Loi n°43-2020 du 20 août 2020 autorisant la ratification de la convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel

L'Assemblée nationale et le Sénat
ont délibéré et adopté ;

Le Président de la République promulgue la loi
dont la teneur suit :

Article premier : Est autorisée la ratification de la convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, dont le texte est annexé à la présente loi.

Article 2 : La présente loi sera publiée au Journal officiel et exécutée comme loi de l'Etat.

Fait à Brazzaville, le 20 août 2020

Par le Président de la République,

Denis SASSOU-N'GUESSO

Le premier ministre, chef du Gouvernement,

Clément MOUAMBA

Le ministre des affaires étrangères, de la coopération et des Congolais de l'étranger,

Jean-Claude GAKOSSO

Le ministre des postes, des télécommunications et de l'économie numérique,

Léon Juste IMBOMBO

CONVENTION DE L'UNION AFRICAINE SUR LA CYBERSECURITE ET LA PROTECTION DES DONNEES A CARACTÈRE PERSONNEL

PREAMBULE

Les Etats membres de l'Union africaine

Guidés par l'Acte Constitutif de l'Union africaine adopté en 2000 ;

Considérant que la présente Convention portant création d'un Cadre juridique sur la cybersécurité et la protection des données à caractère personnel définit les engagements des Etats membres de l'Union africaine aux niveaux sous régional, régional et international en vue de l'édification de la Société de l'Information ;

Rappelant qu'elle 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 économiques régionales (CER) en matière de Technologies de l'information et de la communication ;

Réaffirmant l'attachement des Etats membres aux libertés fondamentales et aux droits de l'Homme et des peuples contenus dans les déclarations, conventions et autres instruments adoptés dans le cadre de l'Union africaine et de l'Organisation des Nations Unies ;

Considérant que la mise en place d'un cadre réglementaire sur la cybersécurité et la protection des données à caractère personnel tient compte des critères de respect des droits des citoyens, garantis en vertu des textes fondamentaux de droit interne et protégés par les Conventions et Traités internationaux relatifs aux droits de l'Homme particulièrement la Charte africaine des droits de l'Homme et des Peuples ;

Soucieux de la nécessité de mobiliser l'ensemble des acteurs public et privés (Etats, collectivité locales, entreprises du secteur privé, organisations de la société civile, médias, institutions de formation et de recherche, etc.) en faveur de la cybersécurité ;

Réitérant les 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 en vue de répondre aux immenses attentes 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 crédible pour les transactions électroniques, la protection des données à caractère personnel et la lutte contre la cybercriminalité ;

Ayant à l'esprit que les principaux défis au développement du commerce électronique en Afrique sont liés à des problèmes de sécurité dont

notamment :

a) les lacunes qui affectent la réglementation en matière de reconnaissance

juridique des communications de données et de la signature électronique ;

b) l'absence de règles juridiques spécifiques protectrices des consommateurs des droits de propriété intellectuelle, des données à caractère personnel et des systèmes d'information ;

c) l'absence de législations relatives aux téléservices et au télétravail ;

d) l'application des techniques électroniques aux actes commerciaux et administratifs ;

e) les éléments probants introduits par les techniques numériques (horodatage, certification, etc.) ;

f) les règles applicables aux moyens et prestations de cryptologie ;

g) l'encadrement de la publicité en ligne ;

h) l'absence de législation fiscales et douanières appropriées au commerce électronique.

Convaincus que le constat ci-dessus justifie l'appel à la mise en place d'un cadre normatif approprié conforme à l'environnement juridique, culturel, économique et social africain, et que l'objet de la présente convention est donc d'assurer la sécurité et le cadre juridique nécessaires à l'émergence de l'économie du savoir en Afrique ;

Soulignant que sur un autre plan, la protection des données à caractère personnel ainsi que de la vie privée se présente comme un enjeu majeur de la Société de l'information, tant pour les pouvoir publics que pour les autres parties prenantes et que cette protection nécessite un équilibre entre l'usage des technologies de l'information et de la communication et la protection de la vie privée des citoyens dans leur vie quotidienne ou professionnelle tout en garantissant la libre circulation des informations ;

Préoccupés par l'urgence de la mise en place d'un dispositif permettant de faire face aux dangers et risques nés de l'utilisation des données électroniques 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 Etats membres de l'Union africaine ;

Considérant que le but de la présente Convention est de répondre aux besoins de législation harmonisée dans le domaine de la cybersécurité dans les Etats membres de l'Union africaine et de mettre en place, dans chaque Etat partie, un mécanisme 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 ; 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 ainsi que les meilleures pratiques reconnues au niveau international ;

Considérant que la protection pénale du système de valeurs de la Société de l'Information s'impose comme une nécessité dictée par des motifs 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 au niveau actuel 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 Etats membres de l'Union africaine, en prenant en compte leurs engagements actuels aux niveaux 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, pour adoption, d'incriminations nouvelles spécifiques aux TIC, et l'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, la Convention définit, le cadre de l'aménagement de la procédure classique concernant les technologies de l"information et de la communication et précise les conditions de l'institution de procédures spécifique à la cybercriminalité ;

Rappelant la décision Assembly/AU/Decl.1(XIU) de la quatorzième session ordinaire de la Conférence des chefs d'Etat et de gouvernement de l'Union africaine sur les technologies de l'information et de la communication en Afrique ; défis et perspectives pour le développement, tenue à Addis-Abeba (Ethiopie) du 31 janvier au 2 février 2010 ;

Tenant compte de la Déclaration d'Oliver Tambo adoptée par la Conférence de l'Union africaine des ministres en charge de la Communication et des Technologies de l'Information à Johannesburg (Afrique du Sud), le 05 novembre 2009 ;

Rappelant les dispositions de la Déclaration d'Abidjan adoptée le 22 février 2012 et la Déclaration d'Addis- Abeba adoptée le 22 juin 2012 sur l'harmonisation des Cyber-législations en Afrique.

Sont convenus de ce qui suit :

Article premier
Définitions

Aux fins de la présente Convention, on entend par :

« UA », l'Union africaine ;

« Code de conduite », ensemble des règles élaborées par le responsable du traitement afin d'instaurer un usage correct des ressources informatiques, des réseaux et des communications électroniques de la structure concernée et homologué par l'autorité des protections ;

« Commission », la Commission de l'Union africaine ;

« Communication avec le public par voie électronique », toute transmission au public ou d'une catégorie de publie, par un procédé de communication électronique ou magnétique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature ;

« la présente Convention », la Convention de l'union africaine sur la Cybersécurité de la protection des données à caractère personnel ;

« Conventions secrètes », 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 ;

« Communication électronique indirecte », tout message de texte, de voix, de son, d'image envoyé via un réseau de communication électronique et stocké sur le réseau ou sur un terminal de communication jusqu'à réception dudit message ;

« 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.

« Cryptologie », la science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation ;

« Moyens de Cryptologie », l'ensemble des outils scientifiques et techniques (matériel ou logiciel) qui permettent de chiffrer et/ou de déchiffrer ;

« Services de cryptologie », toute opération visant à mettre en place des moyens de cryptologie en son nom propre ou en celui d'une autre personne ;

« Activité de Cryptologie », toute activité ayant pour but la production, l'utilisation, l'importation, l'exportation ou la commercialisation des moyens de cryptologie ;

« Dépasser un accès autorisé », le fait d'accéder à un système d'information et d'utiliser un tel accès pour obtenir ou modifier des données dans une partie de l'ordinateur ou le titulaire n'est pas autorisé d'y accéder ;

« Destinataire d'un traitement des données à caractère personnel », 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 ;

« Dispositif de création de signature électronique », ensemble d'éléments logiciels ou matériels permettant la création d'une signature électronique ;

« Dispositif de vérification de signature électronique », ensemble d'éléments logiciels ou matériels permettant la vérification d'une signature électronique.

« Dommage », toute atteinte à l'intégrité ou à la disponibilité des données, d'un programme, d'un système ou d'une information.

« Données à caractère personnel », toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, mentale, économique, culturelle et sociale, « Données informatisées », toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique ;

« Données sensibles », toutes les données à caractère personnel relatives aux opinions ou activités religieuses, philosophiques, politiques, syndicales, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives ;

« Données dans le domaine de la santé », toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques précitées ;

« Double criminalité », une infraction punie à la fois dans l'Etat où un suspect est détenu et un Etat demandant que le suspect soit remis ou transféré ;

« Etat membre (ou Etats membres) », le (les) Etat(s) Membre(s) de l'Union Africaine ;

« Etat partie (ou Etats parties) », Etat membre (ou les Etats membres) qui a (ont) ratifié ou accédé à la présente Convention ;

« Fichier de données à caractère personnel », tout ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;

« Information », 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, ou autre ;

« Infrastructure critique de TIC/Cyberespace », Infrastructure TIC/cyber qui est essentielle aux services vitaux pour la sureté publique, la stabilité économique, la sécurité nationale, la stabilité internationale et pour la pérennité et la restauration du cyberespace critique ;

« Interconnexion des données à caractère personnel », 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 ;

« Mineur ou Enfant », toute personne physique âgée de moins de 18 ans au sens de la Charte Africaine sur les droits et le bien-être de l'Enfant et de la convention des Nations Unies sur les droits de l'enfant ;

« Moyen de paiement électronique », moyen permettant à son titulaire d'effectuer des opérations de paiement électroniques en ligne ;

« Pornographie infantile », toute représentation visuelle d'un comportement sexuellement explicite y compris toute photographie, film, vidéo, image que ce soit fabriquée ou produite par voie électronique, mécanique ou par autres moyens où :

(a) la production de telles représentations visuelles implique un mineur ;

(b) ces représentations visuelles sont une image numérique, une image d'un ordinateur ou une image générée par un ordinateur où un mineur est engagé dans un comportement sexuellement explicite ou lorsque des images de leurs organes sexuels sont produites ou utilisées à des fins principalement sexuelles et exploitées à l'insu de l'enfant ou non ;

(c) cette représentation visuelle a été créée, adaptée ou modifiée pour qu'un mineur engage dans un comportement sexuellement explicite.

« Prestataire de services de cryptologie », toute personne, physique ou morale, qui fournit une prestation de cryptologie ;

« Personne concernée », toute personne physique qui fait l'objet d'un traitement des données à caractère personnel ;

« Prospection directe », tout envoi de message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ; elle vise aussi 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 ;

« Raciste et xénophobe en matière des technologies de l'information et de la communication », tout matériel 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 ;

« Responsable du traitement », toute 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 ;

« Signature électronique », une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de procédé d'identification ;

« Sous-traitant », toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données pour le compte du responsable du traitement ;

« Système informatique », tout dispositif électronique, magnétique, optique, électrochimique ou tout autre dispositif de haut débit isolé ou interconnecté qui per- forme la fonction de stockage de données ou l'installation de communications. Ces communications sont directement liées à ou fonctionnent en association avec d'autre(s) dispositif(s) ;

« Tiers », 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 ;

« Traitement des données à caractère personnel », 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.

CHAPITRE I : LES TRANSACTIONS ELECTRONIQUES

Section I : Le Commerce Electronique

Article 2 : Champ d'application du commerce électronique

1. Les Etats membres veillent à ce que l'activité de commerce électronique s'exerce librement dans tous les Etats parties qui ratifient ou adhèrent à la présente Convention à l'exclusion des domaines suivants :

a) les jeux d'argent, mêmes sous forme de paris et de loteries, légalement autorisés ;

b) les activités de représentation et d'assistance en justice ;

c) les activités exercées par les notaires ou les autorités équivalentes en application des textes en vigueur.

2. Sans préjudice des autres obligations d'information prévues par les textes législatifs et réglementaires en vigueur dans les Etats membres de l'Union Africaine, les Etats Parties veillent à ce que toute personne qui exerce le commerce électronique est tenue d'assurer à ceux à qui est destinée la fourniture des biens ou la prestation de services un accès facile, direct et permanent utilisant un standard ouvert aux informations suivantes :

a) s'il s'agit d'une personne physique, le prestataire doit indiquer ses nom et prénom et, s'il s'agit d'une personne morale, sa raison sociale ; son capital, son numéro d'inscription au registre des sociétés ou association ;

b) l'adresse complète de l'endroit où elle est établie, son adresse de courrier électronique, ainsi que son numéro de téléphone ;

c) 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 ;

d) si elle est assujettie aux taxes, le numéro d'identification fiscal ;

e) si son activité est soumise à un régime d'autorisation, le nom et l'adresse de l'autorité ayant délivré celle-ci ainsi que la référence de l'autorisation ;

f) si elle est membre d'une profession réglementée, la référence aux règles professionnelles applicables, son titre professionnel, l'Etat 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.

3. Toute personne physique ou morale qui exerce l'activité de commerce électronique 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 le prix inclut les taxes, les frais de livraison et autres charges.

Article 3 : La responsabilité contractuelle du fournisseur de biens ou de services électroniques

L'activité de commerce électronique est soumise à la loi de l'Etat partie 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.

Article 4 : Publicité par voie électronique

1. Sans préjudice de l'article 3, 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.

2. 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.

3. Les Etats parties de l'Union Africaine s'engagent à interdire la prospection directe via n'importe quelle forme de communication indirecte 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.

4. Nonobstant les dispositions de l'Article 4.2, la prospection directe par courrier électronique est autorisée si :

a) les coordonnées du destinataire ont été recueillies directement auprès de lui ;

b) le destinataire ayant donné son consentement au prospecteur d'être contacté par ses partenaires ;

c) la prospection directe concerne des produits ou services analogues fournis par la même personne physique ou morale.

5. Les Etats Parties s'engagent à interdire l'émission, à des fins de prospection directe, des messages via n'importe quelle forme de communication indirecte, 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.

6. Les Etats Parties s'engagent à interdire la dissimulation de l'identité de la personne pour le compte de laquelle la publicité accessible par un service de communication en ligne est émise.

Section II : Les obligations conventionnelles sous forme électronique

Article 5 : Les contrats électroniques

1. 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 leurs destinataires ont accepté l'usage de ce moyen. L'utilisation des communications électroniques est présumée recevable sauf si le bénéficiaire a déjà exprimé sa préférence pour un autre moyen de communication.

2. 2. 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 directement ou indirectement, d'une manière qui permette leur conservation et leur reproduction conformément aux législations nationales.

3. 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.

4. La personne qui offre ses produits et services 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.

5. Il peut être dérogé aux dispositions des Articles 5.3 et 5.4 de la présente Convention dans les conventions conclues entre professionnels (B2B).

6. a. Toute personne physique ou morale exerçant l'activité définie au premier alinéa de l'Article 2.1 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.

b. 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 6 : L'écrit sous forme électronique

1. Sans préjudice des dispositions légales en vigueur dans l'Etat Partie, nul ne peut être contraint de poser un acte juridique par voie électronique.

a. Lorsqu'un écrit est exigé pour la validité d'un acte juridique, chaque Etat Partie membre établit les conditions légales pour l'équivalence fonctionnelle entre les communications électroniques et les versions papiers, lorsque la réglementation interne en vigueur exige un écrit pour la validité d'un acte juridique ;

b. 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 ;

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

2. Il est fait exception aux dispositions de l'Article 6.2 de la présente Convention pour :

a) les actes sous seing privé relatifs au droit de la famille et des successions ; et

b) les actes sous seing privé relatifs à des sûretés personnelles ou réelles, de nature civile ou commerciale en conformité avec les législations nationales, sauf s'ils sont passés par une personne pour les besoins de sa profession ;

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

4. Eu égard à leurs fonctions fiscales, les factures doivent faire l'objet d'un écrit permettant d'assurer la lisibilité, l'intégrité et la pérennité du contenu. L'authenticité de l'origine doit également être garantie.

Parmi les méthodes susceptibles d'être mises en œuvre pour atteindre les finalités fiscales de la facture et assurer que ses fonctions ont été satisfaites figure la réalisation de contrôles de gestion qui établiraient une piste d'audit fiable entre une facture et une livraison de biens ou de services.

Outre le type de contrôles de gestion décrits au § 1er, les méthodes suivantes constituent des exemples de technologies permettant d'assurer l'authenticité de l'origine et l'intégrité du contenu d'une facture électronique :

a. une signature électronique qualifiée, telle que définie à l'article 1 ;

b. un échange de données informatisées (EDI), compris comme le transfert électronique, d'un ordinateur à un autre, de données commerciales et administratives sous la forme d'un message EDI structuré conformément à une norme agréée, pour autant que l'accord relatif à cet échange prévoie l'utilisation de procédures garantissant l'authenticité de l'origine et l'intégrité des données.

5. Un document 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.

Section III : La sécurisation des transactions électroniques

Article 7 : Assurer la sécurité des transactions électroniques

1. a. Le fournisseur doit permettre à ces clients d'effectuer leurs paiements en utilisant un moyen de paiement électronique approuvé par l'Etat selon la réglementation en vigueur de chaque Etat Partie ;

b. 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 libéré, doit prouver que l'obligation est inexistante ou éteinte.

2. Lorsque les dispositions légales des pays membres n'ont pas fixé 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 possibles le titre le plus vraisemblable, quel qu'en soit le support.

3. a. 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 de l'Etat

Partie ;

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

4. a. 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 ;

b. 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.

CHAPITRE II : LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Section I : La protection des données à caractère personnel

Article 8 : L'objet de la présente Convention sur les données à caractère personnel

1. Chaque Etat partie s'engage à mettre en place un cadre juridique ayant pour objet de renforcer les droits fondamentaux et les libertés publiques, notamment la protection des données physiques et de réprimer toute infraction relative à toute atteinte à la vie privée sans préjudice du principe de la liberté de circulation des données à caractère personnel.

2. 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 buts pour lesquels les entreprises ont été créées.

Article 9 : Le champ d'application de la Convention

1. Sont soumises à la présente Convention les actions suivantes :

a) Toute collecte, tout traitement, toute transmission, tout stockage ou toute utilisation des données à caractère personnel effectués par une personne physique, par l'Etat, les collectivités locales, les personnes morales de droit public ou de droit privé ;

b) Tout traitement automatisé ou non de données contenues ou appelées à figurer dans un fichier, à l'exception des traitements mentionnés à l'Article 9.2 de la présente Convention ;

c) Tout traitement mis en œuvre sur le territoire d'un Etat Partie de l'Union Africaine ;

d) 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.

2. La présente Convention ne s'applique pas :

(a) 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 ;
(b) aux copies temporaires faites dans le cadre des ac- tivités 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.

Article 10 : Les formalités préalables à la mise en œuvre des traitements des données à caractère personnel

1. Sont dispensés des formalités préalables :

a) les traitements mentionnés à l'Article 9.2 de la présente Convention ;

b) les traitements ayant pour seul objet la tenue d'un registre qui est destiné à un usage exclusivement privé ;

c) 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.

2. En dehors des cas prévus à l'Article 10.1 ci-dessus et aux Articles 10.4 et 10.5 de la présente Convention, les traitements de données à caractère personnel font l'objet d'une déclaration auprès de l'autorité de protection.

3. 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 nationale de protection établit et publie des normes destinées à simplifier ou à exonérer l'obligation de déclaration.

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

a) les traitements des données à caractère personnel portant sur des données génétiques et sur la recherche dans le domaine de la santé ;

b) les traitements des données à caractère personnel portant sur des données relatives aux infractions, condamnations ou mesures de sûreté ;

c) les traitements des données à caractère personnel ayant pour objet une interconnexion de fichiers, telle que définie à l'Article 15 de la présente Convention les traitements portant sur un numéro national d'identification ou tout autre identifiant de la même nature ;

b) aux copies temporaires faites dans le cadre des ac-

d) les traitements des données à caractère personnel comportant des données biométriques ;

e) les traitements des données à caractère personnel ayant un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques.

5. 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 nationale de protection. Ces traitements portent sur :

a) la sûreté de l'Etat, la défense ou la sécurité publique ;

b) la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;

c) le recensement de la population ;

d) 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.

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

a) 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 ;

b) la ou les finalités du traitement ainsi que la description générale de ses fonctions ;

c) les interconnexions envisagées ou toutes autres formes de mise en relation avec d'autres traitements ;

d) les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;

e) la durée de conservation des données traitées ;

f) 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 ;

g) les destinataires habilités à recevoir communication des données ;

h) la fonction de la personne ou le service auprès duquel s'exerce le droit d'accès ;

i) les dispositions prises pour assurer la sécurité des traitements et des données ;

j) l'indication du recours à un sous-traitant ;

k) les transferts de données à caractère personnel envisagés à destination d'un pays tiers non membre de l'Union Africaine, sous réserve de réciprocité.

7. L'autorité nationale 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 nationale de protection.

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

9. L'autorité nationale 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.

Section II : Le cadre institutionnel de la protection des données à caractère personnel

Article 11 : Statut, composition et organisation des autorités nationales de protection des données à caractère personnel

1. a. Chaque Etat Partie s'engage à mettre en place une autorité chargée de la protection des données à caractère personnel.

b. L'autorité nationale 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.

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

3. Sans préjudice aux dispositions de l'article 11.6, chaque Etat Partie détermine la composition de l'autorité nationale chargée de la protection des données à caractère personnel.

4. Des agents assermentés, conformément aux dispositions en vigueur dans les Etats parties, peuvent être appelés à participer à la mise en œuvre des missions de vérification. .

5. a. Les membres de l'autorité nationale de protection sont soumis au secret professionnel conformément aux textes en vigueur dans chaque Etat partie.

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

6. La qualité de membre d'une autorité nationale 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 des technologies de l'information et de la communication.

7. a. Sans préjudice des législations nationales, les membres des autorités nationales de protection jouissent d'une immunité totale pour les opinions émises dans l'exercice ou à l'occasion de l'exercice de leur fonction.

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

8. Les Etats parties s'engagent à doter les autorités nationales de protection des moyens humains, techniques et financiers nécessaires à l'accomplissement de leur mission.

Article 12 : Attributions des autorités nationales de protection

1. Les autorités nationales de protection sont chargées de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente Convention dans les Etats parties de l'Union africaine.

2. Les autorités nationales de protection s'assurent que les Technologies de l'Information et de la Communication ne comportent pas de menace au regard des libertés publiques et de la vie privée des citoyens. A ce titre, elles sont chargées de :

a) répondre à toute demande d'avis portant sur un traitement de données à caractère personnel ;

b) informer les personnes concernées et les responsables de traitement de leurs droits et obligations ;

c) autoriser les traitements de fichiers dans un certain nombre de cas, notamment les fichiers sensibles ;

d) recevoir les formalités préalables à la création de traitements des données à caractère personnel ;

e) 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 ;

f) informer sans délai l'autorité judiciaire pour certains types d'infractions dont elles ont connaissance ;

g) procéder, par le biais de son personnel ou autre expert requis, à des vérifications portant sur tout traitement des données à caractère personnel;

h) prononcer des sanctions, administratives et pécuniaires, à l'égard des responsables de traitement ;

i) mettre à jour un répertoire des traitements des données à caractère personnel et à la disposition du public ;

j) 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 ;

k) autoriser les transferts transfrontaliers de données à caractère personnel ;

l) faire des suggestions susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données ;

m) mettre en place des mécanismes de coopération avec les autorités de protection des données à caractère personnel de pays tiers ;

n) participer aux négociations internationales en matière de protection des données à caractère personnel ;

o) o) établir, selon une périodicité bien définie, un rapport d'activités remis aux autorités compétentes de l'Etat Partie.

3. Les autorités nationales de protection peuvent prononcer les mesures suivantes :

a) un avertissement à l'égard du responsable du traitement ne respectant pas les obligations découlant de la présente Convention ;

b) une lettre d'avertissement pour faire cesser les manquements concernés dans le délai qu'elle fixe.

4. Si le responsable du traitement ne se conforme pas à la lettre d'avertissement qui lui a été adressée, les autorités nationales de protection peuvent prononcer à son encontre, après procédure contradictoire, les sanctions suivantes :

a) un retrait provisoire de l'autorisation accordée ;

b) le retrait définitif de l'autorisation ;

c) une amende pécuniaire.

5. 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 des libertés fondamentaux, les autorités nationales de protection, après procédure contradictoire, peuvent décider :

a) l'interruption de la mise en œuvre du traitement ;

b) le verrouillage de certaines données à caractère personnel traitées ;

c) l'interdiction temporaire ou définitive d'un traitement contraire aux dispositions de la présente Convention.

6. Les sanctions et décisions prises par les autorités nationales de protection sont susceptibles de faire l'objet d'un recours.

Section III : Les obligations relatives aux conditions de traitements de données à caractère personnel

Article 13 : Les principes de base gouvernant le traitement des données à caractère personnel

Principe 1 : Le principe de consentement et de légitimité du traitement des données à caractère personnel

1. 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 :

a) au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

b) 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 ;

c) à l'exécution d'un contrat auquel la personne concernée est partie ou, pour prendre des mesures, à la demande de la personne concernée, avant la conclusion du contrat ;

d) à la sauvegarde des intérêts vitaux ou des droits et libertés fondamentaux de la personne concernée.

Principe 2 : Le principe de la légitimité et de l'équité du traitement des données à caractère personnel

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.

Principe 3 : Le principe de finalité, de pertinence, de conservation des données à caractère personnel traitées

a) la collecte des données s'effectue pour des objectifs spécifiques, explicites et légitimes et ne sont pas traitées de manière incompatible avec ces objectifs ;

b) la collecte des données est adéquate, pertinente et non excessives en ce qui concerne les objectifs pour lesquels les données sont collectées et ensuite traitées ;

c) les données sont conservées pendant une durée qui n'excède pas la période nécessaire des objectifs pour lesquels elles ont été collectées ou traitées ;

d) au-delà de cette période requise, les données ne peuvent être conservées que pour les besoins spécifiques du traitement des données effectué pour des fins historiques, statistiques ou de recherches en vertu des dispositions légales.

Principe 4 : Le principe d'exactitude des données à caractère personnel

Les données collectées doivent être exactes et, si nécessaire, actualisées. Toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles ont été collectées et traitées ultérieurement, soient supprimées ou rectifiées.

Principe 5 : Le principe de transparence
des données à caractère personnel

Le principe de transparence implique la diffusion obligatoire de l'information par le responsable du traitement portant sur les données à caractère personnel.

Principe 6 : Le principe de confidentialité et de sécurité
des traitements de données à caractère personnel

a. les données à caractère personnel sont traitées de manière confidentielle et protégées, notamment lorsque le traitement comporte des transmissions de données dans un réseau ;

b. b. lorsque le traitement est mis en œuvre au nom du responsable du traitement, celui-ci choisit un sous- traitant qui apporte des garanties suffisantes. Il incombe au responsable du traitement ainsi qu'au sous-traitant d'assurer la conformité avec les mesures de sécurité définies dans la présente Convention.

Article 14 : Les principes spécifiques relatifs au traitement de données sensibles

1. Les Etats Parties s'engagent à interdire la collecte et 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.

2. L'interdiction visée à l'Article 14.1 ne s'applique pas aux catégories de traitement suivantes :

a) le traitement des données à caractère personnel porte sur des données manifestement rendues publiques par la personne concernée ;

b) 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 ;

c) 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 ;

d) le traitement, notamment des données génétiques, est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;

e) une procédure judiciaire ou une enquête pénale est ouverte ;

f) le traitement des données à caractère personnel s'avère nécessaire pour un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques ;

g) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à la prise de mesures à la demande de la personne concernée avant la conclusion du contrat ;

h) le traitement est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis ;

i) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou dans l'exercice d'une officielle autorité ou d'une fonction assignée par une autorité publique au responsable du traitement ou à un tiers, auquel les données sont communiquées ;

j) 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, coopérative ou syndicale et à condition que le traitement ne concerne que les membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés aux objectifs et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées.

3. Le traitement des données à caractère personnel réalisé aux fins 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 journalistique ou de recherche conformément aux règles déontologiques de ces professions.

4. Les dispositions de la présente Convention ne font pas obstacle à l'application des dispositions des législations nationales relatives à la presse écrite ou au secteur de l'audiovisuel ainsi qu'aux dispositions 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.

5. Aucune personne ne peut être concernée ni être soumise aux effets néfastes d'une décision qui a des effets juridiques et qui est basée uniquement sur un traitement automatisé des données à caractère personnel pour évaluer certains aspects de sa personnalité.

6. a. Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat membre non-Partie 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 dont les données font ou peuvent faire l'objet d'un traitement ;

b. La précédente interdiction ne s'applique pas lorsqu'avant tout transfert des données à caractère personnel vers ce pays tiers, le responsable du traitement sollicite l'autorisation de l'autorité nationale de protection.

Article 15 : L'interconnexion des fichiers comportant des données à caractère personnel

L'interconnexion des fichiers visée à l'Article 10.4 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 des personnes concernées et doivent être soumises aux mesures de sécurité appropriées et tenir compte du principe de pertinence des données faisant l'objet de l'interconnexion.

Section IV : Les droits de la personne concernée

Article 16 : Droit à l'information

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

a) son identité et, le cas échéant, celle de son représentant ;

b) les objectifs du traitement pour lesquels les données sont prévues ;

c) les catégories de données concernées ;

d) les destinataires auxquels les données pourraient être communiquées ;

e) la capacité à pouvoir demander leur suppression du fichier ;

f) l'existence d'un droit d'accès aux données et du droit de les rectifier ;

g) la durée de conservation des données ;

h) les transferts de données proposés aux pays tiers.

Article 17 : Droit d'accès

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

a) les informations permettant de connaître et de contester le traitement ;

b) la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de traitement ;

c) la communication des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;

d) des informations relatives à l'objectif du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées.

Article 18 : Droit d'opposition

Toute personne physique a le droit de s'opposer, pour des motifs légitimes, au traitement des données à caractère personnel la concernant.

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 à leur nom 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.

Article 19 : Droit de rectification et de suppression

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.

Section V : Les obligations du responsable de traitement de données à caractère personnel

Article 20 : Les obligations de confidentialité

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.

Article 21 : Les obligations de sécurité

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.

Article 22 : Les obligations de conservation

Les données à caractère personnel ne doivent pas être conservées au-delà de la période requise pour les fins en vue desquelles elles ont été recueillies et traitées.

Article 23 : Les obligations de pérennité

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

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

CHAPITRE III :

PROMOTION DE LA CYBERSECURITE ET LUTTE CONTRE LA CYBERCRIMINALITE

Section I : Mesures de Cybersécurité à prendre au niveau national

Article 24 : Cadre de la cybersécurité nationale

1. Politique nationale

Chaque Etat partie s'engage en collaboration avec les parties prenantes, à mettre en œuvre 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 les modalités de réalisation des objectifs de cette politique.

2. Stratégie nationale

Les Etats parties adoptent les stratégies qu'ils jugent appropriées et suffisantes pour mettre en œuvre la politique nationale de cyber sécurité, spécifiquement dans le domaine de la réforme législative et du développement, de la sensibilisation et du développement des capacités, du partenariat public- privé et de la coopération internationale, entre autres. Ces stratégies devront définir les structures organisationnelles, fixer des objectifs et les délais pour la mise en œuvre effective de la politique de cyber sécurité, tout en jetant les bases d'une gestion efficace des incidents de cybersécurité et de la coopération internationale.

Article 25 : Mesures légales

1. Législations contre la cybercriminalité

Chaque Etat partie adopte les mesures législatives et/ ou réglementaires qu'il jugera efficaces en considérant comme des actes d'infractions pénales importantes qui affectent la confidentialité, l'intégrité, la disponibilité et la

survie des systèmes technologies de l'information et de la communication et les données qu'ils traitent et les infrastructures de réseau essentielles, ainsi que les mesures procédurales qu'il juge efficaces pour rechercher et poursuivre les contrevenants. Les Etats parties prennent en considération le choix de la langue utilisée dans les meilleures pratiques internationales.

2. Les autorités réglementaires nationales

Chaque Etat partie adopte les mesures législatives et/ ou réglementaires qu'il juge nécessaires pour conférer la responsabilité spécifique aux institutions - qu'elles soient nouvellement créées ou déjà en place - ainsi qu'aux responsables désignés de ces institutions, afin de leur confier l'autorité statutaire et la capacité légale à agir dans tous les aspects de l'application de la cybersécurité, y compris entre autres, la réponse aux incidents et la coordination et la coopération en matière de justice réparatrice d'investigations scientifiques, la poursuite, etc.

3. Droits des citoyens

En adoptant des mesures législatives en matière de cybersécurité ou en mettant en place le cadre de mise en œuvre de celles-ci, chaque Etat partie veille à ce que les mesures adoptées ne violent pas les droits des citoyens garantis en vertu de la constitution nationale, des lois internes et protégés par les conventions internationales, particulièrement la Charte africaine des droits de l'Homme et des Peuples, ainsi que les droits fondamentaux 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.

4. Protection des infrastructures critiques

Chaque Etat partie adopte des mesures législatives et/ou réglementaires qu'il jugera nécessaires pour identifier les secteurs considérés comme sensibles pour sa sécurité nationale et le bien-être de l'économie ainsi que les systèmes technologies de l'information et de la communication conçus pour fonctionner dans ces secteurs comme des infrastructures critiques de l'information, en proposant à cet égard des sanctions plus sévères pour les activités criminelles sur les systèmes TIC dans ces secteurs ainsi que des mesures pour améliorer la vigilance, la sécurité et la gestion.

Article 26 : Système national de la cybersécurité

1. Culture de cybersécurité

a) Chaque Etat partie s'engage à promouvoir la culture de sécurité chez toutes les parties prenantes notamment les gouvernements, les entreprises et la société civile qui mettent au point, possèdent, gèrent, mettent en service et utilisent les systèmes et les réseaux d'information. La culture de cybersécurité 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 des communications ou des transactions à travers les réseaux.

b) Dans le cadre de la promotion de la culture de sécurité, les Etats parties peuvent adopter les mesures suivantes : mettre en place un plan de cybersécurité pour les systèmes gérés par leurs gouvernements ; élaborer 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 global pour les internautes, les petites entreprises, les écoles et les enfants.

2. Rôle des gouvernements

Chaque Etat partie s'engage à assurer le leadership pour le développement de la culture de la cyber sécurité à l'intérieur de ses frontières. Les Etats membres s'engagent à sensibiliser, assurer l'éducation et la formation ainsi que la diffusion des informations au public.

3. Partenariat Public-Privé

Chaque Etat partie établit un partenariat public-privé en tant que modèle pour engager l'industrie, la société civile et le monde universitaire dans la promotion et le renforcement d'une culture de la cybersécurité.

4. Education et Formation

Chaque Etat partie adopte des mesures de renforcement des capacités afin de proposer des formations couvrant tous les domaines de la cybersécurité aux différentes parties prenantes et fixe des normes pour le secteur privé.

Les Etats Parties s'engagent à promouvoir l'enseignement technique pour les professionnels de la technologie de l'information et de la communication 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 en fonction des besoins.

Article 27 : Structures nationales de suivi de la cybersécurité

1. Gouvernance de la cybersécurité

a) Chaque Etat partie adopte les mesures nécessaires pour mettre en place un dispositif institutionnel approprié chargé de la gouvernance de la cybersécurité.

b) Les mesures adoptées au titre du paragraphe 1 du présent article assurent un leadership efficace et un engagement dans les divers aspects de la cybersécurité des institutions et des groupes professionnels compétents de

l'Etat Partie. A cet égard, les Etats Parties prennent des les mesures nécessaires pour :

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

ii) ii) exprimer un engagement manifeste et engagement transparent en matière de cybersécurité ;

iii) encourager le secteur privé et solliciter son engagement et sa participation aux initiatives entreprises par le gouvernement aux fins de promouvoir la cyber sécurité.

c) La gouvernance de la cybersécurité devra être établie dans un cadre national pouvant répondre aux défis rencontrés et à toute question relative à la sécurité de l'information au niveau national dans le plus grand nombre possible de domaines de la cybersécurité.

2. Le cadre institutionnel

Chaque Etat membre s'engage à adopter des mesures qu'il jugera nécessaires aux fins de créer des institutions compétentes pour lutter contre la cybercriminalité ; assurer le suivi et répondre aux incidents et aux alertes ; d'assurer la coordination nationale et transfrontalière des problèmes de cybersécurité et également la coopération mondiale.

Article 28 : Coopération internationale

1. Harmonisation

Les Etats parties s'assurent que les mesures législatives et/ou réglementaires adoptées pour lutter contre la cybercriminalité renforcent la possibilité d'harmonisation régionale de ces mesures et respectent le principe de la double incrimination.

2. Entraide judiciaire

Les Etats parties qui n'ont pas de conventions d'assistance mutuelle en matière de cybercriminalité s'engagent à encourager la signature des accords d'entraide judiciaire en conformité avec le principe de la double responsabilité tout en favorisant les échanges d'informations ainsi que le partage efficient des données entre les organisations des Etats parties sur une base bilatérale et multilatérale.

3. Echange d'informations

Les Etats parties encourage la mise en place des institutions qui échangent des informations sur les cyber- menaces et sur l'évaluation de la vulnérabilité telles que les équipes de réaction d'urgence en informatique (CERT : Computer Emergency Response Teams) ou les équipes de réaction

aux incidents de sécurité informatique (CSIRTS : Computer Security Incident Response Teams).

4. Moyens de coopération

Les Etats parties utilisent les moyens existants pour la coopération internationale aux fins de répondre aux cyber menaces, d'améliorer la cybersécurité et de stimuler le dialogue entre les parties prenantes. Ces moyens pourraient être internationaux, intergouvernementaux ou régionaux, ou basés sur des partenariats privés et publics.

Section II : Dispositions pénales

Article 29 : Les infractions spécifiques aux Technologies de l'Information et de la Communication

1. Atteintes aux systèmes informatiques

Les Etats parties prennent les mesures législatives et/ou réglementaires nécessaires en vue d'ériger en infraction pénale le fait :

a) d'accéder ou de tenter d'accéder frauduleusement à tout ou partie d'un système informatique ou de dépasser un accès autorisé ;

b) d'accéder ou de tenter d'accéder frauduleusement à tout ou partie d'un système informatique ou de dépasser un accès autorisé avec l'intention de commettre une nouvelle infraction ou de faciliter une telle infraction ;

c) de se maintenir ou de tenter de se maintenir frauduleusement dans tout ou partie d'un système informatique ;

d) d'entraver, fausser ou tenter d'entraver ou de fausser le fonctionnement d'un système informatique;

e) d'introduire ou tenter d'introduire frauduleusement des données dans un système informatique ;

f) 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.

Les Etats parties s'engagent par ailleurs à :

a) adopter des règles qui imposent aux vendeurs de produits des technologies de l'information et de la communication 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.

b) prendre des mesures législatives et/ou réglementaires nécessaires en vue d'ériger en infraction pénale le fait sans droit, 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 créer et produire un mot de passe, un code d'accès ou des données informatisées similaires permettant d'accéder à tout ou partie d'un système informatique.

2. Atteintes aux données informatisées

Les Etat parties prennent les mesures législatives et/ ou réglementaires nécessaires en vue d'ériger en infraction pénale le fait de :

a) 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 ;

b) b) introduire, altérer, effacer ou supprimer intentionnellement des données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention délictueuse similaire pour que la responsabilité pénale soit engagée ;

c) en connaissance de cause, faire usage des données obtenues de manière frauduleuse ;

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 ;

e) même par négligence, faire ou faire traiter des données à caractère personnel sans avoir respecté les formalités préalables à leur traitement ;

f) participer à une association formée ou à un accord conclu en vue de préparer ou de commettre une ou plusieurs des infractions prévues dans la présente convention.

3. Infractions liées au contenu

1. Les Etats parties prennent les mesures législatives et/ou réglementaires nécessaires en vue d'ériger en infraction pénale le fait de :

a) produire, enregistrer, offrir, fabriquer, mettre à disposition, diffuser, transmettre une image ou une représentation de pornographie infantile par le biais d'un système informatique ;

b) se procurer ou de procurer à autrui, importer ou faire importer, exporter ou faire exporter une image ou une représentation de pornographie infantile par le biais d'un système informatique ;

c) posséder une image ou une représentation de pornographie infantile dans un système informatique ou dans un moyen quelconque de stockage de données informatisées ;

d) faciliter et donner l'accès à des images, documents, son ou une représentation de nature pornographique à un mineur ;

e) 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 ;

f) menacer par le biais d'un système informatique, de commettre une infraction pénale contre 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 si cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou contre un groupe de personnes qui se distingue par une de ces caractéristiques ;

g) insulter commise par le biais d'un système informatique 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 l'opinion politique si cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou contre un groupe de personnes qui se distingue par une de ces caractéristiques ;

h) nier, approuver ou justifier délibérément des actes constitutifs de génocide ou de crimes contre l'humanité par le biais d'un système informatique.

2. Les Etats parties prennent les mesures législatives et/ou réglementaires nécessaires en vue d'ériger en infraction pénale les infractions prévues par la présente Convention.

Lorsqu'elles sont commises sous l'égide d'une organisation criminelle, elles seront punies du maximum de la peine prévue pour l'infraction concernée.

3. Les Etats parties prennent les mesures législatives et/ou réglementaires nécessaires pour qu'en sorte qu'en cas de condamnation, les tribunaux nationaux puissent prononcer la confiscation des matériels, équipements, instruments, programmes informatiques ou tous dispositifs ou données appartenant au condamné et ayant servi à commettre les infractions mentionnées dans cette Convention.

4. Infractions liées aux mesures de sécurité des échanges électroniques

Les Etats parties prennent les mesures législatives et/ou réglementaires nécessaires pour que la preuve numérique en matière pénale soit admise pour établir les infractions aux lois pénales internes sous réserve qu'elle ait été apportée au cours des débats et discutée devant le juge et que puisse

être dûment identifiée la personne dont elle émane et qu'elle ait été établie et conservée dans des conditions de nature à en garantir l'intégrité.

Article 30 : L'adaptation de certaines infractions aux technologies de l'information et de la communication

1. Atteintes aux biens

a) Les Etats parties prennent les mesures législatives et/ou réglementaires nécessaires en vue d'ériger en infraction la violation des biens, à savoir le vol, l'escroquerie, le recel, l'abus de confiance, l'extorsion de fonds, le chantage portant sur les données informatiques.

b) Les Etats parties s'engagent prennent les mesures législatives et/ou réglementaires nécessaires en vue de considérer comme circonstance aggravante l'utilisation des technologies de l'information et de la communication pour commettre des infractions comme le vol, l'escroquerie, le recel, l'abus de confiance, l'extorsion de fonds, le terrorisme, le blanchiment d'argent.

c) Les Etats parties prennent les mesures législatives et/ou réglementaires nécessaires pour inclure expressément « les moyens de communication numérique par voie électronique » tels qu'internet dans l'énumération des moyens de diffusion publique prévus dans le droit pénal des Etat parties.

d) Les Etats parties prennent les mesures législatives pénales nécessaires en vue de protéger les systèmes qui ont été considérés comme infrastructure critique de la défense nationale en raison des données critiques de sécurité nationale qu'ils contiennent.

2. Responsabilité pénale des personnes morales

Les Etats parties prennent les mesures législatives nécessaires pour faire veiller à ce 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 en leur nom par leurs organes ou représentants. La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

Article 31 : L'adaptation de certaines sanctions aux technologies de l'information et de la communication

1. Sanctions pénales

a) Les Etats parties prennent les mesures nécessaires pour veiller à ce que les infractions prévues par la présente Convention soient passibles de sanctions pénales effectives, proportionnées et dissuasives.

b) Les Etats parties prennent les mesures nécessaires pour veiller à ce que les infractions prévues par la présente Convention soient passibles de peines appropriées selon sa législation nationale.

c) Les Etats parties prennent les mesures nécessaires pour s'assurer qu'une personne morale tenue responsable conformément aux dispositions de la présente Convention, est passible de peines effectives, proportionnées et dissuasives, y compris des amendes pénales.

2. Autres sanctions pénales

a) Les Etats parties prennent les mesures nécessaires pour veiller à ce qu'en cas de condamnation pour une infraction commise par un moyen de communication numérique, la cour compétente puisse prononcer des peines complémentaires.

b) Les Etats parties prennent les mesures nécessaires pour s'assurer qu'en cas de condamnation pour une infraction commise par le biais d'un support de communication numérique, le juge peut ordonner la diffusion obligatoire au frais du condamné, par extrait de la décision par le même support et selon des modalités précisées dans les législations des Etats membres.

c) Les Etats parties prennent les mesures législatives nécessaires pour veiller à ce que la violation du secret de données stockées dans un système d'information soit punie des mêmes peines applicables au délit de violation du secret professionnel.

3. Droit procédural

a) Les Etats parties prennent les mesures nécessaires pour s'assurer que lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire d'un Etat partie, sont utiles à la manifestation de la vérité, la cour peut procéder à une perquisition pour accéder à tout ou partie d'un système informatique, dès lors que ces données sont accessibles à partir du système initial ou existent dans ce système.

b) Les Etats parties prennent les mesures nécessaires pour faire en sorte que lorsque l'autorité judiciaire en charge de l'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 appropriée, 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, conformément aux modalités prévues dans les législations des Etats parties.

c) Les Etats parties prennent les mesures nécessaires pour veiller à ce que les autorités judiciaires puissent, pour les nécessités de l'enquête ou de

l'exécution d'une délégation judiciaire, procéder aux opérations prévues par la présente Convention.

d) Les Etats parties prennent les mesures nécessaires pour faire en sorte que si les besoins 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 conduite des investigations judiciaires. Le gardien des données ou toute autre personne chargée de conserver celles-ci est tenu d'en garder le secret en ce qui concerne les données.

e) Les Etats parties prennent les mesures nécessaires pour veiller à ce que si les besoins de l'information l'exigent le juge d'instruction en puisse utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, les données relatives au contenu des 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 ou ceux des Etats parties, ou à fournir aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées.

CHAPITRE IV : DISPOSITIONS FINALES

Article 32 : Mesures à prendre au niveau de l'Union africaine

Le Président de la Commission fait rapport à la Conférence sur la mise en œuvre et le suivi du mécanisme opérationnel de la présente Convention.

Le mécanisme de suivi à mettre en place veillera à :

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

b) rassembler les documents et les informations sur les besoins en cybersécurité ainsi que sur la nature et l'ampleur de la cybercriminalité et les atteintes aux droits de l'homme 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 l'homme dans le cyberespace et diffuser l'information, et sensibiliser l'opinion publique aux effets négatifs de ces phénomènes ;

d) conseiller les gouvernements africains sur les moyens de promouvoir la cybersécurité et de lutter contre le fléau de la cybercriminalité et les atteintes aux droits de l'homme dans le cyberespace au niveau national ;

e) recueillir des informations et procéder à des analyses sur le comportement délictueux des usagers des réseaux et des systèmes d'informations opérant en Afrique, et transmettre ces informations aux autorités nationales compétentes ;

f) élaborer et promouvoir l'adoption des codes de conduite harmonisés pour l'usage des agents de l'Etat 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 l'homme dans le cyberespace ;

h) soumettre des rapports réguliers au Conseil Exécutif de l'Union africaine sur les progrès réalisés par chaque Etat partie dans la mise en œuvre des dispositions de la présente Convention ;

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

Article 33 : Dispositions de sauvegarde

Les dispositions de la présente Convention ne peuvent pas être interprétées de manière non conforme aux principes pertinents du droit international, y compris le droit coutumier international.

Article 34 : Règlement des différends

1. Tout différend né de l'application de la présente Convention est réglé à l'amiable, par voie de négociation directe entre les Etats parties concernés.

2. Si le différend ne peut être réglé par voie de négociation directe, les Etats parties s'efforcent de le régler par d'autres moyens pacifiques, y compris les bons offices, la médiation et la conciliation, ou tout autre moyen pacifique agréé par les Parties. A cet égard, les Etats parties sont encouragés à recourir aux procédures et mécanismes de règlement des différends mis en place dans le cadre de l'Union.

Article 35 : Signature, ratification et adhésion

La présente Convention est ouverte à tous les Etats membres de l'Union, pour signature, ratification ou adhésion, conformément à leurs procédures constitutionnelles respectives.

Article 36 : Entrée en vigueur

La présente Convention entre en vigueur trente (30) jours après la réception, par le Président de la Commission de l'Union africaine, du quinzième (15e) instrument de ratification.

Article 37 : Amendement

1. Tout Etat partie peut soumettre des propositions d'amendement ou de révision de la présente Convention.

2. Les propositions d'amendement ou de révision sont soumises au Président de la Commission de l'Union africaine, qui les transmet aux Etats parties dans un délai de trente (30) jours suivant leur réception.

3. La Conférence de l'Union, sur recommandation du Conseil exécutif de l'Union, examine ces propositions à sa prochaine session, à condition que tous les Etats Parties en aient été notifiés trois (3) mois au moins avant le début de la session.

4. La Conférence de l'Union adopte les amendements, conformément à son Règlement intérieur.

5. Les amendements ou révisions entrent en vigueur conformément aux dispositions de l'article 36 ci-dessus.

Article 38 : Dépositaire

1. Les instruments de ratification ou d'adhésion sont déposés auprès du Président de la Commission de l'Union africaine.

2. Tout Etat partie peut dénoncer la présente Convention en notifiant, par écrit, son intention un (1) an à l'avance au Président de la Commission de l'Union africaine.

3. Le Président de la Commission de l'Union africaine informe tous les Etats membres de toute signature de la présente Convention, du dépôt de tout instrument de ratification ou d'adhésion, ainsi que de son entrée en vigueur.

4. Le Président de la Commission informe également les Etats parties des demandes d'amendement ou de retrait de la Convention, ainsi que les réserves à celle-ci.

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

6. La présente Convention, rédigée en quatre (4) textes originaux en Arabe, en Anglais, en Français et en Portugais, tous les quatre (4) textes faisant également foi, est déposée auprès du Président de la Commission de

l'Union africaine qui en transmet une copie certifiée conforme à chaque Etat membre dans sa langue officielle.

Adoptée par la vingt-troisième session ordinaire

de la Conférence de l'Union à Malabo,

Guinée Equatoriale le 27 juin 2014