CONVENÇÃO DA UNIÃO AFRICANA SOBRE CIBERSEGURANÇA E PROTECÇÃO DE DADOS PESSOAIS

PREÂMBULO

Os Estados-membros da União Africana;

Guiados pelo Acto Constitutivo da União Africana, adoptado em 2000;

Considerando que a presente Convenção, relativa à criação de um Quadro Jurídico sobre a **Cibersegurança e Protecção de Dados Pessoais**, incorpora os compromissos existentes dos Estados-Membros da União Africana no plano sub-regional, regional e internacional, com vista a construção da Sociedade de Informação;

Recordando que ela visa definir os objectivos e as orientações gerais da Sociedade de Informação em África e reforçar as legislações existentes dos Estados-membros e da Comunidade Económicas Regionais (CER) em matéria das Tecnologias de Informação e Comunicação (TIC);

Reafirmando o compromisso dos Estados-Membros com as liberdades fundamentais e os direitos humanos e dos povos, consagrados nas declarações, convenções, assim como em outros instrumentos aprovados no quadro da União Africana e das Nações Unidas;

Considerando que a criação de um quadro normativo sobre a cibersegurança e protecção de dados pessoais leva em consideração as exigências do respeito dos direitos dos cidadãos, garantidos pelos textos fundamentais do direito interno e protegidos pelas Convenções e Tratados Internacionais sobre os Direitos Humanos, em particular a Carta Africana dos Direitos do Homem e dos Povos;

Conscientes da necessidade de mobilizar todos os actores públicos e privados (Estados, as comunidades locais, empresas dos sectores público e privado, organizações da sociedade civil, órgãos de informação, instituições de formação e de investigação) a favor da promoção da segurança cibernética;

Reiterando os princípios da Iniciativa da Sociedade de Informação Africana (ISIA) e do Plano de Acção Regional Africano para a Economia do Conhecimento (PARAEC);

Conscientes de que destina-se a regular uma particularidade que envolve uma área tecnológica, e com vista a responder às grandes expectativas de vários actores com diferentes interesses, **a presente Convenção** fixa as normas de segurança essenciais para a criação de um espaço digital credível para as transacções electrónicas, protecção de dados pessoais e luta contra o cibercrime;

Tendo em mente que os principais **desafios** para o desenvolvimento do comércio electrónico em África estão ligados a problemas de segurança, especialmente:

a) As lacunas que afectam a regulamentação no que concerne ao reconhecimento jurídico da comunicação de dados e da assinatura electrónica;

b) A ausência de normas jurídicas específicas que protejam os consumidores, os direitos de propriedade intelectual, e dados de carácter pessoal e sistemas de informação;

c) Ausência de normas legislações relativas a teleserviços e teletrabalho;

d) A aplicação de técnicas electrónicas para os actos comerciais e administrativos;

e) Os elementos de prova introduzidos pelas tecnologias digitais (carimbo da hora e data, certificação).

f) As regras aplicáveis aos aparelhos e serviços de criptologia;

g) Fiscalização da publicidade em linha;

h) A ausência de legislações fiscal e aduaneira apropriadas para o comércio electrónico.

Convencidos de que as constatações atrás referidas justificam o apelo para a criação de um quadro normativo apropriado consistente com o ambiente jurídico, cultural, económico e social africano, e que o objectivo da presente Convenção é, portanto, de proporcionar a segurança e o quadro jurídico necessários para o surgimento da economia do conhecimento em África;

Sublinhando que, a outro nível, a protecção de dados de carácter pessoal e vida privada constitui um grande desafio para a Sociedade de Informação, tanto para os governos como para as outras partes intervenientes, que a referida protecção exige um equilíbrio entre o uso das tecnologias de informação e comunicação e a protecção da vida privada dos cidadãos na sua vida quotidiana ou profissional, ao mesmo tempo que se garante a livre circulação de informação;

Preocupados pela necessidade urgente de criar mecanismos para fazer face aos perigos e os riscos decorrentes da utilização de dados electrónicos e de registos individuais, com vista a respeitar a privacidade e as liberdades, enquanto se intensifica a promoção e o desenvolvimento das Tecnologias de Informação e Comunicação (TIC) nos Estados-membros da União Africana;

Considerando que o objectivo da presente Convenção é o de responder à necessidade de uma legislação harmonizada no domínio da segurança cibernética nos Estados-membros da União Africana e criar, em cada Estado Parte, um mecanismo que permita lutar contra violações da privacidade através da recolha, tratamento, transmissão, armazenamento e uso de dados pessoais; que ao propor

o tipo da base institucional, a Convenção garante que qualquer forma processamento que for utilizada respeite as liberdades fundamentais e os direitos das pessoas, ao mesmo tempo que se toma em consideração as prerrogativas dos Estados-Membros, os direitos das comunidades locais e os interesses das empresas, e ter em conta as melhores práticas reconhecidas a nível internacional;

Considerando que do sistema de valores da sociedade de informação a protecção no âmbito do direito penal impõe-se como uma necessidade ditada por motivos de segurança, que ela se manifesta essencialmente pela necessidade de uma legislação penal apropriada para a luta contra o cibercrime, em geral e, em particular, o branqueamento de capital;

Conscientes de que, perante a situação actual da criminalidade informática, que constitui uma verdadeira ameaça para a segurança das redes informáticas e o desenvolvimento da sociedade de informação em África, é necessário definir as grandes orientações da estratégia de repressão da criminalidade informática nos Estados-Membros da União Africana, tomando em conta os seus compromissos actuais aos níveis sub-regional, regional e internacional;

Considerando que a presente Convenção visa, em matéria do direito penal substantivo, modernizar os instrumentos de repressão do cibercrime, através da elaboração de uma política de adopção de novas ofensas específicas para as TIC, e harmonizando alguns sistemas de ofensas, sanções e responsabilidade penal em vigor nos Estados-membros com o ambiente das tecnologias de informação e comunicação;

Considerando ainda que, em matéria do direito processual penal, a Convenção define o quadro de adaptação de procedimentos normativos relativamente às tecnologias de informação e comunicação e indica com precisão as condições da criação de procedimentos específicos para a criminalidade informática;

Evocando a Decisão Assembly/AU/Decl.1(XIV), da 14ª Sessão Ordinária da Cimeira dos Chefes de Estado e de Governo da União Africana sobre as Tecnologias de Informação e Comunicação em África: Desafios e Perspectivas para o Desenvolvimento, realizada em Adis Abeba, Etiópia, de 31 de Janeiro a 2 de Fevereiro de 2010;

Tendo em conta a Declaração de Oliver Tambo, adoptada pela Conferência Extraordinária dos Ministros responsáveis pelas Tecnologias de Informação e Comunicação, realizada em Joanesburgo, a 05 de Novembro de 2009.

Evocando as disposições da Declaração de Abidjan, adoptada a 22 de Fevereiro de 2012, bem como a Declaração de Adis Abeba, adoptada a 22 de Junho de 2012, sobre a Harmonização da Legislação referente a Cibernética em África.

ACORDARAM NO SEGUINTE:

Artigo 1º
Definições

Para os efeitos da presente Convenção

UA significa a União Africana;

Pornografia infantil: qualquer representação visual de um comportamento sexualmente explícito, incluindo qualquer fotografia, filme, vídeo, imagem, quer fabricada ou produzida por via electrónica, mecânica ou por outros meios, onde:

a) a produção dessa representação visual envolve um menor;

b) essa representação visual é uma imagem digital, uma imagem exibida por um computador ou uma imagem criada por um computador, onde um menor está envolvido num comportamento sexualmente explícito ou quando as imagens dos seus órgãos sexuais são produzidas ou utilizadas para fins principalmente sexuais e exploradas com ou sem o conhecimento da criança;

c) essa representação visual tenha sido criada, adaptada ou alterada para parecer que um menor está envolvido num comportamento sexualmente explícito;

Código de conduta: conjunto de regras elaboradas pelo funcionário responsável pelo processamento de dados, a fim de estabelecer o uso correcto dos recursos informáticos, das redes e comunicações electrónicas da estrutura competente e homologada pela Autoridade de Protecção;

Comissão: a Comissão da União Africana;

Comunicação com o público por via electrónica: qualquer disponibilização ao público ou segmentos do público, através de um processo electrónico ou de comunicação magnética, de signos, sinais, material escrito, imagem, mensagens áudio ou de qualquer natureza, através do processo de comunicação electrónica e magnética;

Sistema informático: qualquer dispositivo electrónico, magnético, óptico, electroquímico ou qualquer outro dispositivo de processamento de dados em alta velocidade, ou grupo de aparelhos interconectado ou relacionados, que executa funções lógicas, aritméticas ou de armazenamento de dados, e inclui qualquer dispositivo de armazenamento de dados ou de comunicação directamente relacionado ao ou funcionando em paralelo com tal dispositivo ou outro(s) dispositivo(s);

Dados informatizados: qualquer representação de factos, informações ou de conceitos apropriados para serem processados num computador;

Consentimento dos sujeitos titular dos dados: qualquer manifestação de vontade expressa, inequívoca, livre, específica e informada através da qual a pessoa interessada ou o seu representante legal, judicial ou convencional aceita que os seus dados pessoais sejam processados manual ou electronicamente;

A (ou a presente) Convenção: a Convenção da União Africana sobre a Segurança Cibernética e Protecção de Dados Pessoais;

Infra-estruturas Críticas das TIC/Cibernéticas: Infra-estruturas das TIC/cibernética que são essenciais aos serviços vitais da segurança pública, estabilidade económica, segurança nacional, estabilidade internacional bem como para a manutenção e a restauração do ciberespaço;

Actividade de Criptologia: qualquer actividade que tem como objectivo a produção, utilização, importação, exportação ou a comercialização dos equipamentos de criptologia;

Criptologia: a ciência de protecção e segurança da informação, visando particularmente garantir a confidencialidade, autenticidade, integridade e não repúdio;

Ferramenta de Criptologia: o leque de ferramentas científicas e técnicas (equipamento ou software) que permitem a cifragem e/ou decifragem;

Serviços de Criptologia: qualquer operação que visa a utilização, por conta própria ou de outrem, dos meios de criptologia;

Provedor de serviços de criptologia: qualquer pessoa singular ou colectiva que presta serviços de criptologia;

Danos: qualquer prejuízo à integridade ou à disponibilidade de dados, de um programa, sistema ou uma informação;

Responsável pelos dados: qualquer pessoa singular ou colectiva, pública ou privada, qualquer outra organização ou associação que sozinha ou em conjunto com outras pessoas decida recolher e processar dados pessoais e determinar a sua finalidade;

Sujeito titular dos dados: qualquer pessoa singular que está sujeita ao processamento de dados pessoais;

Marketing directo: o despacho de qualquer mensagem que visa promover, directa ou indirectamente, os bens e serviços ou a imagem de uma pessoa que vende

esses bens ou presta tais serviços; também se refere a qualquer tipo de solicitação realizada por meio de envio de mensagem, independentemente da base ou natureza da mensagem, especialmente mensagens de natureza comercial, política ou de caridade, destinada a promover, directa ou indirectamente, bens e serviços ou a imagem de uma pessoa que vende os bens ou presta os serviços;

Dupla criminalidade: crime punido simultaneamente no país onde o suspeito está detido e o país que solicita que o suspeito seja entregue ou transferido;

Comunicação electrónica: qualquer transmissão ao público ou a uma categoria de público, através de um meio de comunicação electrónico ou magnético de signos, sinais, escritos, imagens, sons ou de mensagens de qualquer natureza;

Comércio Electrónico (e- comércio) o acto de oferta, compra ou fornecimento de bens e serviços através de sistemas de computadores e redes de telecomunicações tais como a Internet ou qualquer outra rede através de meios electrónicos, dispositivos ópticos ou similares para troca de informações à distância;

Correio electrónico: qualquer mensagem, sob a forma de texto, voz, som ou de imagem enviada por uma rede pública de comunicação, armazenada num servidor de rede ou no terminal de um meio pertencente ao destinatário, até que este último a recupere;

Assinatura electrónica: dados em forma electrónica, que estão associados ou ligados logicamente a outros dados electrónicos, servindo para procedimentos de identificação;

Dispositivo de verificação da assinatura electrónica: conjunto de elementos materiais ou de software que permitem a verificação de uma assinatura electrónica;

Dispositivo de criação da assinatura electrónica: conjunto de elementos materiais ou de software que permitem a criação de uma assinatura electrónica;

Encriptação: todas as técnicas que consistem de um processamento de dados digitais num formato ininteligível usando instrumentos de criptologia;

Exceder o acesso autorizado: ter acesso a um computador com autorização e usar esse acesso para obter ou alterar informação no computador que o usuário não tem direito de o fazer;

Dados no domínio da saúde: qualquer informação sobre o estado físico e mental de uma pessoa titular dos dados, incluindo as informações genéticas acima mencionadas;

Comunicação electrónica indirecta: qualquer mensagem de texto, voz, som ou de imagem enviada através de uma rede de comunicação electrónica e armazenada num terminal de comunicação até a sua recepção pelo destinatário;

Informação: qualquer elemento de conhecimento susceptível de ser representado através de convenções, a fim de ser utilizado, conservado, processado ou transmitido. A informação pode ser exprimida sob a forma escrita, visual, sonora, digital ou de outra natureza;

Interconexão de dados pessoais: qualquer mecanismo de conexão que consiste em estabelecer a ligação entre os dados processados para uma determinada finalidade com outros dados processados para finalidades idênticas ou não, ou ainda ligadas por um ou vários funcionários processadores;

Meio de pagamento electrónico: meio que permite ao seu titular efectuar operações electrónicas de pagamento em linha;

Estado-membro ou Estados-membros: O(os) Estado(s)-membro(s) da União Africana;

Criança ou Menor: qualquer pessoa singular com menos de 18 anos de idade, ao abrigo da Carta Africana sobre os Direitos e o Bem-estar da Criança e da Convenção das Nações Unidas sobre os Direitos da Criança, respectivamente;

Dados pessoais: qualquer informação relativa a uma pessoa singular identificada ou identificável, através da qual esta pessoa pode ser identificada, directa ou indirectamente, em particular através de referência a um número de identificação ou a um ou vários factores específicos à sua identidade física, fisiológica, mental, económica, cultural ou social;

Ficheiro de dados pessoais: todo o pacote estruturado de dados acessíveis, de acordo com critérios determinados, independentemente de tais dados estarem ou não centralizados, descentralizados ou distribuídos de uma forma funcional ou geográfica;

Processamento de Dados Pessoal: qualquer operação ou conjunto de operações efectuadas sobre os dados pessoais, que através de meios automáticos ou não, tais como tais como recolha, registo, organização, armazenamento, adaptação, alteração, recuperação, suporte, cópia, consulta, utilização, divulgação, ou qualquer outra forma de distribuição, ou doutro modo, fazendo disponibilização, alinhamento ou combinação e bloqueio, encriptação, supressão ou destruição de dados pessoais;

Racismo e xenofobia nas tecnologias de informação e comunicação: qualquer material escrito, imagem ou outra representação de ideias ou teorias que defendem ou encorajam o ódio, a discriminação ou a violência contra uma pessoa ou um

grupo de pessoas por razões fundadas na sua raça, cor da pele, descendência, origem nacional ou étnica ou religião;

Destinatário dos dados pessoais processados: qualquer pessoa autorizada para receber a transmissão desses dados, para além do sujeito titular dos dados, o indivíduo responsável pelos dados, a pessoa subcontratada ou as pessoas que, devido às suas funções, têm a responsabilidade de processar os dados;

Convenções secretas: códigos não publicados, necessários para executar um meio ou serviços de criptologia para as operações de cifragem ou decifragem;

Dados sensíveis: todos os dados pessoais relativos às opiniões ou actividades religiosas, filosóficas, políticas, sindicais, bem como relacionadas à vida sexual ou raça, saúde, medidas sociais, processos judiciais, sanções penais ou administrativas;

Estado Parte (ou Estados Partes): Estado-membro ou Estados-membros que tenha(m) ratificado ou aderido à presente Convenção;

Subcontratado: qualquer pessoa, singular ou colectiva, pública ou privada, qualquer outra organização ou associação que processa dados em nome do responsável pelos dados;

Terceiro: qualquer pessoa, singular ou colectiva, pública ou privada, outro organismo ou associação, que não seja o sujeito titular dos dados, Responsável pelos dados, processador de dados, da pessoa subcontratada e de outras pessoas que, sob a autoridade directa do indivíduo responsável pelo tratamento ou do subcontratado, está autorizada a fazer o processamento de dados;

CAPÍTULO I
TRANSACÇÕES ELECTRÓNICAS

Secção I: Comércio Electrónico

Artigo 2:
Âmbito de aplicação do comércio electrónico

1. Os Estados-membros devem garantir que as actividades do comércio electrónico sejam exercidas livremente em todos os Estados Partes que tenham ratificado ou aderido à presente Convenção, excepto nos seguintes domínios:

   a) Jogos de azar, sob a forma de apostas e lotarias, legalmente autorizados;

b) Actividades de representação e de assistência jurídica;

c) Actividades exercidas pelos notários ou pelas autoridades equivalentes, em cumprimento da legislação em vigor.

2. Sem prejuízo de outras obrigações de informação previstas nos documentos legislativos e regulamentares em vigor nos Estados-membros da União Africana, os Estados Partes garantem que qualquer indivíduo que exerce o comércio electrónico deva assegurar que os destinatários da prestação desses serviços tenham acesso fácil, directo e permanente, usando normas genéricas para as seguintes informações:

a) Quando houver um envolvimento de uma pessoa física, o provedor de serviços deve indicar o nome e o apelido e, quando for uma pessoa colectiva, deve indicar nome da empresa, o seu capital, o seu número de registo na conservatória comercial ou de associações;

b) O endereço completo do seu estabelecimento, o seu endereço electrónico assim como o seu número de telefone;

c) Se a pessoa estiver sujeita às formalidades de registo comercial ou ao cadastro nacional de empresas e associações empresariais, deve indicar o seu número de registo, o seu capital social e o endereço da sua sede social;

d) Se a pessoa estiver sujeita ao pagamento de taxas, deve indicar o número de identificação tributária;

e) Se a sua actividade estiver sujeita ao regime de licenciamento, deve indicar o nome e o endereço da entidade emissora dessa licença bem como a respectiva referência;

f) Se for membro de uma associação profissional autorizada, deve indicar as normas profissionais aplicáveis, o seu título profissional, o Estado-membro da União Africana onde obteve o título profissional assim como o nome da ordem ou do organismo profissional junto do qual está inscrito.

3. Qualquer pessoa, singular ou colectiva, que exerce uma actividade de comércio electrónico deve, mesmo sem contrato, desde que mencione um preço, indicar esse preço de uma forma clara e não ambígua e, principalmente, se o preço incluir taxas, despesas de transporte e outros encargos.

Artigo 3°
Responsabilidade contratual do fornecedor de bens e serviços por meios electrónicos

A actividade do comércio electrónico está sujeita à legislação do Estado Parte em cujo território reside a pessoa que a exerce, sujeita a intenção expressa comum entre essa pessoa e o destinatário dos bens ou serviços.

Artigo 4°
Publicidade por via electrónica

1. Sem prejuízo do Artigo 3º, independentemente da sua forma, acessível aos serviços de comunicação em linha, qualquer publicidade deve ser claramente identificada como tal. Deve identificar claramente a pessoa singular ou colectiva em nome de quem é realizada.

2. As condições que determinam a possibilidade de ofertas promocionais assim como de participar em concursos ou jogos promocionais, onde tais ofertas, concursos ou jogos são publicitados por via electrónica, devem indicar claramente a sua localização e serem facilmente acessíveis.

3. Os Estados Partes membros da União Africana devem proibir o marketing directo através de qualquer forma de comunicação indirecta utilizando, sob qualquer forma, os detalhes pessoais de uma pessoa que não tenha exprimido o seu consentimento prévio de receber publicidade directa por esse meio.

4. Não obstante as disposições do Artigo 4º (2), o marketing directo, por correio electrónico, é autorizado quando:

   a) Os detalhes do endereço do destinatário forem obtidos directamente junto dele;

   b) O destinatário tiver dado o seu consentimento ao remetente para ser contactado pelos seus parceiros de marketing;

   c) O marketing directo referir-se a produtos ou serviços análogos fornecidos pelo mesmo indivíduo ou empresa.

5. Os Estados Partes proíbem a transmissão de mensagens, para fins publicitários directos, através de qualquer forma de comunicação electrónica indirecta, sem indicar os detalhes pessoais válidos através dos quais o destinatário possa enviar um pedido de interrupção dessas comunicações sem custos adicionais, excepto os que decorrem da transmissão desse pedido.

6. Os Estados Partes comprometem-se a proibir a dissimulação da identidade da pessoa por conta de quem a publicidade acessível para um serviço de comunicação em linha é feita.

Secção II: Obrigações Contratuais em Forma Electrónica

Artigo 5º
Contratos electrónicos

1. As informações que são solicitadas para a celebração de um contrato ou informações disponíveis durante a execução do contrato podem ser transmitidas por via electrónica se os seus destinatários aceitarem o uso desse meio. Presume-se que a utilização das comunicações electrónicas deve ser aceite, excepto quando o beneficiário tiver previamente exprimido a sua preferência para um outro meio de comunicação.

2. O prestador de serviços ou fornecedor de bens, a título profissional, por via electrónica, deve pôr criar condições contratuais aplicáveis, directa ou indirectamente, por forma a facilitar a sua conservação e a sua reprodução, em conformidade com as legislações nacionais.

3. Para que o contrato seja válido, o destinatário da oferta deve ter a possibilidade de verificar os detalhes da sua encomenda, principalmente o preço, antes de confirmá-la, exprimindo a sua aceitação.

4. A pessoa que oferece os seus bens e serviços deve acusar sem demora injustificada a recepção, por via electrónica, da encomenda que lhe for enviada.

   A encomenda, a confirmação da aceitação da oferta e a acusação da recepção são consideradas como recebidas quando as partes a quem são enviadas poderem ter acesso.

5. Podem ser dispensadas as disposições dos Artigos 5º (3) e 5º (4) da presente Convenção para acordos celebrados entre empresas e profissionais (B2B).

6. a) Qualquer pessoa, singular ou colectiva, que exerce a actividade definida na primeira alínea do Artigo 2º (1) da presente Convenção é responsável, *ipso facto,* perante o seu parceiro contratual pelo cumprimento das obrigações decorrentes do contrato, independentemente de tais obrigações serem cumpridas por si próprio ou por outros provedores de serviços, sem prejuízo do seu direito de queixa contra esses provedores de serviço.

b) Todavia, a pessoa singular ou jurídica pode estar isenta de toda ou parte da responsabilidade, apresentado a prova de que a falta de cumprimento ou a má execução do contrato deveu-se, quer da outra parte contratante, quer por motivos de força maior.

Artigo 6º
Escrita em forma electrónica

1. Sem prejuízo das disposições legais internas em vigor no Estado Parte, ninguém pode ser obrigado a praticar um acto jurídico por via electrónica.

   a) Quando um documento escrito for exigido para a validade de um acto jurídico, cada Estado Parte deve estabelecer as condições legais com vista à equivalência funcional entre as comunicações electrónicas e as versões em papel, quando a regulamentação interna em vigor exigir um documento escrito para a validade de um acto jurídico.

   b) Quando o documento escrito em forma de papel estiver sujeito a condições particulares, como leitura ou apresentação, o documento escrito sob a forma electrónica estará sujeito às mesmas condições.

   c) A exigência de entrega de várias cópias considera-se satisfeita quando o mesmo documento escrito poder ser reproduzido sob uma forma material pelo destinatário.

2. As disposições do Artigo 6º (2) da presente Convenção não se aplicam para os seguintes casos:

   a) Os actos privados assinados relativos ao direito da família e das sucessões; e

   b) Os actos privados relativos à garantias pessoais ou reais, quer seja ao abrigo do direito civil ou comercial, em conformidade com as legislações nacionais, salvo quando forem celebrados por uma pessoa para fins da sua profissão.

3. A entrega de um documento escrito sob a forma electrónica torna-se efectiva quando o destinatário, depois de tomar conhecimento, acusar a recepção.

4. No que diz respeito às suas funções fiscais, as facturas devem ser apresentadas por escrito a fim de assegurar a sua legibilidade, integridade e a **manutenção** do seu conteúdo. Deve ser igualmente garantida a autenticidade da sua origem.

   Entre os métodos que podem ser implementados para cumprir os objectivos fiscais da factura e assegurar que as suas funções sejam satisfeitas, figura o estabelecimento de controlo da gestão que criará uma pista de auditoria fiável entre uma factura e a entrega dos bens ou serviços.

Para além do tipo de controlo descrito no §1, os métodos que se seguem constituem exemplos de tecnologias que permitem assegurar a autenticidade da origem do conteúdo de uma factura electrónica:

a) uma assinatura electrónica qualificada, tal como está definido no Artigo 1º;

b) uma troca de dados informatizados (TDI), por exemplo a transferência electrónica, de um computador para o outro, de dados comerciais e administrativos, sob a forma de uma mensagem de TDI estruturada em conformidade com a norma acordada, desde que o acordo relativo a esta troca prevê a utilização de procedimentos que garantam a autenticidade da origem e a integridade dos dados.

5. Um documento escrito em forma electrónica é admitida como prova da mesma forma que o escrito e tem valor idêntico jurídico, desde que o o seu remetente possa ser devidamente identificado, e que foi feito e conservado por forma a garantir a sua integridade.

Secção III: Segurança das Transacções Electrónicas

Artigo 7º
Garantia de Segurança das Transacções Electrónicas

1. a) O fornecedor de bens deve permitir aos seus clientes efectuar os seus pagamentos utilizando um meio electrónico aprovado pelo Estado, de acordo com os regulamentos em vigor em cada Estado Parte.

   b) O fornecedor de bens ou o provedor de serviços por meios electrónicos que reclamar cumprimento de uma obrigação deve provar a sua existência e, ou de outro modo, provar que a obrigação era inexistente ou foi cumprida.

2. Quando os dispositivos legais dos Estados Partes não fixarem outros princípios e onde não existe nenhum acordo válido entre as partes, o juiz deve resolver os conflitos comprovados, determinando, por todos os meios possíveis, a reivindicação mais justa, independentemente do suporte apresentado.

3. a) A cópia ou qualquer outra reprodução de contratos assinados por meios electrónicos têm o mesmo valor de prova como o contrato em forma de papel, quando for confirmada pelos organismos devidamente credenciados por uma autoridade do Estado Parte.

   b) A certificação, se for necessário, resultará na emissão de um certificado de conformidade.

4. a) Uma assinatura electrónica, criada por um dispositivo seguro que o signatário possa guardar sob o seu controlo exclusivo, com base num certificado digital, é aceite como assinatura, com valor idêntico à assinatura manuscrita.

   b) Presume-se a fiabilidade deste procedimento, até prova contrário, se a assinatura electrónica for criada por um dispositivo seguro de criação de assinatura, que a garanta a integridade do acto e que a identificação do signatário seja assegurada.

CAPÍTULO II
PROTECÇÃO DE DADOS PESSOAIS

Secção I: Protecção de Dados Pessoais

Artigo 8º
Objectivo da Presente Convenção em Relação aos Dados Pessoais

1. Cada Estado Parte compromete-se a criar um quadro jurídico, tendo como objectivo reforçar os direitos fundamentais e as liberdades públicas, nomeadamente a protecção de dados físicos, e reprimir qualquer infracção relativa à vida privada, sem prejuízo do princípio da liberdade de circulação de dados pessoais.

2. Esse mecanismo assim criado deve garantir que qualquer tratamento de dados, respeite as liberdades e os direitos fundamentais das pessoas singulares, ao mesmo tempo reconhecendo-se as prerrogativas do Estado, os direitos das comunidades locais e os objectivos para os quais as empresas foram criadas.

Artigo 9º
Âmbito de Aplicação da Convenção

1. Estão sujeitos à presente Convenção:

   a) Qualquer recolha, processamento, armazenagem ou utilização de dados pessoais por uma pessoa singular, pelo Estado, pelas comunidades locais e pelos organismos públicos ou privados;

   b) Qualquer processamento informatizado ou não de dados contidos ou que devem figurar num ficheiro, excepto os processamentos de dados mencionados no Artigo 9º (2) da presente Convenção;

   c) Qualquer processamento de dados feitos no território de um Estado-membro da União Africana;

d) Qualquer processamento de dados relativos à segurança pública, defesa, investigação e processos penais ou à segurança do Estado, sujeitos a excepções definidas por disposições específicas fixadas por outras leis em vigor.

2. A presente Convenção não se aplica:

a) Ao processamento de dados feitos por uma pessoa singular no quadro exclusivo das suas actividades pessoais ou domésticas, desde que esses dados não sejam destinados a uma comunicação sistemática a terceiros ou à difusão;

b) Às cópias temporárias feitas no quadro das actividades técnicas de transmissão e acesso a uma rede digital, com o objectivo de armazenamento automático, intermédio e temporário de dados, tendo como finalidade exclusiva permitir aos destinatários do serviço o melhor acesso possível às informações enviadas.

Artigo 10º
Formalidades prévias ao tratamento de dados pessoais

1. Estão isentos de formalidades prévias:

a) O processamento de dados mencionados no Artigo 9º (2) da presente Convenção;

b) O processamento de dados realizados com objectivo único de manter um registo destinado ao uso exclusivamente privado;

c) O processamento de dados feito por uma associação ou por qualquer organismo sem fins lucrativos, com fins religiosos, filosóficos, políticos ou sindicais, desde que esses dados correspondam ao objectivo da associação ou do organismo, relacionados somente com os seus membros, não devendo ser revelados a terceiros.

2. Com excepção dos casos previstos nos Artigos 10º (1), 10º (4) e 10º (5) da presente Convenção, o processamento de dados pessoais sujeita-se a uma declaração junto da autoridade de protecção.

3. Para as categorias mais comuns de processamento de dados pessoais, que provavelmente não constituam uma violação da privacidade ou das liberdades individuais, a autoridade de protecção pode estabelecer e publicar normas destinadas a simplificar ou introduzir isenções da obrigação de apresentar declaração.

4. As seguintes acções são implementadas depois da autorização da autoridade nacional de protecção:

a) O processamento de dados pessoais envolvendo informações genéticas e à investigação na área da saúde;

b) O processamento de dados pessoais envolvendo informação sobre infracções, condenações ou medidas de segurança;

c) O processamento de dados pessoais que têm como objectivo estabelecer uma interconexão de ficheiros, tal como está definido no Artigo 15º da presente Convenção, processamento de dados relativos ao número nacional de identificação ou qualquer outra forma que identifica o mesmo tipo;

d) O processamento de dados pessoais relativo a informações biométricas;

e) O processamento de dados pessoais de interesse público, nomeadamente para fins históricos, estatísticos ou científicos.

5. O processamento de dados pessoais efectuado em nome do Estado, de uma instituição pública, de uma comunidade local, um organismo de empresa privada que faz a gestão de um serviço público, deve estar em conformidade com a legislação ou acto regulamentar adoptado, mediante um parecer da autoridade de protecção.

Esse processamento de dados diz respeito:

a) À segurança do Estado, defesa ou segurança pública;

b) A prevenção, investigação, detecção ou julgamento de infracções penais ou execução de condenações penais ou ainda de medidas de segurança;

c) Ao inquérito populacional;

d) Aos dados pessoais que indicam, directa ou indirectamente, as origens rácicas, étnicas ou regionais, filiação, opiniões políticas, filosóficas ou religiosas, ou ainda, filiação sindical das pessoas ou ainda as informações relativas à saúde ou vida sexual pessoal.

6. Os pedidos de parecer, as declarações e os pedidos de autorização devem indicar:

a) A identidade e o endereço do responsável pelos dados ou, se essa pessoa não residir no território de um Estado-membro da União Africana, a identidade e o endereço do seu representante, devidamente mandatado;

b) A(s) finalidade(s) do processamento de dados assim como a descrição geral das suas funções;

c) As interconexões previstas ou todas as outras formas de harmonização com outras actividades de processamento;

d) Os dados pessoais processados, a sua origem e as categorias das pessoas envolvidas no processamento;

e) Período de conservação dos dados processados;

f) O serviço ou serviços responsáveis pelo processamento de dados bem como as categorias das pessoas que, devido às exigências das funções ou do serviço, têm acesso directo aos dados registados;

g) Os destinatários autorizados a receber a transmissão de dados;

h) A função da pessoa ou do serviço perante o qual é exercido o direito de acesso;

i) As medidas tomadas para garantir a segurança das acções de processamento e de dados;

j) A indicação relativa ao uso de um subcontratado;

k) A transferência prevista de dados pessoais para um terceiro país que não seja membro da União Africana, sujeito a reciprocidade.

7. A autoridade nacional deve pronunciar-se dentro de um prazo fixo, contado a partir da recepção do pedido de parecer ou de autorização. Todavia, esse prazo pode ser prorrogado ou não, por decisão fundamentada da autoridade nacional de protecção.

8. A notificação, a declaração ou o pedido de autorização pode ser enviado à autoridade nacional de protecção por via electrónica ou correio.

9. A autoridade nacional de protecção pode ser contactada por qualquer pessoa, agindo em seu próprio nome, através do seu advogado ou por intermédio de uma outra pessoa, singular ou colectiva, devidamente mandatada.

Secção II: Quadro Institucional da Protecção de Dados de Carácter Pessoais

Artigo 11º
Estatuto, Composição e Organização das Autoridades Nacionais de Protecção de Dados de Pessoais

1. a) Cada Estado Parte deve criar uma autoridade responsável pela protecção de dados pessoais.

b) A autoridade nacional de protecção é um órgão administrativo independente e autónomo, com a tarefa de garantir que o processamento de dados pessoais seja feito em conformidade com as disposições da presente Convenção.

2. A autoridade nacional de protecção deve informar as pessoas interessadas e os funcionários responsáveis pelo processamento de dados sobre os seus direitos e suas obrigações.

3. Sem prejuízo das disposições do Artigo 11º (6), cada Estado Parte determina a composição da autoridade nacional de protecção de dados pessoais.

4. Funcionários ajuramentados podem ser convidados a participar na realização de missões de auditoria, em conformidade com as disposições em vigor nos Estados Partes.

5. a) Os membros da autoridade nacional de protecção estão sujeitos a obrigação do sigilo profissional, em conformidade com a legislação em vigor em cada Estado Parte.

b) Cada autoridade nacional de protecção elabora um regimento interno contendo, *inter alia,* normas que regulam as deliberações, o processamento e apresentação de casos.

6. O membro de uma autoridade nacional de protecção não deve ser um membro do Governo, nem pessoa que exerce funções executivas e possui acções em empresas no sector de tecnologias de informação; e.

7. a) Sem prejuízo das legislações nacionais, os membros das autoridades nacionais de protecção gozam de imunidade total em relação às opiniões expressas durante o exercício ou em conexão com o exercício das suas funções.

b) No exercício das suas atribuições, eles não recebem instruções de nenhuma autoridade.

8. Os Estados Partes comprometem-se a dotar as autoridades de protecção de recursos humanos, técnicos e financeiros necessários para o cumprimento da sua missão.

Artigo 12º
Atribuições e Competências das Autoridades Nacionais de Protecção

1. As autoridades nacionais de protecção devem garantir que o processamento de dados pessoais nos Estados-membros da União Africana seja feito em conformidade com as disposições da presente Convenção.

2. As autoridades nacionais de protecção devem assegurar que as Tecnologias de Informação e Comunicação não constituam uma ameaça às liberdades públicas e à vida privada dos cidadãos. Para este fim, elas têm como responsabilidade:

a) Responder a qualquer pedido de parecer sobre o processamento de dados pessoais;

b) Informar as pessoas interessadas e aos responsáveis pelo tratamento dos dados sobre os seus direitos e as suas obrigações;

c) Autorizar o processamento de ficheiros, em determinados casos, especialmente os ficheiros sensíveis;

d) Receber as formalidades prévias para o processamento de dados pessoais;

e) Receber as reclamações, petições e as queixas relativas ao processamento de dados pessoais e informar os seus autores sobre os resultados inerentes a esta matéria;

f) Informar, de imediato, a autoridade judiciária sobre determinados tipos de infracções de que tiver conhecimento;

g) Proceder, através dos seus funcionários ou de funcionários ajuramentados, à auditoria de todos os dados pessoais processados;

h) Impor sanções administrativas e pecuniárias, sobre os controladores de dados;

i) Actualizar o directório de dados pessoais processados que é acessível ao público;

j) Aconselhar as pessoas e os organismos que fazem o processamento de dados pessoais ou que fazem ensaios ou experiências susceptíveis de culminar com o processamento de dados;

k) Autorizar a transferência transfronteiriça de dados pessoais;

l) Formular sugestões susceptíveis de simplificar e melhorar o quadro legislativo e regulamentar para o processamento de dados;

m) Estabelecer mecanismos de cooperação com as autoridades de protecção de dados pessoais de outros países;

n) Participar em negociações internacionais em matéria de protecção de dados pessoais;

o) Elaborar relatório de actividades, de acordo com uma periodicidade claramente definida, a ser submetido às autoridades competentes do Estado Parte.

3. As autoridades nacionais de protecção podem decidir sobre as seguintes medidas:

   a) Uma advertência a qualquer responsável pelos dados que não cumprir com as obrigações decorrentes da presente Convenção;

   b) Um aviso oficial no sentido de por termo a tais violações dentro de um prazo fixado pela autoridade.

4. Caso o responsável pelos dados não cumpra o estipulado na carta de aviso oficial a si dirigido, a autoridade nacional de protecção pode, depois de processo contraditório, impor as seguintes sanções:

   a) Retirada provisória da autorização concedida;

   b) Retirada definitiva da autorização;

   c) Aplicar uma multa pecuniária.

5. Em caso de urgência, quando o processamento ou o uso de dados pessoais resultar na violação de direitos fundamentais e liberdades, a autoridade nacional de protecção pode, após processo contraditório, decidir o seguinte:

   a) A interrupção da realização do processamento de dados;

   b) O bloqueio de alguns dos dados pessoais processados;

   c) Proibição temporária ou definitiva de qualquer processamento de dados contrários às disposições da presente Conversão.

6. As sanções impostas e as decisões tomadas pelas autoridades nacionais de protecção podem ser objecto de recurso.

Secção III: Obrigações Relativas às Condições de Processamento de Dados Pessoais

Artigo 13º
Princípios de Base que Regem o Processamento de Dados Pessoais

Princípio 1: Princípio de Consentimento e de Legitimidade do Processamento de Dados Pessoais

O processamento de dados pessoais é considerado legítimo quando o titular dos dados der o seu consentimento. Todavia, este requisito pode ser revogado quando o processamento de dados se for necessário para:

a) Cumprimento de uma obrigação legal à qual o controlador de dados se subordina;

b) Execução de uma missão de interesse público, no exercício de autoridade pública conferida ao controlador de dados ou a uma terceira parte, a que os dados serão submetidos;

c) Execução de um contrato ao qual o titular dos dados é parte ou a fim de tomar medidas a pedido do titular dos dados, antes de celebrar um contrato;

d) Salvaguarda de interesses vitais ou dos direitos fundamentais e liberdades do titular dos dados.

Princípio 2 : Princípio da legalidade e da lealdade do processamento de dados pessoais

A recolha, o registo, processamento, armazenamento e transmissão de dados pessoais devem ser feitos de uma forma lícita, justa e não fraudulenta.

Princípio 3º: Princípio de finalidade, pertinência, conservação e do processamento de dados pessoais

a) A recolha de dados deve ser feita para fins específicos, explícitos e legítimos, não devendo ser processados posteriormente de uma maneira incompatível com esses fins;

b) Os dados devem ser adequados, pertinentes e não excessivos em relação à finalidade para a qual foram recolhidos e processados;

c) Os dados devem ser conservados durante um prazo que não excede o período necessário para a finalidade para a qual foram recolhidos ou processados;

d) Para além deste período exigido, os dados podem ser conservados apenas necessidades específicas do processamento de dados realizado para fins históricos ou de pesquisa ao abrigo da lei.

Princípio 4: Princípio de exactidão dos dados pessoais

Os dados recolhidos devem ser exactos e, se for necessário, mantê-los actualizados. Devem ser tomadas todas as medidas necessárias para garantir que os dados inexactos ou incompletos, tendo em conta os fins para os quais foram recolhidos e posteriormente processados, possam ser apagados ou rectificados.

Princípio 5: Princípio de transparência do processamento de dados pessoais

O princípio de transparência implica uma formação obrigatória da pessoa responsável pelo tratamento dos dados pessoais.

Princípio 6: Princípio de confidencialidade e de segurança no processamento de dados pessoais

a) Os dados pessoais devem ser processados num ambiente confidencial e serem protegidos, principalmente quando o processamento envolve transmissão de dados através de uma rede.

b) Quando o processamento é feito por conta do responsável pelos dados, este deve escolher um processador que oferece garantias suficientes. Compete ao controlador e ao processador garantir o cumprimento das medidas de segurança definidas na presente Convenção.

Artigo 14º
Princípios específicos relativos ao processamento de dados sensíveis

1. Os Estados Partes comprometem-se a proibir qualquer recolha e processamento de dados que revelam a origem racial, étnica ou regional, filiação, ideologia, políticas, crenças religiosas ou convicções filosóficas, filiação sindical, vida sexual, informação genética ou, de uma forma geral, as informações relativas ao estado de saúde do titular dos dados.

2. A proibição estabelecida no Artigo 14º (1) não se aplica para as categorias de processamento que se seguem, quando:

   a) O processamento de dados pessoais estão manifestamente tornadas públicas pelo sujeito titular dos dados;

   b) O sujeito titular dos dados tiver dado o seu consentimento por escrito, usando qualquer meio que seja, ao processamento e em conformidade com a legislação em vigor;

   c) O processamento de dados pessoais for necessário para proteger os interesses vitais do titular dos dados ou de uma outra pessoa, se o sujeito titular dos dados estiver física ou juridicamente incapacitado para dar o seu consentimento.

   d) O processamento, particularmente de informações genéticas, for necessário para o estabelecimento, exercício ou defesa de reivindicações legais;

   e) Um processo judicial ou uma investigação penal tiver sido iniciado;

f) O processamento for necessário no interesse público, especialmente para fins históricos, estatísticos ou científicos;

g) O processamento for necessário para a execução de um contrato para o qual o titular dos dados é parte ou para tomar medidas a pedido do sujeito titular dos dados antes da celebração do contrato;

h) O processamento for necessário para o cumprimento de uma obrigação legal ou regulamentar ao qual o sujeito titular dos dados está vinculado;

i) O processamento de dados for necessário para a execução de uma missão no interesse público ou no exercício de competências oficiais ou assinado por uma autoridade pública delegada na pessoa do controlador de dados ou numa terceira parte a quem os dados são apresentados;

j) O processamento de dados for efectuado no quadro de actividades legítimas de uma fundação, uma associação ou de um outro organismo sem fins lucrativos e com fins políticos, filosóficos, religiosos, cooperativistas ou sindicais, e sob condições em que o processamento se relaciona exclusivamente aos membros do organismo ou pessoas que têm contacto regular com ele em conexão com os propósitos e que os dados não sejam revelados a terceiros sem consentimento dos sujeitos titulares dos mesmos.

3. O processamento dos dados pessoais, realizado para fins jornalísticos, de investigação, artísticos ou de expressão literária é aceitável quando for feito apenas para fins de expressão literária, artística ou de exercício profissional da actividade jornalística ou de investigação, de acordo com código de conduta dessas profissões.

4. As disposições da presente Convenção não excluem a aplicação das disposições das legislações nacionais relativas à imprensa escrita ou ao sector audiovisual, assim como as disposições do código penal, que prevêem as condições do exercício do direito de resposta e previnem, limitam, concertam e, se for necessário, reprimem as violações de privacidade e danos à reputação pessoal.

5. Uma pessoa não deve sujeitar-se a uma decisão que produz efeitos jurídicos a si mesmo, ou afecta muito significativamente e com base unicamente no processamento automático dos dados destinados a avaliar certos aspectos pessoais referentes a ela.

6. a) O responsável pelos dados não deve transferir dados pessoais para um Estado não membro da União Africana, salvo quando tal Estado garante um nível adequado de protecção suficiente da privacidade,

das liberdades e dos direitos fundamentais das pessoas cujos dados estão a ser ou podem ser processados.

b) A proibição anterior não se aplica quando, antes de transferência de quaisquer dados pessoais para um terceiro país, o responsável pelos dados solicitar previamente a permissão dessa transferência à autoridade nacional de protecção.

Artigo 15º
Interconexão de Ficheiros que Contêm Dados Pessoais

A interconexão de ficheiros fixada no Artigo 10º (4) da presente Convenção deve ajudar para o alcance dos objectivos legais ou estatutários que são de legítimo interesse dos controladores de dados. A referida interconexão não dever levar à discriminação ou à limitação dos direitos, liberdades e garantias dos sujeitos titulares de dados, mas deve estar sujeita a medidas de segurança apropriadas bem como tomar em conta o princípio de relevância dos dados que estão a ser interconectados.

Secção IV: Direitos do Sujeito Titular dos Dados

Artigo 16º
Direito à informação

O responsável pelos dados deve fornecer à pessoa singular cujos dados são objectos de processamento, o mais tardar até à data da recolha de dados e independentemente dos meios e facilidades usadas, com a seguinte informação:

a) A sua identidade e, se houver, a do seu representante;
b) A finalidade do processamento para a qual se destinam os dados;
c) As categorias dos dados abrangidos;
d) Possíveis destinatários dos dados;
e) Capacidade de solicitar que seja retirado do ficheiro;
f) A existência de um direito de acesso e de rectificar os dados que lhe dizem respeito;
g) Período de conservação dos dados;
h) Proposta de transferência de dados para um país terceiro.

Artigo 17º
Direito de acesso

Qualquer pessoa singular, cujos dados pessoais estão para ser processados, pode solicitar ao responsável pelos dados, o acesso aos seus dados, sob a forma das seguintes perguntas:

a) Informações que a permitam conhecerem e contestar o processamento;

b) Confirmação de que os dados pessoais são ou não objecto de processamento;

c) Comunicação de dados pessoais passando o processamento e qualquer informação disponível como a sua origem;

d) Informações relativas à finalidade do processamento, categorias dos dados pessoais processados, destinatários ou categorias dos destinatários para quem os dados são submetidos.

Artigo 18º
Direito de oposição

Qualquer pessoa singular tem o direito de se opor, por razões legítimas, a que dados pessoais que lhe dizem respeito sejam objecto de um processamento.

Ela tem o direito de ser informada antes de os dados pessoais que lhe dizem respeito serem revelados, pela primeira, a terceiros ou serem utilizados em nome de terceiros para fins de marketing e, assiste-lhe o direito de se opor, gratuitamente, a tal revelação ou utilização de tais dados.

Artigo 19º
Direito de rectificação e supressão

Qualquer pessoa singular pode exigir ao responsável dos dados que os seus dados sejam, segundo o caso, rectificados, completados, actualizados, bloqueados ou suprimidos por serem inexactos, incompletos, equívocos, desactualizados ou cuja recolha, utilização, revelação ou conservação sejam proibidas.

Secção V: Obrigações do Responsável dos Dados Pessoais

Artigo 20º
Obrigações de confidencialidade

O processamento de dados pessoais é confidencial. É efectuado exclusivamente por indivíduos que agem sob a autoridade do responsável dos dados e somente sob as suas instruções.

Artigo 21º
Obrigações de segurança

O responsável pelos dados deve tomar todas as precauções apropriadas, de acordo com a natureza dos dados e, em particular, evitar que esses dados sejam alterados ou destruídos, utilizados por pessoas não autorizadas.

Artigo 22º
Obrigações de conservação

Os dados pessoais não devem ser conservados para além do período necessário para fim pelo qual se fez a sua recolha e o seu processamento.

Artigo 23º
Obrigações de manutenção

a) O responsável pelos dados deve tomar todas as medidas necessárias com vista a assegurar que os dados pessoais processados possam ser explorados independentemente do dispositivo técnico utilizado no processo.

b) O funcionário que faz o processamento deve, em particular, assegurar que as mudanças tecnológicas não constituam um obstáculo para a utilização dos dados.

CAPÍTULO III – PROMOÇÃO DA CIBERSEGURANÇA E A LUTA CONTRA O CIBERCRIME

Secção I: Medidas de Cibersegurança a Serem Tomadas ao Nível Nacional

Artigo 24º
Quadro da Cibersegurança Nacional

1. Política nacional

Cada Estado Parte deve desenvolver, em colaboração com as outros actores, uma política nacional de cibersegurança que reconhece a importância da Infra-estrutura da Informação Crítica (IIC) para o país identificar os riscos que enfrenta ao da utilizar uma abordagem perigosa e define como é que se pode alcançar os objectivos dessa política.

2. Estratégia nacional

Os Estados Partes devem adoptar as estratégias que considerarem apropriadas e suficientes para a implementação da política nacional de cibersegurança, especialmente nos domínios da reforma legislativa e desenvolvimento,

sensibilização e desenvolvimento de capacidades, parceria público-privada e cooperação internacional, entre outras coisas. Tais estratégias deverão definir estruturas organizacionais e fixar os objectivos assim como os prazos, com vista a uma boa execução da política de cibersegurança e criar as bases de uma gestão efectiva dos incidentes de cibersegurança e a cooperação internacional.

Artigo 25º
Medidas legais

1. Legislação de Combate ao Cibercrime

Cada Estado Parte deve adoptar as medidas legislativas e/ou regulamentares que julgar eficazes, considerando como infracções criminais substantiva os actos que afectam a confidencialidade, integridade, disponibilidade e sobrevivência dos sistemas das tecnologias de informação e comunicação, os dados que eles processam e as infra-estruturas de rede subjacentes, assim como as medidas consideradas eficazes para a busca e julgamento dos criminosos. Os Estados Partes devem tomar em consideração a escolha da linguagem que é utilizada nas melhores práticas internacionais.

2. Autoridades Reguladoras Nacionais

Cada Estado Parte deve adoptar medidas legislativas e/ou regulamentares que julgar necessárias para conferir a responsabilidade específica às instituições – quer instituições já existentes, quer novas – assim como aos funcionários dessas instituições que forem designados, a fim de lhes conferir a autoridade estatutária e a capacidade legal de agir em todos os aspectos da aplicação à cibersegurança, não se limitando a dar resposta aos incidentes este domínio, coordenação e cooperação em matéria da justiça de reparadora, investigações forense, julgamentos, etc.

3. Direitos dos cidadãos

Ao adoptar as medidas legais e/ou regulamentares em matéria da cibersegurança e ao criar o respectivo quadro de aplicação, cada Estado Parte deve assegurar que as medidas adoptadas não infrinjam os direitos dos cidadãos garantidos pela constituição nacional, pelo direito interno e protegidos pelas convenções internacionais, em particular pela Carta Africana dos Direitos Humanos e dos Povos, bem como outros direitos fundamentais, tais como o direito à liberdade de expressão, o direito à privacidade e o direito a uma audição justa, entre outros.

4. Protecção de infra-estruturas críticas

Cada Estado Parte deve adoptar as medidas legislativas e/ou regulamentares que julgar necessárias para a identificação dos sectores considerados sensíveis para a sua segurança nacional e o bem-estar da economia e dos sistemas das tecnologias de informação e comunicação, destinadas a funcionar nesses sectores como infra-

estruturas críticas de informação; e neste contexto, propor, sanções mais severas para as actividades criminosas sobre os sistemas das TIC nestes sectores, incluindo a tomada de disposições que visam a melhoria da vigilância, da segurança e gestão.

Artigo 26º
Sistema nacional de Cibersegurança

1. Cultura de Cibersegurança

a) Cada Estado Parte compromete-se a promover a cultura de cibersegurança entre todos os actores, nomeadamente instituições governamentais, empresas e a sociedade civil, que desenvolvem, possuem, gerem, implementam e utilizam os sistemas e as redes de informação. A cultura de cibersegurança deve pôr ênfase na segurança no desenvolvimento de sistemas e redes de informação, incluindo a adopção de novas formas de pensamento e comportamento durante a utilização dos sistemas de informação, bem como durante a comunicação e transacções comerciais nas redes.

b) Como parte da promoção da cultura de cibersegurança, os Estados Partes podem adoptar as seguintes medidas: a criação de um plano de cibersegurança para os sistemas geridos pelos seus governos; elaboração e implementação de programas e iniciativas de sensibilização sobre segurança aos utilizadores dos sistemas e das redes; incentivar o desenvolvimento de uma cultura de cibersegurança nas empresas; promoção do envolvimento da sociedade civil; lançamento de um programa nacional abrangente e detalhado; sensibilização para os usuários da Internet, pequenas empresas, escolas e crianças.

2. Papel dos governos

Cada Estado Parte compromete-se a liderar o desenvolvimento da cultura de cibersegurança dentro das suas fronteiras. Os Estados-membros da União Africana comprometem-se a sensibilizar, educar, formar, bem como difundir as informações junto do público desta matéria.

3. Parceria público-privada

Cada Estado Parte deve desenvolver uma parceria público-privada como modelo para envolver a indústria, a sociedade civil e a comunidade académica na promoção e no reforço de uma cultura de cibersegurança.

4. Educação e Formação

Cada Estado Parte deve adoptar medidas que visam o reforço de capacidade, de tal modo a providenciar uma formação que cobre todas as áreas de cibersegurança para os diferentes actores da Sociedade de Informação e fixar normas para o sector privado.

Os Estados Partes comprometem-se a promover a educação técnica dos profissionais das tecnologias de informação e comunicação, dentro e fora das instituições governamentais, através da certificação e da normalização da formação, categorização das qualificações profissionais, desenvolvimento e distribuição do material educativo, em função das necessidades.

Artigo 27º
Estruturas nacionais de Acompanhamento da Cibersegurança

1. Gestão da Cibersegurança

a) Cada Estado Parte deve adoptar as medidas necessárias com vista à criação de um mecanismo institucional apropriado responsável pela gestão da cibersegurança.

b) As medidas adoptadas no parágrafo 1 do presente Artigo devem criar uma forte liderança e um envolvimento em diferentes aspectos das instituições da cibersegurança, bem como das entidades profissionais competentes dos Estados Partes. Para este fim, os Estados Partes devem tomar as medidas necessárias para:

   i) Estabelecer uma responsabilização clara em matéria da cibersegurança a todos os níveis do governo, através de uma definição precisa de papéis e responsabilidades;

   ii) Exprimir um compromisso claro, público e transparente em matéria da cibersegurança;

   iii) Encorajar o sector privado, solicitando o seu envolvimento e a sua participação nas iniciativas dirigidas pelo governo para fins da promoção da cibersegurança.

c) A gestão da cibersegurança deve ser criada dentro de um quadro nacional capaz de responder aos desafios actuais assim como a quaisquer questões relativas à segurança da informação ao nível nacional, no maior número possível das áreas da cibersegurança.

2. Quadro institucional

Cada Estado-membro deve adoptar as medidas que julgar necessárias para fins de criação de instituições competentes para o combate do cibercrime cibernética, dar

uma resposta a incidentes e outros alertas, assegurar a coordenação nacional e transfronteiriça dos problemas da cibersegurança, incluindo a cooperação global.

Artigo 28
Cooperação internacional

1. Harmonização

Os Estados Partes devem garantir que as medidas legislativas e/ou regulamentares adoptadas para lutar contra o cibercrime reforcem a possibilidade de harmonização regional destas medidas e respeitem o princípio da dupla responsabilidade criminal.

2. Cooperação judiciária

Os Estados Partes que não têm acordos de assistência mútua em matéria da cibercriminalidade são incentivados a assinar acordos de assistência judiciária mútua, em conformidade com o princípio da dupla responsabilidade penal, promovendo ao mesmo tempo a troca de informações e partilha eficiente de dados entre as organizações dos Estados Partes no âmbito bilateral e multilateral.

3. Troca de informações

Os Estados Partes devem incentivar a criação de instituições que trocam informações sobre ciberameaças bem como a avaliação da vulnerabilidade, tais como a Equipa de Resposta a Emergências Informáticas *(CERT–Computer Emergency Response Team)* ou as Equipas de Resposta a Incidentes no Domínio da Cibersegurança *(CSIRTS: Computer SecurityIncident Response Teams)*.

4. Meios de cooperação

Os Estados Partes devem fazer uso dos meios existentes de cooperação internacional, a fim de responder a ciberameaças, melhorar a cibersegurança e promover o diálogo entre os actores. Estes meios poderão ser internacionais, intergovernamentais ou regionais ou ainda baseados nas parcerias públicas privadas.

Secção II: Disposições penais

Artigo 29º
Ofensas Específicas Contra as Tecnologia de Informação e Comunicação

1. Ataques contra Sistemas Informáticos

Os Estados Partes devem tomar medidas legislativas ou regulamentares necessárias para a criminalização penal dos seguintes actos:

a) Aceder ou tentar aceder, sem autorização, a todo ou parte do sistema informático ou ultrapassar o acesso autorizado;

b) Aceder ou tentar aceder, sem autorização, a todo ou parte do sistema informático ou ultrapassar o acesso autorizado, com a intenção de cometer uma nova infracção ou facilitar a prática dessa ofensa;

c) Manter-se ou tentar manter-se de forma fraudulenta, no seu todo ou parte de um sistema informático;

d) Dificultar, distorcer ou tentar dificultar ou distorcer o funcionamento de um sistema informático.

e) Introduzir ou tentar introduzir fraudulentamente dados num sistema informático;

f) Causar danos ou tentar causar, apagar ou tentar apagar, deteriorar ou tentar deteriorar, alterar ou tentar alterar, modificar ou tentar modificar fraudulentamente dados informáticos.

Os Estados Partes devem igualmente:

g) Adoptar normas que obrigam os vendedores de produtos de tecnologias de informação e comunicação a realizar, através de peritos ou investigadores independentes na área da cibersegurança, ensaios de vulnerabilidade e avaliações da garantia de segurança e divulgar aos consumidores todas as vulnerabilidades detectadas nos produtos assim como as soluções recomendadas para a sua correcção;

h) Tomar medidas legislativas e/ou regulamentares necessárias para criminalização penal a, produção, venda, importação, posse, disseminação, oferta, cedência ou oferta de um equipamento, um programa informático, qualquer dispositivo ou dado concebido ou adaptado especialmente para cometer infracções ou uma senha semelhantes que permitem aceder a todo ou parte de um sistema informático ilegalmente.

2. Violações de Dados informatizados

Os Estados Partes devem tomar medidas legislativas o/eu regulamentares necessárias para criminalização penal dos seguintes actos:

a) Interceptar ou tentar interceptar fraudulentamente, através de meios técnicos, dados informatizados durante a sua transmissão não pública para, de ou dentro de um sistema informático;

b) Introduzir, alterar, apagar ou suprimir intencionalmente dados informáticos, criando dados não originais, com a intenção de serem

considerados ou utilizados para fins legais como se fossem originais, independentemente de os dados serem directamente de fácil leitura ou percepção. Uma Parte pode exigir uma intenção fraudulenta ou uma intenção delituosa semelhante para que a responsabilidade penal seja iniciada;

c) Com conhecimento de causa, fazer o uso de dados obtidos de uma forma fraudulenta de um sistema de informática;

d) Obter fraudulentamente, para si ou para outrem, qualquer benefício, através da introdução, alteração, eliminação ou supressão de dados informatizados ou por meio de qualquer outra forma que interfere com o funcionamento de um sistema informático;

e) Por negligência, processar ou mandar processar dados pessoais sem respeitar as formalidades prévias de processamento;

f) Participar em uma associação formada ou num acordo estabelecido com vista a preparar ou cometer uma ou várias ofensas previstas na presente Convenção.

3. Infracções relativas ao conteúdo

1. Os Estados Partes devem tomar medidas legislativas e/ou regulamentares necessárias para incriminação penal dos seguintes actos:

a) Produzir, registar, oferecer, fabricar, disponibilizar, difundir, transmitir uma imagem ou uma representação de pornografia infantil, através de um sistema informático;

b) Adquirir para si próprio ou para outrem, importar ou mandar importar, exportar ou mandar exportar uma imagem ou uma representação de pornografia infantil, através de um sistema informático;

c) Possuir uma imagem ou uma representação de pornografia infantil num sistema informático ou em qualquer meio de armazenamento de dados informatizados;

d) Facilitar ou dar acesso a imagens, documentos, som ou representação de pornografia a um menor;

e) Criar, descarregar, difundir ou disponibilizar, sob qualquer forma escrita, mensagens, fotos, desenhos ou qualquer representação de ideias ou teorias de natureza racista e xenófoba, através de um sistema informático;

f) Ameaçar, através de um sistema informático, cometer uma infracção penal contra uma pessoa por pertencer a um grupo distinguido pela raça, cor da pele, descendência ou origem nacional ou étnica ou ainda a

religião, quando tal filiação serve de pretexto ou ideologia política, se for usado como pretexto para qualquer destes factores, ou contra um grupo de pessoas que se distingue por qualquer destas características; tendo em conta que essa filiação serve de pretexto a um desses elementos ou a um grupo de pessoas que se distingue por uma dessas características;

g) Insultar, através de um sistema informático, pessoas que pertencem a um grupo que se distingue pela raça, cor da pele, descendência ou origem nacional ou étnica ou ainda a religião, quando tal filiação serve de pretexto ou ideologia política, se for usado como pretexto para qualquer destes factores, ou contra um grupo de pessoas que se distingue por qualquer destas características;

h) Negar, deliberadamente, aprovar ou justificar actos constitutivos de genocídio ou de crimes contra a humanidade através de um sistema informático.

2. Os Estados Partes devem tomar as medidas legislativas e/ou regulamentares necessárias para incriminar penalmente as infracções previstas na presente Convenção.

Quando essas infracções forem cometidas sob a égide de uma organização criminosa serão punidas com as penas máximas previstas para a infracção em causa.

3. Os Estados Partes comprometem-se a tomar as medidas legislativas e/ou regulamentares necessárias para fazer com que, em caso de condenação, os tribunais nacionais possam decidir sobre a confiscação dos materiais, instrumentos, programas informáticos ou quaisquer dispositivos que pertencem ao condenado e que tenham servido para cometer as infracções mencionadas na presente Convenção.

4. Infracções relativas às medidas de segurança das trocas comerciais electrónicas

Os Estados Partes devem tomar as medidas legislativas e/ou regulamentares necessárias para que a prova digital em casos penais seja admitida, a fim de determinar as ofensas ao abrigo do direito penal interno, desde que essa prova tenha sido apresentada durante o processo judicial e discutida perante o Juiz, que a pessoa de quem é originária pode ser devidamente identificada, que foi feita e guardada de modo que possa assegurar a sua integridade.

Artigo 30º
Adaptação de Algumas Infracções às Tecnologias de Informação e Comunicação

1. Ofensas Contra a Propriedade

a) Os Estados Partes devem tomar as medidas legislativas e/ou regulamentares necessárias para incriminação penal das violações contra a propriedade tais como o furto, a fraude, transacção de bens roubados, abuso de confiança, extorsão de dinheiro e chantagem envolvendo dados informáticos;

b) Os Estados Partes devem tomarem medidas legislativas ou regulamentares necessárias para considerar como circunstâncias agravantes, o uso das tecnologias de informação e comunicação na prática de ofensas tais como, o furto, fraude, transacção de bens roubado, abuso de confiança, extorsão de dinheiro, terrorismo e branqueamento de capital;

c) Os Estados Partes devem tomar medidas legislativas e/ou regulamentares necessárias para incluir especificamente "pelos meios de comunicação electrónica digital" tais como a Internet na listagem dos meios de difusão pública previstos nas leis penais dos Estados Membros;

d) Os Estados Partes devem tomar as medidas legislativas penais necessárias destinadas a restringir o acesso aos sistemas protegidos que foram classificados como infra-estruturas críticas de defesa nacional, devido aos dados críticos da segurança nacional que eles contêm.

2. Responsabilidade penal das pessoas colectivas

Os Estados Partes devem tomar as medidas legislativas necessárias para garantir que as pessoas colectivas, para além do Estado, as comunidades locais e as instituições públicas possam ser responsabilizadas pelas infracções previstas na presente Convenção, cometidas em nome dos seus órgãos ou seus representantes. A responsabilidade das pessoas colectivas não exclui a das pessoas singulares que são autoras ou cúmplices na prática das mesmas infracções.

Artigo 31º
Adaptação de Algumas Sanções às Tecnologias de Informação e Comunicação

1. Sanções penais

a) Os Estados Partes devem tomar medidas legislativas necessárias para garantir que as ofensas previstas ao abrigo da presente Convenção sejam punidas com penas apropriadas nos termos das legislações nacionais;

b) Os Estados Partes devem tomar medidas legislativas necessárias para assegurar que as ofensas previstas na presente Convenção sejam punidas com penas apropriadas, nos termos das suas respectivas legislações nacionais;

c) Os Estados Partes devem tomar medidas legislativas necessárias para assegurar que uma pessoa colectiva considerada responsável nos termos da presente Convenção seja punida com sanções efectivas, proporcionais e dissuasiva, incluindo multas penais.

2. Outras sanções penais

a) Os Estados Partes devem a tomar as medidas legislativas necessárias para assegurar que, em caso de condenação por uma infracção cometida através de um meio de comunicação digital, o tribunal competente possa decidir sobre sanções adicionais;

b) Os Estados Partes devem tomar as medidas necessárias para que, em caso de condenação por uma infracção cometida através de um meio de comunicação digital, o Juiz pode ordenar, a divulgação obrigatória, a expensas do condenado, um extracto da decisão, através do mesmo meio e de acordo com as modalidades prescritivas pelas mesmas penas como aquelas aplicáveis por violação do sigilo profissional;

c) Os Estados Partes devem tomar as medidas legislativas necessárias para assegurar que uma violação de confidencialidade dos dados armazenados num sistema informático seja punida com as mesmas penas aplicáveis à violação do segredo profissional.

3. Direito processual

a) Os Estados Partes devem tomar as medidas legislativas necessárias para assegurar que, quando os dados armazenados num sistema informático ou num meio que permite o armazenamento de dados informatizados no território de um Estado Parte são úteis para estabelecer a verdade, o tribunal competente pode fazer um busca para aceder a todos ou parte do sistema informático através de outro sistema

informático, onde os dados referidos são acessíveis ou disponíveis para o sistema inicial;

b) Os Estados Partes devem tomar as medidas legislativas necessárias para assegurar que, caso a autoridade judiciária encarregue pela instrução descobrir, num sistema informático, dados armazenados que são úteis para o estabelecimento da verdade, mas a confiscação do suporte não parece ser apropriada, os referidos dados, bem como todos aqueles dados necessário para sua compreensão, devem ser copiados em dispositivos de armazenamento informático que possam ser confiscados e selados, de acordo com as modalidades previstas ao abrigo das legislações dos Estados Partes;

c) Os Estados Partes devem tomar as medidas legislativas necessárias para assegurar que as autoridades judiciárias possam, para fins de investigação ou de execução de um mandato judiciário, realizar as operações previstas na presente Convenção;

d) Os Estados Partes devem tomar as medidas legislativas necessárias para assegurar que, quando as necessidades de informação assim o exigirem, particularmente se houver motivos para acreditar que a informação armazenada num sistema informático é particularmente susceptível de se perder ou ser alterada, o juiz de instrução pode impor uma injunção sobre qualquer pessoa a fim de proteger a integridade dos dados em sua posse ou sob seu controlo, por um período máximo de dois anos, a fim de garantir o curso normal da investigação. Espere-se que depositário dos dados ou outra pessoa responsável pela sua conservação mantenha sigilo em relação aos dados;

e) Os Estados Partes devem tomar as medidas legislativas necessárias para assegurar que, quando as necessidades da informação o assim exigirem, o juiz de instrução pode usar os meios técnicos apropriados para a recolha ou o registo, em tempo real, dos dados relativos ao conteúdo de comunicações específicas no seu território, transmitidas através de um sistema informático, ou obrigar um provedor de serviços, no quadro das suas capacidades técnicas, para recolher ou registar, usando os meios técnicos existentes no seu território ou nos territórios dos Estados Partes, ou prestar apoio às autoridades competentes para a recolha e registo dos referidos dados informatizados.

CAPÍTULO IV
DISPOSIÇÕES FINAIS

Artigo 32º
Medidas a Serem Tomadas ao Nível da União Africana

O Presidente da Comissão deve apresentar um relatório à Cimeira sobre a criação e acompanhamento do mecanismo operacional da presente Convenção.

O mecanismo de acompanhamento a ser criado deve garantir o seguinte:

a) Promover e incentivar o Continente a adoptar e implementar medidas que visam o reforço da cibersegurança nos serviços electrónicos e na luta contra o cibercrime bem como a violação dos direitos humanos no ciberespaço;

b) Juntar documentos e informações sobre as necessidades de cibersegurança, assim como a natureza e a dimensão do cibercrime e das violações dos direitos humanos no ciberespaço;

c) Desenvolver métodos para analisar as necessidades da cibersegurança, assim como a natureza e a dimensão do cibercrime e as violações contra os direitos humanos no ciberespaço, difundir a informação e sensibilizar o público sobre os efeitos negativos destes fenómenos;

d) Assessorar os governos africanos sobre a maneira de promover a cibersegurança e lutar contra o flagelo do cibercrime e as violações dos direitos humanos no ciberespaço a nível nacional;

e) Recolher informações e fazer análises sobre o comportamento criminoso dos usuários das redes e dos sistemas de informação que operam em África e transmitir essas informações às autoridades nacionais competentes;

f) Elaborar e promover a adopção de códigos de conduta harmonizados para ser utilizado pelos funcionários públicos em matéria de cibersegurança;

g) Criar parcerias com a Comissão e o Tribunal Africano dos Direitos Humanos e dos Povos, a sociedade civil africana, organizações governamentais, intergovernamentais e não-governamentais, a fim de facilitar o diálogo sobre o combate contra o cibercrime e violações dos direitos humanos no ciberespaço;

h) Submeter relatórios regulares ao Conselho Executivo da União Africana sobre os progressos realizados por cada Estado Parte na aplicação das disposições da presente Convenção;

i) Realizar quaisquer outras actividades relativas ao cibercrime e violações dos direitos humanos no ciberespaço de indivíduos que lhe podem ser confiadas pelos órgãos deliberativos da União Africana.

Artigo 33º
Disposições de Salvaguarda

As disposições da presente Convenção não podem ser interpretadas de uma forma inconsistente com os princípios pertinentes do Direito Internacional, incluindo o Direito Costumeiro Internacional.

Artigo 34º
Resolução de Litígios

1. Qualquer litígio que possa surgir da presente Convenção deve ser resolvido de uma forma amigável, por via de negociação directa entre os Estados Partes interessados.

2. Quando o litígio não poder ser resolvido pela via de negociação directa, os Estados Partes devem esforçar-se por resolvê-lo usando outros meios pacíficos, incluindo os bons ofícios, a mediação, a conciliação ou qualquer outro meio pacífico acordado pelas Partes. A este respeito, os Estados Partes são encorajados a recorrer aos procedimentos e mecanismos de resolução de litígios estabelecidos no quadro da União Africana.

Artigo 35º
Assinatura, Ratificação e Adesão

A presente Convenção está aberta a todos os Estados-membros da União Africana para assinatura, ratificação e adesão, em conformidade com os seus respectivos procedimentos constitucionais.

Artigo 36º
Entrada em Vigor

A presente Convenção entra em vigor trinta (30) dias depois da recepção, pelo Presidente da Comissão da União Africana, do décimo quinto (15º) instrumento de ratificação ou de adesão.

Artigo 37º
Alterações

1. Qualquer Estado Parte pode submeter propostas de emendas ou de revisão à presente Convenção.

2. As propostas de emendas ou de revisão são submetidas ao Presidente da Comissão da União Africana que comunica aos Estados Partes, dentro de um prazo de trinta (30) dias depois da sua recepção.

3. A Cimeira da União, sob recomendação do Conselho Executivo, examina essas propostas na sessão seguinte, desde que todos os Estados Partes tenham sido notificados pelo menos três (3) meses antes do início da sessão.

4. A Cimeira da União adopta as emendas, em conformidade com o seu Regimento Interno.

5. As emendas ou as revisões entram em vigor ao abrigo das disposições do Artigo 36º da presente Convenção.

Artigo 38º
Depositário

1. Os instrumentos de ratificação ou de adesão são depositados junto do Presidente da Comissão da União Africana.

2. Qualquer Estado Parte pode retirar-se da presente Convenção notificando, por escrito, a sua intenção, com um (1) ano de antecedência ao Presidente da Comissão da União Africana.

3. O Presidente da Comissão da União Africana notifica os Estados-Membros sobre qualquer assinatura da presente Convenção, o depósito de qualquer instrumento de ratificação ou de adesão, assim como a sua entrada em vigor.

4. O Presidente da Comissão notifica igualmente os Estados-Membros sobre os pedidos de emendas ou de retirada da Convenção, assim como as reservas feitas.

5. Mediante a entrada em vigor da presente Convenção, o Presidente da Comissão da União Africana deve registá-la junto do Secretário-Geral da Organização das Nações Unidas, em conformidade com o Artigo 102º da Carta das Nações Unidas.

6. A presente Convenção, redigida em quatro (4) textos originais, em línguas Árabe, Inglês, Francês e Português, sendo todos os quatro (4) textos autênticos, é depositada junto do Presidente da Comissão da União Africana que envia uma cópia autenticada a cada Estado-Membro, na sua língua oficial.

ADOPTADA PELA VIGÉSIMA TERCEIRA SESSÃO ORDINÁRIA DA CIMEIRA, REALIZADA EM MALABO, GUINE EQUATORIAL

A 27 DE JUNHO DE 2014

****