2. Entrará em vigor doze meses após registo, pelo Director Geral, das ratificações de dois Membros.

3. Em seguida, esta Convenção entrará em vigor para cada Membro doze meses após a data em que tiver sido registada a sua ratificação.

ARTIGO 9.º

1. Qualquer Membro que tiver ractificado a presente Convenção poderá denunciá-la decorrido um período de dez anos, a contar da data da entrada em vigor inicial da Convenção, por comunicação enviada ao Director Geral da Repartição Internacional do Trabalho e por ele registada.

2. Qualquer Membro que tiver ractificado a presente Convenção e que, no prazo de um ano após ter expirado o período de dez anos mencionado no parágrafo anterior, não fizer uso da faculdade de denúncia prevista no presente artigo ficará obrigado por um novo período de dez anos e poderá depois denunciar a presente Convenção nas condições previstas neste artigo, no termo de cada período de dez anos.

ARTIGO 10.º

1. O Director Geral da Repartição Internacional do Trabalho participará a todos os Membros da Organização Internacional do Trabalho o registo de todas as ractificações e denúncias que lhe forem comunicadas pelos Membros da Organização.

2. Ao notificar os Membros da Organização do registo da segunda ractificação que lhe tiver sido comunicada, o Director Geral chamará a atenção dos Membros para a data da entrada em vigor da presente Convenção.

ARTIGO 11.º

O Director Geral da Repartição Internacional do Trabalho comunicará ao Secretário Geral das Nações Unidas, para efeitos de registo, de acordo com o artigo 102.º da Carta das Nações Unidas, informações completas sobre todas as ractificações e todos os actos de denúncia que tiver registado de acordo com os artigos anteriores.

ARTIGO 12.º

Sempre que o considere necessário, o Conselho de Administração da Repartição Internacional do Trabalho apresentará à Conferência Geral um relatório sobre a aplicação da presente Convenção e examinará a oportunidade de inscrever na ordem do dia da Conferência a questão da sua revisão total ou parcial.

ARTIGO 13.º

1. No caso de a Conferência adoptar uma nova convenção que implique revisão total ou parcial da presente Convenção, e salvo disposição em contrário da nova Convenção:

a) A ractificação por um Membro da nova Convenção revista implicará de pleno direito, não obstante o artigo 9.º, atrás referido, a denúncia imediata da presente Convenção, desde que a nova Convenção revista tenha entrado em vigor;

b) A partir da data da entrada em vigor da nova Convenção revista, a presente Convenção deixará de estar aberta à ractificação dos Membros.

2. A presente Convenção manter-se-á em todo o caso em vigor na sua forma e conteúdo para os Membros que a tiverem ratificado e que não ractificarem a convenção revista.

ARTIGO 14.º

As versões francesa e inglesa da presente Convenção são igualmente autênticas.

O Presidente da Assembleia Nacional, *Fernando da Piedade Dias dos Santos.*

Resolução n.º 33/19
de 9 de Julho

Considerando a necessidade de existência de uma legislação harmonizada no domínio da segurança cibernética nos Estados-Membros da União Africana que combata as violações da privacidade através da recolha, tratamento, transmissão, armazenamento e uso de dados pessoais;

Considerando a necessidade de se criar mecanismos para fazer face aos perigos e aos 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 nos Estados-Membros da União Africana;

Considerando que a presente Convenção, incorpora os compromissos existentes dos Estados-Membros da União Africana com vista a construção da sociedade de informação;

A Assembleia Nacional aprova, por mandato do Povo, nos termos das disposições combinadas da alínea k) do artigo 161.º e da alínea f) do n.º 2 do artigo 166.º, ambos da Constituição da República de Angola, a seguinte Resolução:

1.º — Aprovar, para ratificação, a Convenção da União Africana sobre a Cibersegurança e Protecção de Dados, anexa à presente Resolução.

2.º — A presente Resolução entra em vigor à data da sua publicação.

Vista e aprovada pela Assembleia Nacional, em Luanda aos 23 de Maio de 2019.

Publique-se.

O Presidente da Assembleia Nacional, *Fernando da Piedade Dias dos Santos.*

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 compromis-

sos existentes dos Estados-Membros da União Africana no plano subregional, 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 apropriada 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 subregional, 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 14.ª 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 5 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 1.º
(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.º
(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.º
(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.º
(Publicidade por via electrónica)

1. Sem prejuízo do artigo 3.º, 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 4.º (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 5.º
(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 5.º (3) e 5.º (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 2.º (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 6.º
(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 6.º (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 1.º;

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 7.º
(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 8.º
(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 9.º
(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 9.º (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 10.º
(Formalidades prévias ao tratamento de dados pessoais)

1. Estão isentos de formalidades prévias:

a) O processamento de dados mencionados no artigo 9.º (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 10.º (1), 10.º (4) e 10.º (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 15.º 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 11.º
(Estatuto, composição e organização das Autoridades Nacionais de Protecção de Dados 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 11.º (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 12.º
(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 13.º

(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 3: 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 14.º

(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 14.º (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;