de traitement de leurs droits et obligations ;
3) autoriser les traitements de fichiers dans un certain nombre de cas, notamment les fichiers sensibles ;
4) recevoir les formalités préalables à la création de traitements des données à caractère personnel ;
5) recevoir les réclamations, les pétitions et les plaintes relatives à la mise en œuvre des traitements des données à caractère personnel et informer leurs auteurs des suites données à celles-ci ;
6) informer sans délai l'autorité judiciaire pour certains types d'infractions dont elle a connaissance ;
7) procéder, par le biais d'agents assermentés, à des vérifications portant sur tout traitement des données à caractère personnel ;
8) prononcer des sanctions, administratives et pécuniaires, à l'égard d'un responsable de traitement ;
9) mettre à jour un répertoire des traitements des données à caractère personnel et à la disposition du public ;
10) conseiller les personnes et organismes qui font les traitements des données à caractère personnel ou qui procèdent à des essais ou expériences de nature à aboutir à de tels

traitements ;

11) autoriser les transferts transfrontaliers de données à caractère personnel ;
12) faire des suggestions susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données ;
13) mettre en place des mécanismes de coopération avec les autorités de protection des données à caractère personnel de pays tiers ;
14) participer aux négociations internationales en matière de protection des données à caractère personnel ;
15) établir, selon une périodicité bien définie, un rapport d'activités remis soit au Président de la République, soit au Président de l'Assemblée nationale, soit au Premier ministre, soit au Ministre de la Justice.

Article 74 :

L'autorité de protection peut prononcer les mesures suivantes :

1) un avertissement à l'égard du responsable du traitement ne respectant pas les obligations découlant de la présente Convention ;
2) une mise en demeure de faire cesser les manquements concernés dans le délai qu'elle fixe.

Article 75 :

Si le responsable du traitement ne se conforme pas à la mise en demeure qui lui a été adressée, l'autorité de protection peut prononcer à son encontre, après procédure contradictoire, les sanctions suivantes :

1) un retrait provisoire de l'autorisation accordée ;
2) le retrait définitif de l'autorisation ;
3) une amende pécuniaire ;

Article 76 :

En cas d'urgence, lorsque la mise en œuvre d'un traitement ou l'exploitation de données à caractère personnel entraîne une violation de droits et libertés, l'autorité de protection, après procédure contradictoire, peut décider :

1) l'interruption de la mise en œuvre du traitement ;
2) le verrouillage de certaines données à caractère personnel traitées ;
3) l'interdiction temporaire ou définitive d'un traitement contraire aux dispositions de la présente Convention.

Article 77 :

Les sanctions et décisions prises par l'autorité de protection sont susceptibles de faire l'objet d'un recours.

Titre IV : Les obligations relatives aux conditions de traitements de données à caractère personnel

Chapitre Premier : Les principes de base gouvernant le traitement des données à caractère personnel

Section Première : Le principe de consentement et de légitimité du traitement des données à caractère personnel

Article 78 :

Le traitement des données à caractère personnel est considéré comme légitime si la personne concernée donne son consentement.

Toutefois, il peut être dérogé à cette exigence du consentement lorsque le traitement est nécessaire :

1) au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
2) à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ;
3) à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande ;
4) à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée.

Section II : Le principe de la licéité et de la loyauté du traitement des données à caractère personnel

Article 79 :

La collecte, l'enregistrement, le traitement, le stockage et la transmission des données à caractère personnel doivent se faire de manière licite, loyale et non frauduleuse.

Section III : Le principe de finalité, de pertinence, de conservation du traitement des données à caractère personnel

Article 80 :

Les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités.

Elles doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement.

Elles doivent être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées.

Au-delà de cette période requise, les données ne peuvent faire l'objet d'une conservation qu'en vue de répondre spécifiquement à un traitement à des fins historiques, statistiques ou de recherches en vertu des dispositions légales.

Section IV : Le principe d'exactitude des données à caractère personnel

Article 81 :

Les données collectées doivent être exactes et, si nécessaire, mises à jour. Toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement, soient effacées ou rectifiées.

Section V : Le principe de transparence des données à caractère personnel

Article 82 :

Le principe de transparence implique une information obligatoire de la part du responsable du traitement portant sur les données à caractère personnel.

Section VI : Le principe de confidentialité et de sécurité des traitements de données à caractère personnel

Article 83 :

Les données à caractère personnel doivent être traitées de manière confidentielle et être protégées, notamment lorsque le traitement comporte des transmissions de données dans un réseau.

Article 84 :

Lorsque le traitement est mis en œuvre pour le compte du responsable du traitement, celui-ci doit choisir un sous-traitant qui apporte des garanties suffisantes. Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect des mesures de sécurité définies de la présente Convention.

Chapitre II : les principes spécifiques relatifs au traitement de certaines catégories de données à caractère personnel

Article 85 :

Dans l'Union Africaine, il est interdit de procéder à la collecte et à tout traitement qui révèlent l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée.

Article 86 :

L'interdiction fixée à l'Article 85 ne s'applique pas pour les catégories de traitements suivantes lorsque :

1) le traitement des données à caractère personnel porte sur des données manifestement rendues publiques par la personne concernée ;
2) la personne concernée a donné son consentement par écrit, quel que soit le support, à un tel traitement et en conformité avec les textes en vigueur ;
3) le traitement des données à caractère personnel est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
4) le traitement, notamment des données génétiques, est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
5) une procédure judiciaire ou une enquête pénale est ouverte ;
6) le traitement des données à caractère personnel s'avère nécessaire pour un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques ;
7) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée pendant la période précontractuelle ;
8) le traitement est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis ;

9) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou est effectué par une autorité publique ou est assigné par une autorité publique au responsable du traitement ou à un tiers, auquel les données sont communiquées ;
10) le traitement est effectué dans le cadre des activités légitimes d'une fondation, d'une association ou de tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse, mutualiste ou syndicale. Toutefois, le traitement doit se rapporter aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées.

Article 87 :

Le traitement des données à caractère personnel réalisé aux fins de journalisme**,** de recherche ou d'expression artistique ou littéraire est admis lorsqu'il est mis en œuvre aux seules fins d'expression littéraire et artistique ou d'exercice, à titre professionnel, de l'activité de journaliste ou chercheur, dans le respect des règles déontologiques de ces professions.

Article 88 :

Les dispositions de la présente Convention ne font pas obstacle à l'application des dispositions des lois relatives à la presse écrite ou au secteur de l'audiovisuel et du code pénal qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes physiques.

Article 89 :

Dans l'Union Africaine, il est interdit de procéder à la prospection directe à l'aide de tout moyen de communication utilisant, sous quelque forme que ce soit, les données à caractère personnel d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir de telles prospections.

Article 90 :

Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé des données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

Aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé des données à caractère personnel destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

Article 91 :

Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un pays non membre de l'Union Africaine que si cet Etat assure un niveau de protection suffisant de la vie privée, des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet.

Avant tout transfert des données à caractère personnel vers ce pays tiers, le responsable du traitement doit préalablement informer l'autorité de protection.

Chapitre III : L'interconnexion des fichiers comportant des données à caractère personnel

Article 92 :

L'interconnexion des fichiers visée à l'Article 48 de la présente Convention doit permettre d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements. Elle ne peut pas entraîner de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées ni être assortie de mesures de sécurité appropriées et doit tenir compte du principe de pertinence des données faisant l'objet de l'interconnexion.

Titre V : Les droits conférés à la personne dont les données font l'objet d'un traitement

Chapitre Premier : Droit à l'information

Article 93 :

Le responsable du traitement doit fournir à la personne dont les données font l'objet d'un traitement, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes :

1) son identité et, le cas échéant, celle de son représentant;
2) la ou les finalités déterminées du traitement auquel les données sont destinées ;
3) les catégories de données concernées ;
4) le ou les destinataires auxquels les données sont susceptibles d'être communiquées ;
5) le fait de pouvoir demander à ne plus figurer sur le fichier ;
6) l'existence d'un droit d'accès aux données la concernant et de rectification de ces données ;
7) la durée de conservation des données ;
8) l'éventualité de tout transfert de données à destination de pays tiers.

Chapitre II : Droit d'accès

Article 94 :

Toute personne physique dont les données à caractère personnel font l'objet d'un traitement peut demander au responsable de ce traitement, sous forme de questions :

1) les informations permettant de connaître et de contester le traitement ;
2) la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;
3) la communication des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;
4) des informations relatives aux finalités du traitement, aux catégories de données à

caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées.

Chapitre III : Droit d'opposition

Article 95 :

Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Elle a le droit, d'une part, d'être informée avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et, d'autre part, de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

Chapitre IV : Droit de rectification et de suppression

Article 96 :

Toute personne physique peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou supprimées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Titre VI : Les obligations du responsable de traitement de données à caractère personnel

Chapitre Premier : Les obligations de confidentialité

Article 97 :

Le traitement des données à caractère personnel est confidentiel. Il est effectué exclusivement par des personnes qui agissent sous l'autorité du responsable du traitement et seulement sur ses instructions.

Chapitre II : Les obligations de sécurité

Article 98 :

Le responsable du traitement est tenu de prendre toute précaution utile au regard de la nature des données et, notamment, pour empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Chapitre III : Les obligations de conservation

Article 99 :

Les données à caractère personnel doivent être conservées pendant une durée fixée par un texte réglementaire et uniquement pour les fins en vue desquelles elles ont été recueillies.

Chapitre IV : Les obligations de pérennité

Article II - 100 :

Le responsable du traitement est tenu de prendre toute mesure utile pour assurer que les données à caractère personnel traitées pourront être exploitées quel que soit le support technique utilisé.

Il doit particulièrement s'assurer que l'évolution de la technologie ne sera pas un obstacle à cette exploitation.

PARTIE III - LA LUTTE CONTRE LA CYBERCRIMINALITE

Titre Premier : Principes fondamentaux

Chapitre Premier : Terminologie

Article 101 : Au sens de la présente convention, les expressions ci-dessous sont définies comme suit :

1) **Communication électronique :** vise toute mise à disposition au public ou d'une catégorie de public, par un procédé de communication électronique ou magnétique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature ;
2) **Données informatisées :** visent toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique ;
3) **Raciste et xénophobe en matière des TIC** : vise tout écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique ou de la religion, dans la mesure ou cette dernière sert de prétexte à l'un ou à l'autre de ces éléments ou qui incite à de tels actes ;
4) **Mineur :** vise toute personne âgée de moins de 18 ans au sens de la convention des Nations Unies sur les droits de l'enfant ;
5) **Pornographie infantile :** vise toute donnée quelle qu'en soit la nature ou la forme représentant de manière visuelle un mineur se livrant à un agissement sexuellement explicite ou des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite ;
6) **Système informatique :** vise tout dispositif isolé ou non, tout ensemble de dispositifs interconnectés assurant en tout ou partie, un traitement automatisé de données en exécution d'un programme.

CHAPITRE 1 : Cadre de la cybersécurité nationale

Article 102 :

Chaque État membre devra – en collaboration avec les parties prenantes clés comprenant les gouvernements à tous les niveaux ; l'industrie et les organisations professionnelles ; les sociétés civiles et les citoyens en général – se doter d'une politique nationale de cybersécurité qui reconnaisse l'importance de l'infrastructure essentielle de l'information (IEI) pour la nation, qui identifie les risques auxquels elle est confrontée en utilisant une approche tous risques et qui définit dans les grandes lignes la façon dont les objectifs seront mis en œuvre.

Article 103 :

Les États membres devront adopter les stratégies qu'ils jugent appropriées et suffisantes pour mettre en œuvre la politique nationale de cybersécurité, spécifiquement dans le domaine de la réforme légale et du développement, de la sensibilisation et du développement des capacités, du partenariat public-privé et de la coopération internationale, pour ne citer que ceux-ci. Les stratégies devront établir des structures organisationnelles et se fixer des objectifs ainsi que des délais pour mener à bien tous les aspects de la politique de cybersécurité, tout en posant les bases d'une gestion effective des incidents et de la coopération internationale.

CHAPITRE 2 : Mesures légales

Article 104 :

Chaque État membre devra adopter les mesures législatives qu'il jugera efficaces en considérant comme infractions criminelles substantielles des actes qui affectent la confidentialité, l'intégrité, la disponibilité et la survivance des systèmes TIC et des infrastructures réseau sous-jacentes, ainsi que les mesures procédurales qu'il jugera efficaces pour rechercher et poursuivre les contrevenants. Les États membres sont invités à prendre en considération le choix du langage approuvé dans les modèles mondiaux de législations de cybercriminalité tel que celui adopté par le Conseil de l'Europe et le Commonwealth des Nations s'il y a lieu.

Article 105 :

Chaque État membre devra adopter les mesures législatives qu'il jugera nécessaires pour conférer la responsabilité spécifique aux institutions - qu'elles soient nouvellement créées ou préexistantes – ainsi qu'aux officiels désignés de ces institutions, afin de leur impartir l'autorité statutaire et la capacité légale à agir dans tous les aspects de l'application de la cybersécurité, y compris mais sans s'y limiter, la réponse aux incidents et la coordination en matière de justice réparatrice, les investigations en criminalistique, la poursuite, etc.

Article 106 :

En adoptant des mesures légales en matière de cybersécurité ou en créant le cadre d'application de celle-ci, chaque État membre devra s'assurer que les mesures adoptées n'entraveront pas les droits des citoyens garantis en vertu de la constitution nationale et protégés par les conventions internationales, particulièrement la Charte africaine des droits de l'Homme, ainsi que les droits tels que le droit à la liberté d'expression, le droit au respect de la vie privée et le droit à une instruction équitable, entre autres.

Article 107 : Protection de l'infrastructure essentielle de l'information

Chaque État membre devra adopter les mesures légales qu'il jugera nécessaires pour identifier les secteurs considérés comme sensibles pour la sécurité nationale et le bien-être de l'économie et des systèmes TIC désignés pour fonctionner dans ces secteurs comme constituant des infrastructures essentielles de l'information, en proposant à cet égard une sanction plus sévère pour les activités criminelles sur les systèmes TIC dans ces secteurs et également des dispositions pour améliorer la vigilance, la sécurité et la gestion.

Chapitre III : Système national de la cybersécurité

Article 108 :

1. Chaque État membre devra s'attacher à promouvoir une culture de la sécurité chez toutes les parties prenantes – gouvernements, entreprises et société civile – qui développent, possèdent, gèrent, mettent en service et utilisent les systèmes et les réseaux d'information. La culture de la sécurité devra mettre l'accent sur la sécurité dans le développement des systèmes et des réseaux d'information et sur l'adoption de nouvelles façons de penser et de se comporter lors de l'utilisation des systèmes d'information et lors de la communication ou de la transaction à travers les réseaux.

2. Dans le cadre de la promotion d'une culture de la sécurité, les États membres peuvent adopter les mesures suivantes : mettre en place un plan de cybersécurité pour les systèmes gérés par le gouvernement ; rechercher et mettre en œuvre des programmes et des initiatives de sensibilisation à la sécurité pour les utilisateurs des systèmes et des réseaux ; inciter au développement d'une culture de la sécurité dans les entreprises ; favoriser l'engagement de la société civile ; lancer un programme de sensibilisation nationale détaillé et complet ; renforcer les activités de sciences et de technologie (S&T) et de recherche et développement (R-D) ainsi que la sensibilisation aux cybermenaces et aux solutions disponibles.

Article 109 :

Chaque État membre devra être le garant d'un leadership pour le développement d'une culture de la sécurité à l'intérieur de ses frontières. Les États membres devront par conséquent développer la sensibilisation, assurer l'éducation et la formation ainsi que la diffusion des informations au public.

Article 110 :

Chaque État membre devra adopter un partenariat public-privé en tant que modèle afin d'engager l'industrie, la société civile et universitaire dans la promotion et le renforcement d'une culture de la cybersécurité.

Article 111 :

Chaque État membre devra adopter des mesures de développement des capacités afin de proposer une formation couvrant tous les domaines de la cybersécurité aux institutions appropriées du gouvernement, tout en fixant des normes pour le secteur privé. Cette formation devrait permettre de promouvoir l'échange d'informations entre les experts et les vendeurs en sécurité, les détenteurs, les gestionnaires et les utilisateurs des TIC. Les États membres devront promouvoir l'éducation technique des professionnels des TIC à l'intérieur et à l'extérieur des instances gouvernementales par le biais de la certification et de la normalisation des formations ; la catégorisation des qualifications professionnelles et le développement et la distribution de matériel éducatif en fonction des besoins.

Article 112 :

1. Chaque État membre devra adopter un programme efficace de sensibilisation à la cybersécurité nationale aux fins de promouvoir la sensibilisation à la cybersécurité au sein du public et des parties prenantes clés ; établir des relations avec les professionnels de la cybersécurité afin de partager les informations relatives aux initiatives en matière de cybersécurité et de promouvoir la collaboration sur les questions de cybersécurité ;
2. Lors du développement d'un programme de sensibilisation, les États membres devront prendre en considération :
    i. l'accompagnement et l'engagement des parties prenantes pour développer et établir des relations de confiance entre l'industrie, le gouvernement et le monde universitaire aux fins d'augmenter le niveau de sensibilisation à la cybersécurité ;
    ii. la coordination et la collaboration sur les activités en matière de cybersécurité dans l'ensemble du gouvernement ; et

iii. les communications, avec les organismes tant internes qu'externes : autres agences gouvernementales, industrie, institutions éducatives, utilisateurs d'ordinateurs domestiques et grand public.

3. Pour augmenter le niveau de sensibilisation sur les questions de cybersécurité, les responsables politiques et les autres parties prenantes en matière de cybersécurité pourraient :

i. établir des partenariats public-privé lorsque cela est nécessaire ;

ii. lancer des campagnes de publicité de grande envergure afin de toucher le plus grand nombre de personnes possible ;

iii. utiliser les ONG, les institutions, les banques, les FAI, les librairies, les organisations commerciales locales, les centres communautaires, les magasins d'informatique, les collèges communautaires et les programmes éducatifs pour adultes, les associations scolaires et les associations de parents d'élèves pour faire passer le message d'un cybercomportement sûr.

Chapitre IV : Structures nationales de suivi de la cybersécurité

Article 113 :

1. Chaque État membre devra adopter les mesures nécessaires pour mettre en place une structure institutionnelle et de gouvernance appropriée en matière de cybersécurité.

2. Les mesures adoptées au titre du paragraphe 1 du présent article viseront à établir un fort leadership et un engagement dans les divers aspects de la cybersécurité des institutions et des groupes professionnels compétents de l'État membre. À cet égard, les États membres devront prendre des dispositions pour :

   i. établir une responsabilité claire en matière de cybersécurité à tous les niveaux du gouvernement en définissant précisément les rôles et les responsabilités ;

   ii. prendre un engagement manifeste en matière de cybersécurité, qui soit public et transparent ;

   iii. encourager le secteur privé, en sollicitant son engagement et sa participation dans des initiatives dirigées par le gouvernement aux fins de promouvoir la cybersécurité.

3. La gouvernance de la cybersécurité devra être établie en fonction d'un cadre national qui soit en mesure de répondre aux défis perçus et également à toute question relative à la sécurité de l'information au niveau national dans le plus grand nombre possible de domaines de la cybersécurité.

Article 114 :

1. Chaque État membre devra adopter les mesures qu'il jugera nécessaires aux fins de créer des institutions compétentes pour lutter contre la cybercriminalité ; de mener une veille, une réponse aux incidents et aux alertes ; d'assurer la coordination nationale et transfrontalière des problèmes de cybersécurité et également la coopération mondiale.

2. Les structures organisationnelles pourraient se présenter sous l'une des formes suivantes : un Conseil national de la cybersécurité (NCC), une Autorité nationale de

la cybersécurité (NCA) et une CERT et/ou CSIRT nationale. Chaque État membre peut adapter ses structures aux fins de fournir « un ajustement précis » en fonction de leur niveau de développement TIC, de la disponibilité des ressources et des partenariats public-privé. Les structures peuvent exister sous d'autres noms ou des noms différents.

3. Il est recommandé aux États membres d'établir un centre de liaison national ou une entité organisationnelle spécifique aux fins de supporter une politique de cybersécurité nationale et de faciliter la coopération régionale et internationale.

Article 115 -

Chaque État membre devra créer un Conseil national de la cybersécurité (NCC) ou son équivalent, en tant qu'entité spécifique (séparée) ou une composante du Conseil national de la sécurité. Le NCC devra servir de centre de liaison à haut niveau pour la cybersécurité au sein de l'État membre et devra adopter ou approuver les politiques proposées pour sa mise en œuvre par une Autorité nationale de la cybersécurité (NCA) ou son équivalent au sein de l'État membre en relation avec :

i. la politique et la stratégie en matière de cybersécurité nationale ;

ii. les priorités et les initiatives en matière de cybersécurité nationale ;

iii. la coordination des actions en matière de cybersécurité au niveau national ;

iv. l'identification des protagonistes chargés de la cybersécurité dans l'économie et l'établissement de relations public-privé nécessaires pour aborder les questions de cybersécurité ;

v. la collaboration avec plusieurs services ou agences gouvernementaux tels que les services de renseignements, les services secrets, la Direction générale de la sécurité, les forces de police, l'unité de la criminalité technologique, etc., aux fins d'élaborer des normes, d'établir des procédures d'investigation uniformes et de développer un consensus institutionnel ;

vi. la collaboration avec les organismes chargés de l'application de la loi au niveau régional ou international ;

vii. la surveillance des systèmes gouvernementaux de l'information et des infrastructures essentielles ;

viii. la coordination des actions et du développement des systèmes d'identité numérique et la gestion et les bonnes pratiques en relation avec les identités numériques, entre autres ; et

ix. le développement de formations types et de programmes de développement des capacités pour les agences et la création d'une plateforme nationale aux fins de coordonner l'assistance technique et les initiatives de formation au niveau international.

Article 116 :

Il est fortement recommandé à chaque État membre d'adopter des mesures en vue de l'établissement d'une Autorité nationale de la cybersécurité (NCA) chargée de la mise en place de la politique et de la stratégie de la cybersécurité nationale de l'État membre et également de la coordination de toutes les initiatives nationales en matière de cybersécurité.

1. La NCA, distincte du NCC et dotée d'un certain degré d'indépendance, devra exécuter les fonctions visant à faciliter la mise en place des mesures identifiées dans la politique nationale approuvée par le NCC ; la vérification de la conformité, les audits de risque et l'évaluation de sécurité ; assister le NCC dans toutes ses activités opérationnelles et aider l'industrie à tester son plan d'urgence ; travailler avec l'industrie pour établir des objectifs et des règles pour la sécurité de l'infrastructure et des services TIC et pour contribuer à l'application des normes internationales relatives à la cybersécurité et à l'accréditation ou à la certification des infrastructures, des services ou des fournisseurs TIC.

Article 117 :

1. Chaque État membre devra établir une CERT nationale chargée de représenter sa protection de l'infrastructure de l'information et servant de point de coordination national en vue de réagir aux menaces de sécurité TIC au niveau régional et mondial.

2. Les États membres devront garantir que leurs CERT nationales sont capables de fournir des services réactifs et proactifs et de communiquer des informations en temps opportun sur les dernières menaces pertinentes et d'apporter leur aide pour réagir aux incidents lorsque cela s'avère nécessaire.

3. Les États membres devront garantir que la CERT établie au titre du présent article devra exécuter les services minimum suivants :

    i. services réactifs : alertes et mises en garde, traitement des incidents, analyse des incidents, support de réponse aux incidents, coordination de la réponse aux incidents, réponse aux incidents sur site, traitement de la vulnérabilité, analyse de vulnérabilité, réponse à la vulnérabilité et coordination de la réponse à la vulnérabilité ;

    ii. services proactifs : annonces, veille technologique, audits ou évaluations de sécurité, configuration et maintenance des installations de sécurité, développement des outils de sécurité, services de détection d'intrusion et diffusion des informations relatives à la sécurité ; et

    iii. traitement des artéfacts : analyse d'artéfacts, réponse aux artéfacts, coordination de réponse aux artéfacts, analyse du risque, poursuite de l'activité et reprise après sinistre, consultation de sécurité, campagne de sensibilisation, éducation/formation et évaluation ou certification de produit.

Article 118 :

Chaque État membre devra adopter les mesures nécessaires à la mise en place et au maintien de collaborations transfrontalières avec d'autres CERT/CSIRT au niveau régional et mondial. Les États membres peuvent rejoindre des réseaux d'alerte et de veille existants (WWN) tels que le réseau FIRST (Forum of Incident Response and Security Team – Forum des équipes de réponse aux incidents et de sécurité), le groupe CERT du gouvernement européen (EGC), etc.

Chapitre V : Coopération internationale

Article 119 :

Chaque État membre devra garantir que les mesures législatives adoptées sur les dispositions substantives et procédurales de la cybercriminalité reflètent la meilleure pratique internationale, en prenant en compte le standard minimum adopté dans les législations en vigueur dans l'ensemble de la région afin de renforcer la possibilité d'harmonisation régionale de ces mesures légales.

Article 120 :

Le principe cardinal de coopération en matière d'application de la loi contre la criminalité transfrontalière repose sur le fait que les lois au titre desquelles cette coopération est recherchée par chaque État membre soient uniformes par rapport à la conduite prohibée et à la procédure d'application. Chaque État membre devra adopter les mesures légales qui devront respecter le principe de la double criminalité.

Article 121 :

Chaque État membre devra adopter les mesures légales qu'il jugera nécessaires pour permettre des échanges d'informations ainsi que le partage des données rapides, expéditifs et réciproques par les organisations des États membres et par des organisations similaires d'autres États membres chargées de faire appliquer la loi sur le territoire sur une base bilatérale ou multilatérale.

Article 122 :

Les États membres devront créer des institutions qui échangent des informations sur les menaces et sur l'évaluation de la vulnérabilité telles que les CERT (Computer Emergency Response Teams : équipes de réaction d'urgence en informatique) ou les CSIRTS (Computer Security Incident Response Teams : équipes de réaction aux incidents de sécurité

informatique). Ces équipes seront chargées d'instaurer des relations de confiance avec les parties prenantes clés, de travailler avec les vendeurs afin de diffuser les alertes de menaces à la sécurité cybernétique ; de développer et de mettre en place des capacités de réaction aux incidents en informatique, en collaboration avec des organisations similaires ou autres organisations des États membres.

Article 123 :

Outre les mesures légales que les États membres doivent adopter pour créer les bases juridiques requises pour la coopération, chaque État membre devra adopter les mécanismes ou les procédures qu'il jugera efficaces aux fins de créer et d'entretenir des contacts réguliers avec le plus grand nombre possible d'institutions nationales, régionales et mondiales, et de permettre aux institutions des États membres de fournir sur demande ou de recevoir comme requis toutes les informations ou l'assistance relatives à la cybersécurité sur une base réciproque en temps voulu.

Article 124 :

Chaque État membre devra se prévaloir de moyens existants pour la coopération internationale aux fins de répondre aux cybermenaces, d'améliorer la cybersécurité et de stimuler le dialogue entre les parties prenantes. Ces moyens pourraient être intergouvernementaux internationaux, intergouvernementaux régionaux ou basés sur des partenariats privés et publics, que ce soit au niveau régional ou international.

Article 125 :

Chaque État membre devra adopter les mesures et les stratégies qui lui seront nécessaires pour prendre part à la coopération régionale et internationale en matière de cybersécurité. Les résolutions promouvant la participation des États membres dans ce cadre de relations ont été adoptées par un grand nombre d'organismes gouvernementaux internationaux comprenant notamment les Nations Unies, l'Union africaine, l'Union européenne et le groupe d'États du

G8. Des organisations telles que l'Union internationale des télécommunications, le Conseil de l'Europe, le Commonwealth des Nations, ont mis en place des cadres types pour la coopération internationale que l'État membre peut adopter à titre de guide.

Titre II : Droit pénal substantiel

Chapitre Premier : Les infractions spécifiques aux Technologies de l'Information et de la Communication

Section Première : Atteintes aux systèmes informatiques

Article 126 :

Chaque État membre devra adopter des mesures de développement des capacités afin de proposer une formation couvrant tous les domaines de la cybersécurité aux institutions appropriées du gouvernement, tout en fixant des normes pour le secteur privé. Cette formation devrait permettre de promouvoir l'échange d'informations entre les experts et les vendeurs en sécurité, les détenteurs, les gestionnaires et les utilisateurs des TIC. Les États membres devront promouvoir l'éducation technique des professionnels des TIC à l'intérieur et à l'extérieur des instances gouvernementales par le biais de la certification et de la normalisation des formations ; la catégorisation des qualifications professionnelles et le développement et la distribution de matériel éducatif en fonction des besoins.

Article 127 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait d'accéder ou de tenter d'accéder frauduleusement dans tout ou partie d'un système informatique.

Article 128 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait de se maintenir ou de tenter de se maintenir frauduleusement dans tout ou partie d'un système informatique.

Article 129 :

Chaque Etat Membre l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait d'entraver, fausser ou aura tenter d'entraver ou de fausser le fonctionnement d'un système informatique.

Article 130 :

Chaque Etat Membre l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait d'introduire ou tenter d'introduire frauduleusement des données dans un système informatique.

Article 131 :

Chaque Etat Membre l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait d'intercepter ou tenter d'intercepter frauduleusement par des moyens techniques des données informatisées lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique.

Article 132 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait 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.

Article 133 :

Les États membres devront adopter les règles qui imposent aux vendeurs de produits TIC de faire réaliser, par des experts et des chercheurs en sécurité informatique indépendants, un essai de vulnérabilité et une évaluation de la garantie de sécurité, et de divulguer aux consommateurs toutes les vulnérabilités décelées dans les produits ainsi que les solutions recommandées pour y remédier.

Section II : Atteintes aux données informatisées

Article 134 :

Chaque Etat Membre l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait de produire ou de fabriquer un ensemble de données numérisées par l'introduction, l'effacement ou la suppression frauduleuse de données informatisées stockées, traitées ou transmises par un système informatique, engendrant des données contrefaites, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient originales.

Article 135 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait, en connaissance de cause, de faire usage des données obtenues.

Article 136 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait d'obtenir frauduleusement, pour soi-même ou pour autrui, un avantage quelconque, par l'introduction, l'altération, l'effacement ou la suppression de données informatisées ou par toute forme d'atteinte au fonctionnement d'un système informatique.

Article 137 :

Chaque Etat Membre l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait, même par négligence, de procéder ou faire procéder à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre prévues par la loi sur les données personnelle prévue à cet effet dans chaque Etat Membre.

Article 138 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait de produire, vendre, importer, détenir, diffuser, offrir, céder ou mettre à disposition un équipement, un programme informatique, tout dispositif ou donnée conçue ou spécialement adaptée pour commettre des infractions ou un mot de passe, un code d'accès ou des données informatisées similaires permettant d'accéder à tout ou partie d'un système informatique.

Article 139 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait de participer à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues dans la présente convention.

Section III : Infractions se rapportant au contenu

Article 140 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait de produire, enregistrer, offrir, de mettre à disposition, de diffuser, de transmettre une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique.

Article 141 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait de procurer ou de procurer à autrui, d'importer ou de faire importer, d'exporter ou de faire exporter une image ou une représentation présentant un caractère de pornographie infantile par le biais d'un système informatique.

Article 142 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait de posséder une image ou une représentation présentant un caractère de pornographie infantile dans un système informatique ou dans un moyen quelconque de stockage de données informatisées.

Article 143 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait de faciliter l'accès à des images, des documents, du son ou une représentation présentant un caractère de pornographie à un mineur.

Article 144 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale les infractions prévues par la présente Convention, lorsqu'elles ont été commises en bande organisée, seront punies du maximum de la peine prévue à l'infraction concernée.

Article 145 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait de créer, télécharger, diffuser ou de mettre à disposition sous quelque forme que ce soit des écrits, messages, photos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste ou xénophobe, par le biais d'un système informatique.

Article 146 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale, la menace commise par le biais d'un système informatique, de commettre une infraction pénale, envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques.

Article 147 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale l'insulte commise par le biais d'un système informatique envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion ou l'opinion politique dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques.

Article 148 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en infraction pénale le fait intentionnel de nier, d'approuver ou de justifier des actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système informatique.

Article 149 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires pour faire en sorte qu'en cas de condamnation, que le tribunal puisse prononcer la confiscation des matériels équipements, instruments, programmes informatiques ou tous dispositifs ou données appartenant au condamné et ayant servi à commettre les infractions.

Section III : Infractions se rapportant aux mesures de sécurisation des échanges électroniques

Article 150 :

Chaque État membre devra adopter les mesures législatives qu'il jugera efficaces en considérant comme infractions criminelles substantielles des actes qui affectent la confidentialité, l'intégrité, la disponibilité et la survivance des systèmes TIC et des infrastructures réseau sous-jacentes, ainsi que les mesures procédurales qu'il jugera efficaces pour rechercher et poursuivre les contrevenants. Les États membres sont invités à prendre en considération le choix du langage approuvé dans les modèles mondiaux de législations de cybercriminalité tel que celui adopté par le Conseil de l'Europe et le Commonwealth des Nations s'il y a lieu.

Article 151 :

Chaque Etat membre de l'Union Africaine doit prendre les mesures législatives nécessaires pour faire en sorte que l'écrit électronique en matière pénale est admis à établir les infractions à la loi pénale sous réserve qu'il soit apporté au cours des débats et discuté devant le juge et 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.

Chapitre II : L'adaptation de certaines infractions aux Technologies de l'Information et de la Communication.

Section Première : Atteintes aux biens

Article 152 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger en circonstance aggravante l'utilisation des TIC en vue de commettre des infractions de droit commun, comme le vol, l'escroquerie, le recel, l'abus de confiance, l'extorsion de fonds, le terrorisme, le blanchiment de capitaux notamment.

Article 153 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'ériger infraction les atteintes juridiques aux biens, à savoir le vol, l'escroquerie, le recel, l'abus de confiance, l'extorsion de fonds, le chantage portant sur les données informatiques.

Article 154 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'inclure expressément « les moyens de communication numérique par voie électronique » à l'image d'Internet dans l'énumération des moyens de diffusion publique prévus dans leurs textes pénaux.

Article 155 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires en vue d'intégrer expressément les nouveaux supports immatériels que sont les « données numérisées » ou les « fichiers informatisés » qui doivent être tenus secrets dans l'intérêt de la défense nationale.

Section II : Responsabilité pénale

Article 156 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures législatives nécessaires pour faire en sorte que les personnes morales autres que l'Etat, les collectivités locales et les établissements publics puissent être tenues pour responsables des infractions prévues par le présente Convention, commises pour leur compte par leurs organes ou représentants. La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

Article 157 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures des mesures législatives nécessaires en vue de soumettre les infractions de presse commises par le biais du réseau Internet, à l'exception de celles commises par la presse sur Internet, au régime de la responsabilité de droit commun de la responsabilité pénale.

Chapitre III : L'adaptation de certaines sanctions aux Technologies de l'Information et de la Communication

Section Première : Sanctions pénales

Article 158 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures nécessaires pour faire en sorte que les infractions prévues par la présente Convention soient passibles de sanctions pénales effectives, proportionnées et dissuasives.

Article 159 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures nécessaires pour faire en sorte que les infractions prévues par la présente Convention soient passibles d'une peine d'emprisonnement maximale d'au moins un (1) à cinq (5) ans.

Article 160 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures nécessaires pour faire en sorte qu'une personne morale déclarée responsable au sens de la présente Convention, soit passible de peines effectives, proportionnées et dissuasives, qui comprennent des amendes pénales et non pénales.

Section II : Autres sanctions pénales

Article 161 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures nécessaires pour faire en sorte qu'en cas de condamnation pour une infraction commise par le biais d'un support de communication numérique, la juridiction d'instruction ou de jugement saisie puisse prononcer à titre de peines complémentaires.

Article 162 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures nécessaires pour ériger en infraction pénale, la violation des interdictions ci-dessus prononcées par le juge.

Article 163 :

Chaque Etat Membre de l'Union Africaine doit prendre les mesures nécessaires pour faire en sorte qu'en cas de condamnation pour une infraction commise par le biais d'un support de communication numérique, le juge puisse ordonner à titre complémentaire obligatoire la diffusion au frais du condamné, par extrait, de la décision sur ce même support, et selon des modalités précisées dans les législations des Etats Membres.

Titre III : Droit procédural

Article 164 :

Chaque Etat membre de l'Union Africaine doit prendre les mesures nécessaires pour faire en sorte que lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire des Etats Membres, sont utiles à la manifestation de la vérité, le juge d'instruction puisse opérer une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

Article 165 :

Chaque Etat membre de l'Union Africaine doit prendre les mesures nécessaires pour faire en sorte que lorsque le juge d'instruction découvre dans un système informatique des données stockées qui sont utiles pour la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ces données, de même que celles qui sont nécessaires pour les comprendre, soient copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés, selon des modalités prévues dans les législations des Etats Membres.

Article 166 :

Chaque Etat membre de l'Union Africaine doit prendre les mesures nécessaires pour faire en sorte que les officiers de police judiciaire puissent, pour les nécessités de l'enquête ou de l'exécution d'une délégation judiciaire, procéder aux opérations prévues par la présente Convention .

Titre IV : Les infractions propres aux technologies de l'information et de la communication

Article 170 :

Chaque Etat membre de l'Union Africaine doit prendre les mesures nécessaires pour faire en sorte que si les nécessités de l'information l'exigent, notamment lorsqu'il y a des raisons de penser que des données informatisées archivées dans un système informatique sont particulièrement susceptibles de perte ou de modification, le juge d'instruction puisse faire injonction à toute personne de conserver et de protéger l'intégrité des données en sa possession ou sous son contrôle, pendant une durée de deux ans maximum, pour la bonne marche des investigations judiciaires. Le gardien des données ou une toute autre personne chargée de conserver celles-ci est tenu d'en garder le secret.

Article 171 :

Chaque Etat membre de l'Union Africaine doit prendre les mesures législatives nécessaires pour faire en sorte que la violation du secret soit punie des peines applicables au délit de violation du secret professionnel.

Article 172 :

Chaque Etat membre de l'Union Africaine doit prendre les mesures nécessaires pour faire en sorte que si les nécessités de l'information l'exigent le juge d'instruction puisse utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique ou obliger un fournisseur de services, dans le cadre de ses capacités techniques à collecter ou à enregistrer, en application de moyens techniques existant sur son territoire des Etats Parties, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées.

PARTIE IV - DISPOSITIONS COMMUNES ET FINALES

TITRE 1 - Mécanisme de suivi

Article 173 :

1. Il est créé un Comité consultatif sur la cybersécurité au sein de l'Union africaine.

2. Le Comité est composé de onze (11) membres élus par le Conseil exécutif, à partir d'une liste d'experts réputés pour leur grande intégrité, leur impartialité et leur haute compétence dans les questions relatives à la cybersécurité, et proposés par les Etats parties. Pour l'élection des membres du Comité, le Conseil exécutif veille au respect de la représentation adéquate des femmes et à une représentation géographique équitable.

3. Les membres du Comité siègent à titre personnel.

4. Le mandat des membres du Comité est de deux (2) ans, renouvelable une fois.

5. Les fonctions du Comité sont de :

a. promouvoir et d'encourager sur le continent l'adoption et l'application de mesures de renforcement de la cybersécurité dans les téléservices et de lutte contre la cybercriminalité et les atteintes aux droits de la personne dans le cyberespace ;

b. rassembler des documents et des informations sur les besoins en cybersécurité ainsi que sur la nature et l'ampleur de la cybercriminalité et les atteintes aux droits de la personne dans le cyberespace ;

c. élaborer des méthodes pour analyser les besoins en cybersécurité ainsi que sur la nature et l'ampleur de la cybercriminalité et les atteintes aux droits de la personne dans le cyberespace et diffuser l'information, et sensibiliser l'opinion publique sur les effets négatifs de ces phénomènes ;

d. conseiller les gouvernements sur la manière de promouvoir la cybersécurité et de lutter contre le fléau de la cybercriminalité et les atteintes aux droits de la personne dans le cyberespace au niveau national ;

e. recueillir des informations et procéder à des analyses sur la conduite et le comportement délictueux des usagers des réseaux et des systèmes d'informations

opérant en Afrique, et diffuser ces informations auprès des autorités nationales compétentes ;

f. élaborer et promouvoir l'adoption de codes de conduite harmonisés à l'usage des agents publics en matière de cybersécurité ;

g. établir des partenariats avec la Commission et la Cour africaines des droits de l'homme et des peuples, la société civile africaine, les organisations gouvernementales, intergouvernementales et non gouvernementales, afin de faciliter le dialogue sur la lutte contre la cybercriminalité et les atteintes aux droits de la personne dans le cyberespace ;

h. faire régulièrement rapport au Conseil exécutif sur les progrès réalisés par chaque Etat partie dans l'application des dispositions de la présente Convention ;

i. s'acquitter de toute autre tâche relative à la cybercriminalité et les atteintes aux droits de la personne dans le cyberespace que peuvent lui confier les organes délibérants de l'Union africaine.

6. Le Comité adopte son propre règlement intérieur.

7. Les Etats parties communiquent au Comité, un an après l'entrée en vigueur de la présente Convention, les progrès réalisés dans sa mise en œuvre. Après quoi, chaque Etat partie, par ses procédures pertinentes, veille à ce que les autorités ou les agences nationales chargées de la lutte contre cybercriminalité et les atteintes aux droits de la personne dans le cyberespace , fasse rapport au Comité au moins une fois par an, avant les sessions ordinaires des organes délibérants de l'UA.

TITRE 2 - DISPOSITIONS FINALES

Article 171 :

1. La présente Convention est ouverte à la signature, ratification, ou adhésion par les Etats membres de l'Union africaine.

2. La présente Convention entre en vigueur trente (30) jours après la date du dépôt du quinzième instrument de ratification ou d'adhésion.

3. Pour chaque Etat partie qui ratifie ou adhère à la présente Convention après la date du dépôt du quinzième instrument de ratification, la Convention entre en vigueur trente (30) jours après la date du dépôt, par cet Etat partie de son instrument de ratification ou d'adhésion.

Article 172 :

1. Tout Etat partie peut, au moment de l'adoption, de la signature, de la ratification ou de l'adhésion, émettre des réserves sur la présente Convention, à condition que chaque réserve concerne une ou plusieurs dispositions spécifiques et ne soit pas incompatible avec l'objet et les fins de la présente Convention.

2. Tout Etat partie ayant émis une réserve la retire dès que les circonstances le permettent. Le retrait se fait par notification adressé au Président de la Commission.

Article 173 :

1. La présente Convention peut être amendée à la demande d'un Etat partie qui adresse par écrit, à cet effet, une requête au Président de la Commission.

2. Le Président de la Commission communique la proposition d'amendement à tous les Etats parties qui ne l'examinent que six (6) mois après la date de communication de la proposition.

3. L'amendement entre en vigueur après son approbation par la majorité des deux tiers des Etats membres de l'Union africaine.

Article 174 :

1. Tout Etat partie peut dénoncer la présente Convention en notifiant par écrit le Président de la Commission. Cette dénonciation prend effet six (6) mois après la date de réception de la notification par le Président de la Commission.

Article 175 :

1. Le Président de la Commission est le dépositaire de la présente Convention et de ses amendements.

2. Le Président de la Commission informe tous les Etats parties de l'état de signature, de ratification et d'adhésion, ainsi que de l'entrée en vigueur, des requêtes d'amendement introduites par les Etats, de l'approbation des propositions d'amendement, et des dénonciations.

3. Dès l'entrée en vigueur de la présente Convention, le Président de la Commission l'enregistre auprès du Secrétaire général des Nations unies, conformément à l'article 102 de la Charte des Nations unies.

Article 176 :

La présente Convention établie en quatre originaux en arabe, en anglais, en français et en portugais, les quatre textes faisant également foi, est déposée auprès du Président de la Commission.

EN FOI DE QUOI, NOUS, Chefs d'Etat et de gouvernement de l'Union africaine, ou nos représentants dûment autorisés, avons adopté la présente Convention.

Adopté par la XX session ordinaire de la Conférence de l'Union à (lieu), le (date)