

- Preâmbulo-

A Constituição da República de Angola assegura, sem reservas, a protecção dos dados pessoais como um direito fundamental.

Este compromisso é respaldado, desde logo, pelo artigo 32.º, que garante o direito à reserva da intimidade da vida privada e familiar, proibindo a obtenção e utilização abusiva de informações relativas a indivíduos e famílias, em contrariedade à dignidade humana, bem como pelo artigo 69.º, o qual prevê o recurso à providencia do habeas data, permitindo que os cidadãos tenham acesso às informações sobre si mesmos e solicitem a correcção ou actualização das mesmas.

A tutela do direito à protecção dos dados pessoais e da privacidade é também reforçada por instrumentos jurídicos internacionais de que Angola é signatária, tais como a Declaração Universal dos Direitos Humanos, a Carta Africana dos Direitos Humanos e dos Povos e a Convenção da União Africana sobre Cibersegurança e Protecção de Dados.

Havendo, por conseguinte, a necessidade de actualizar a actual regulação da protecção dos dados pessoais, de modo a doptar o ordenamento jurídico nacional de um instrumento legal que priorize a preservação mais efectiva da fundamentalidade desse direito, incentive a inovação tecnológica assente em padrões éticos e crie confiança entre as partes envolvidas por meio de normas transparentes.

A Assembleia Nacional aprova por mandato do povo, nos termos do n.º 2 do artigo 165.º e da alínea d) do n.º 2 do artigo 166.º, ambos da Constituição da República de Angola, a seguinte:

Lei da Protecção de Dados Pessoais

Capítulo I

Disposições Gerais

Artigo 1.º

(Objecto)

A presente lei estabelece as regras jurídicas aplicáveis ao tratamento de dados pessoais com o objectivo de garantir o respeito pelas liberdades públicas e os direitos e garantias fundamentais das pessoas singulares.

Artigo 2.º

(Âmbito material)

A presente lei aplica-se ao tratamento de dados pessoais realizado por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.

Artigo 3.º

(Âmbito subjectivo e territorial)

1. Estão sujeitos à presente lei os tratamentos de dados pessoais efectuados por entidades do sector público e privado.
2. A presente lei aplica-se ao tratamento de dados pessoais efectuados nos seguintes casos:
 - a) Quando o responsável pelo tratamento ou subcontratado estiver estabelecido na República de Angola.
 - b) Quando o responsável pelo tratamento ou subcontratado não estiver estabelecido na República de Angola, mas procede ao tratamento de dados pessoais cujos titulares se encontram em território angolano, e esteja relacionado com as seguintes situações:

- i. Oferta de bens ou serviços a esses titulares de dados em território nacional, independentemente da exigência de os titulares dos dados procederem a um pagamento financeiro;
 - ii. controlo de comportamentos ou interesses, assim como a elaboração de perfís, quando estes tenham lugar em território nacional.
- c) Fora da República de Angola, em local onde a legislação angolana seja aplicável por força do direito internacional.
- d) A quem se encontre no território da República de Angola e não seja aí residente, nomeadamente pessoas em trânsito e turistas.
3. O responsável pelo tratamento que esteja abrangido por estatuto de extraterritorialidade, de imunidade ou por qualquer outro que impeça o procedimento criminal, deve designar, mediante comunicação à Agência de Protecção de Dados (APD), um representante estabelecido em território nacional, que se lhe substitua em todos os seus direitos e obrigações, sem prejuízo da sua própria responsabilidade.

Artigo 4.º

(Exclusão do âmbito de aplicação)

1. A presente lei não se aplica ao tratamento de dados pessoais efectuado por uma pessoa singular no exercício de actividades exclusivamente pessoais ou domésticas, salvo se se destinar a comunicação sistemática ou difusão.
2. A presente lei não se aplica, igualmente, aos tratamentos de dados para fins exclusivamente de:
 - a) Segurança pública;
 - b) Defesa nacional;
 - c) Inteligência e segurança interna e externa do Estado;
 - d) Actividades de investigação e repressão das infracções penais.

3. O tratamento de dados pessoais referidos no número anterior rege-se por legislação específica, a qual deve prever medidas proporcionais e estritamente necessárias à prossecução do interesse público, bem como os princípios gerais de protecção de dados e os direitos dos titulares previstos na presente lei.

Artigo 5.º

(Definições)

1. Para efeitos da presente lei, entende-se por:

a) «Dados pessoais» - informação relativa a uma pessoa singular identificada ou identificável, incluindo som e imagem. Entende-se por "identificável" a pessoa que possa ser identificada, directa ou indirectamente, através de um identificador, como por exemplo, informação de identificação pessoal, número de identificação do titular, contacto do titular, dados de localização, metadados ou por um ou vários elementos característicos da sua identidade física, fisiológica, genética, psíquica, económica, cultural ou social.

b) «Dados de tráfego»- qualquer dado tratado para efeitos de envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos da facturação da mesma, incluindo os dados que indicam a origem, destino, trajecto, hora, data tamanho e duração da comunicação, ou o tipo de serviço subjacente.

c) «Tratamento de dados pessoais»- qualquer operação ou conjunto de operações efectuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, a transferência, a difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, o apagamento ou a destruição.

c) «Ficheiro»- conjunto estruturado de dados pessoais, independentemente da sua forma ou modalidade de criação, organização, conservação e acesso aos

dados, segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico.

e) «Consentimento do titular dos dados»- manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita que os dados pessoais que lhe dizem respeito sejam objecto de tratamento.

f) «Interconexão de dados»-forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de outro ou outros ficheiros mantidos pelo mesmo responsável ou por outro ou outros responsáveis com outra finalidade;

g) «Responsável pelo tratamento» - pessoa singular ou colectiva, a autoridade pública, que, individualmente ou em conjunto, determina as finalidades e os meios de tratamento de dados.

g) «Subcontratado»- pessoa singular ou colectiva, a autoridade pública, que trate os dados pessoais por conta do responsável pelo tratamento destes.

h) «Destinatário»- pessoa singular ou colectiva, a autoridade pública ou qualquer outro organismo a quem seja comunicado dados pessoais, independentemente de se tratar ou não de um terceiro.

i) «Terceiro»- pessoa singular ou colectiva, pública ou privada, distinta do titular dos dados, do responsável pelo tratamento, do subcontratante ou das pessoas autorizadas a tratar os dados pessoais sob a autoridade directa do responsável pelo tratamento ou do subcontratado.

j) «Violação de dados pessoais»-consiste em uma afectação da segurança que provoque, de modo accidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

k) «Representante» - pessoa singular ou colectiva estabelecida na República de Angola, designada por escrito pelo responsável pelo tratamento ou pelo

subcontratado, e que representa estes no que se refere às suas obrigações respectivas nos termos da presente lei.

l) «Dados especiais»- informações pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada, origem racial ou étnica, saúde, vida sexual, orientação sexual, dados biométricos e dados genéticos.

n) «Dados genéticos» - são as informações pessoais relativas às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa.

o) «Dados biométricos» - consistem em informações pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos.

p) «Dados relativos à saúde» - informações pessoais relacionadas com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde.

m) «Definição de perfis» - consiste em qualquer forma de tratamento automatizado de dados pessoais que permita utilizar esses dados pessoais para avaliar certos aspectos de uma pessoa singular, nomeadamente para analisar ou prever o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.

m) «Decisões parcialmente automatizadas ou semi-automatizadas»- aquelas em que não há intervenção humana significativa.

q) «Pseudonimização»- consiste no tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

r) «Anonimização»- aplicação de medidas voltadas para impedir a identificação ou reidentificação de uma pessoa física, sem esforços ou prazos desproporcionados ou inviáveis, levando em consideração factores como os custos e o tempo necessários para a identificação ou reidentificação da pessoa à luz da tecnologia disponível no momento do tratamento.

s) «Titular dos dados»- pessoa singular cujos dados são objecto do tratamento ao qual se refere a presente lei.

t) «Transferência internacional»- transmissão de dados pessoais para fora do território nacional.

2. Para efeito do disposto na alínea a) do número anterior, os dados pessoais identificados têm uma natureza directa, enquanto os dados pessoais identificáveis revestem uma natureza indirecta, e a presente lei só lhes é aplicável se existir uma probabilidade razoável de se proceder à identificação de uma pessoa singular considerando, nomeadamente, os custos e o tempo necessário para o efeito.

3. Sempre que as finalidades e os meios de tratamento sejam determinados por disposições legislativas ou regulamentares, o responsável pelo tratamento deve ser indicado na lei de organização e funcionamento ou no estatuto da entidade legal ou estatutariamente competente para tratar dos dados pessoais em causa.

Capítulo II

Tratamento de Dados Pessoais

SECÇÃO I

Princípios Fundamentais

Artigo 6.º

(Princípio da licitude)

1. O tratamento de dados pessoais deve ser efectuado de forma lícita e leal.
2. O princípio da licitude concretiza-se através dos seguintes elementos:
 - a) Referência expressa à base de legitimidade de tratamentos de dados pessoais;
 - b) Caso o tratamento de dados pessoais se funde na lei ou noutro acto normativo, deve verificar-se a sua identificação expressa;
 - c) Cumprimento da lei, nomeadamente, quanto aos dados pessoais a tratar, ao exercício dos direitos pelos titulares dos dados, à comunicados de dados pessoais, aos limites a que devem obedecer as operações de tratamento e à definição dos prazos de conservação.

Artigo 7.º

(Princípio da minimização de dados)

1. Os dados pessoais devem ser tratados de maneira que sejam adequados, pertinentes e limitados ao necessário em relação aos propósitos para os quais foram recolhidos.
2. A pedido da Agência de Protecção de Dados, os responsáveis pelo tratamento de dados ou os subcontratantes devem fornecer uma justificação para a necessidade de colectar os dados em cada caso.

Artigo 8.º

(Princípio da transparência)

1. Para garantir o exercício dos direitos previstos na lei pelos titulares dos dados pessoais, o princípio da transparência exige que, no momento da recolha ou em outro determinado por lei, seja transmitida a informação necessária sobre o modo como se procede ao tratamento de dados.
2. A linguagem utilizada pelo responsável pelo tratamento deve ser clara e simples, em especial quando as informações são dirigidas especificamente a crianças.
3. As informações devem ser prestadas por escrito, ou oralmente se tal for solicitado pelo titular dos dados.
4. A informação deve ser prestada de forma concisa e inteligível, de forma a evitar a comunicação de informação complexa e excessiva.

Artigo 9.º

(Princípio da finalidade)

1. Os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo manifestar uma natureza genérica ou indeterminada.
2. A recolha dos dados pessoais, em conformidade com o princípio da finalidade, deve ser realizada de forma que seja possível a sua justificação.
3. O responsável pelo tratamento e o subcontratado devem definir medidas de segurança adequadas para que os dados não possam ser tratados para finalidade não previstas nos números anteriores do presente artigo.
4. O princípio da finalidade implica a utilização dos dados necessários para a realização de um tratamento fundado na base de legitimidade adequada e lícita.

5. Os dados necessários previstos no número anterior podem:

- a) Ter uma dimensão limitada, e referirem-se a um conjunto de informação reduzido, ou;
- b) Respeitar a um conjunto de informação amplo, por ser a única forma de assegurar a realização de um tratamento de dados pessoais com certa finalidade.

Artigo 10.º

(Princípio da exactidão)

1. Os dados pessoais sujeitos a tratamento devem ser exactos e actualizados.
2. A actualização deve ser efectuada, por regra, oficiosamente e sem demora pelo responsável pelo tratamento.
3. O titular dos dados exerce o direito de rectificação, actualização ou eliminação, nos termos da presente lei.

Artigo 11.º

(Princípio da conservação de dados)

1. Os dados pessoais devem ser conservados de uma forma que permita a identificação dos titulares dos dados pessoais durante o período necessário à prossecução das finalidades de um tratamento.
2. O período de conservação dos dados pessoais é definido por lei ou pela Agência de Protecção de Dados no momento do registo ou autorização do tratamento.
3. Os dados pessoais podem ser conservados durante períodos mais extensos do que os necessários para a prossecução das finalidades determinadas, desde que tal seja definido por lei ou decidido pela Agência de Protecção de Dados.
4. Os tratamentos de dados pessoais que se destinem exclusivamente para fins de arquivo de interesse público, investigação científica ou histórica ou para

fins estatísticos, devem garantir as medidas de segurança adequadas aos tratamentos realizados.

5. Findo o prazo de conservação para a realização definido nos números anteriores, os dados pessoais devem ser eliminados ou anonimizados.

Artigo 12.º

(Princípio da integridade e da confidencialidade)

1. Os dados pessoais devem ser tratados de forma que seja garantida a sua segurança adoptando-se medidas técnicas ou organizativas adequadas.

2. No tratamento de dados pessoais deve ser avaliado o risco existente relativamente ao cumprimento do princípio da licitude e no que respeita à qualidade dos dados precavendo-se, designadamente, a sua perda, destruição ou dano.

3. A integridade do tratamento de dados pessoais implica que não seja permitido guardar informação pessoal no *browser*, na memória ou no disco, para além do tempo da sessão e apenas na medida do necessário.

4. A fim de limitar situações de risco, a criação de perfís deve ser construída definindo apenas os privilégios necessários, de acordo com a necessidade de intervir nos tratamentos de dados pessoais.

5. Com o propósito de rastrear comportamentos, devem ser criados registos de acesso, alteração e remoção com informação sobre quem acedeu e de onde acedeu ao tratamento de dados pessoais.

Artigo 13.º

(Estratégia Nacional de Cibersegurança)

A protecção de dados pessoais deve estar alinhada à Estratégia Nacional de Cibersegurança prevista na Convenção da União Africana sobre

Cibersegurança e Protecção de Dados ratificada, através da Carta de Ratificação 1/290, de 3 de Março.

SECÇÃO II

Regras Gerais e Especiais de Legitimidade para o Tratamento de Dados Pessoais

Artigo 14.º

(Legitimidade para o tratamento de dados pessoais)

1. O tratamento de dados pessoais só pode ser realizado se, pelos menos, verificado uma das seguintes condições:

- a) Consentimento inequívoco e expresso do seu titular, como meio de autodeterminação, de acordo com o conceito previsto na presente lei, sendo, para tal, informado das finalidades em causa.
- b) Celebração ou execução de um contrato no qual o titular dos dados é parte, ou para realização de diligências pré-contratuais a seu pedido;
- c) Cumprimento de obrigação legal a que o responsável pelo tratamento de dados esteja sujeito;
- d) Defesa de interesses vitais do titular dos dados ou de outra pessoa singular, independente de consentimento ou previsão legal.
- e) Exercício de funções de interesse público ou o exercício da autoridade pública definidas legislativamente como responsáveis pelo tratamento.
- f) Se for necessário para a prossecução dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, excepto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a protecção dos dados pessoais.

2. Além da verificação das condições de legitimidade, o tratamento de dados pessoais carece de autorização ou notificação da Agência de Protecção de Dados, nos termos da presente lei.

Artigo 15.º

(Condições aplicáveis ao consentimento)

1. Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.
2. Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples.
3. Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato.
4. A ausência de consentimento para a realização de um tratamento de dados pessoais, quando não essencial para o cumprimento das finalidades, não pode privar o titular do direito de adquirir, por via gratuita ou onerosa, um bem, de celebrar contratos ou de ser afectado em relações com a Administração Pública.
5. Com respeito pelo princípio da boa-fé, o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento, fazendo-o com o mesmo nível de proporcionalidade que existiu no momento do consentimento inicial.
6. A retirada do consentimento não prejudica a licitude do tratamento de dados efectuado, embora obrigue o responsável pelo tratamento a eliminar os dados objecto de tratamento e que se encontrem na sua titularidade.

Artigo 16.º

(Condições aplicáveis ao consentimento de incapazes)

1. O tratamento de dados pessoais de incapazes, quer em razão da idade quer em razão da anomalia psíquica, só é lícito se o consentimento for prestado ou autorizado pelos respectivos representantes legais ou havendo suprimento legal do consentimento, salvo o previsto no n.º 2 da presente disposição.
2. O consentimento da criança só é validamente prestado quando tenha idade igual ou superior a 16 (dezasseis anos), sem prejuízo de disposição legal em contrário.
3. De acordo com o estado da tecnologia e com as regras de boas práticas, o responsável pelo tratamento prossegue os esforços adequados para verificar a idade do menor.
4. No caso de se tratar da matéria contratual, é aplicável a legislação da República de Angola, nomeadamente no que toca à validade de contratos.

Artigo 17.º

(Legitimidade para o tratamento de dados especiais)

1. É proibido o tratamento de dados pessoais relativos às convicções ou posições políticas, filosóficas ou ideológicas, à fé religiosa, à filiação partidária ou sindical, à origem racial ou étnica, bem como o tratamento de dados genéticos, dados biométricos, dados relativos à vida privada, à saúde, à vida sexual ou orientação sexual, salvo:
 - a) Mediante consentimento expresso do titular, com garantias de não discriminação e com as medidas de segurança adequadas;
 - b) Mediante autorização prevista na lei, com garantias de não discriminação e com as medidas de segurança adequadas;

c) Quando se destinem a processamento de dados estatísticos não individualmente identificáveis, com as medidas de segurança adequadas;

d) Mediante autorização da Agência de Protecção de Dados, quando o tratamento tiver como fundamento um interesse público importante ou for necessário para a prossecução de interesses legítimos do responsável pelo tratamento, com garantias de não discriminação e com as medidas de segurança adequadas.

2. Na concessão de autorização prevista na alínea b) do número anterior, a lei deve ater-se, designadamente, à indispensabilidade do tratamento dos dados pessoais para o exercício das atribuições legais ou estatutárias do seu responsável, por motivos de interesse público importante.

3. O tratamento dos dados referidos no n.º 1 é ainda permitido quando se verificar uma das seguintes condições:

a) Ser necessário para proteger interesses vitais do titular dos dados ou de uma outra pessoa e o titular dos dados estiver física ou legalmente incapaz de dar o seu consentimento;

b) Ser efectuado, com o consentimento do titular, por fundação, associação ou organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, no âmbito das suas actividades legítimas, sob condição de o tratamento respeitar apenas aos membros dessa fundação, associação ou desse organismo ou às pessoas com quem ele mantenha contactos periódicos ligados às suas finalidades legítimas, e de os dados não serem comunicados a terceiros sem consentimento dos seus titulares;

c) Dizer respeito a dados manifestamente tornados públicos pelo seu titular, desde que se possa legitimamente deduzir das suas declarações o consentimento para o tratamento dos mesmos;

d) Ser necessário à declaração, exercício ou defesa de um direito em processo judicial e for efectuado exclusivamente com essa finalidade;

e) Ser necessário por motivos de interesse público no domínio da saúde pública, tais como a protecção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, desde que sejam adoptadas medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional.

4. O tratamento dos dados pessoais referentes à saúde, à vida sexual e orientação sexual, incluindo os dados genéticos, é permitido quando for necessário para efeitos de medicina preventiva, para avaliação da capacidade de trabalho do colaborador, diagnóstico médico, prestação de cuidados ou tratamentos de saúde ou de acção social ou de gestão de sistemas e serviços de saúde ou de acção social, desde que seja efectuado por um profissional de saúde obrigado ao segredo profissional ou por outra pessoa igualmente sujeita a uma obrigação de segredo equivalente, tenha sido notificada à Agência de Protecção de Dados e sejam garantidas medidas adequadas de segurança da informação.

5. O tratamento dos dados referidos no n.º 1 pode ainda ser efectuado, com medidas adequadas de segurança da informação, quando se mostrar indispensável à protecção da segurança do Estado, da defesa da segurança pública e da prevenção, investigação ou repressão de infracções penais.

6. São proibidas as definições de perfis que conduzam à discriminação de pessoas singulares com base nas categorias especiais de dados pessoais previstos no n.º 1.

Artigo 18.º

(Legitimidade para o tratamento de dados pessoais em sistemas de videovigilância e outros meios de controlo remoto)

1. Sem prejuízo do previsto em legislação especial, o tratamento de dados pessoais efectuado com recurso aos sistemas de videovigilância e outras formas de captação, tratamentos e difusão de sons e imagens que permitam identificar pessoas, sempre que o responsável pelo tratamento esteja domiciliado ou sediado em território nacional ou recorra a um fornecedor de acesso a redes informáticas e telemáticas nele estabelecido, está sujeito ao disposto na presente lei.
2. O tratamento de dados referido no número anterior representa um tratamento de dados especiais, pelo que estão sujeitos a uma avaliação de impacto.
3. Com as necessárias adaptações são aplicáveis aos tratamentos de dados referidos no n.º 1 relativos à videovigilância e com recurso a outros meios remotos os direitos do titular de dados previstos na presente lei.

Artigo 19.º

(Legitimidade para o tratamento de dados pessoais para fins de marketing e publicidade)

1. O tratamento de dados pessoais para fins de envio de mensagens publicitárias endereçadas para o domicílio, por via postal ou por distribuição directa, é permitido mediante notificação à Agência de Protecção de Dados, excepto quando o assinante se tenha oposto ao tratamento e utilização dos seus dados para esta finalidade.
2. O titular dos dados deve ter acesso a meios que lhe permitam a qualquer momento recusar, sem ónus, gratuitamente e independentemente de justa causa, o envio dessa publicidade para o futuro.

3. A Agência de Protecção de Dados apoia a constituição de listas de titulares de dados que manifestem a sua oposição à recepção de mensagens publicitárias.

4. O responsável pelo tratamento de dados pessoais para os fins constantes deste artigo deve informar o destinatário:

a) Sobre a introdução dos seus dados pessoais, no caso de os mesmos terem origem em fontes acessíveis ao público;

b) De que os seus dados serão comunicados a destinatários para fins de publicidade, podendo o titular dos dados manifestar o seu direito de oposição;

d) Sobre a identidade do responsável pelo tratamento, sendo proibido o envio de publicidade por via postal ou distribuição directa ocultando ou dissimulando a identidade da pessoa em nome de quem é efectuada a comunicação.

Artigo 20.º

(Legitimidade para o tratamento de dados pessoais para fins de marketing e publicidade por via electrónica)

1. O tratamento de dados pessoais para fins de envio de mensagens publicitárias endereçadas por meios electrónicos, nomeadamente, por via de aparelhos de chamada automática, aparelhos de telecópia ou por correio electrónico, está sujeito aos seguintes requisitos:

a) Consentimento expresso do titular dos dados;

b) Notificação à Agência de Protecção de Dados.

2. O tratamento de dados pessoais para os fins previstos no número anterior pode ser efectuado sem o consentimento do titular dos dados nas seguintes circunstâncias:

a) Quando as mensagens sejam enviadas ao titular dos dados enquanto representante, trabalhador ou colaborador de uma pessoa colectiva;

b) Quando as mensagens sejam enviadas pela Administração Pública através do sistema de governação electrónica do Executivo angolano;

c) Quando as mensagens sejam enviadas a pessoas singulares com quem o fornecedor do produto ou o prestador do serviço tenha celebrado anteriormente transacções, se aquele tiver sido explicitamente oferecida a possibilidade de o recusar por ocasião da transacção realizada e se não implicar para o destinatário dispêndio adicional ao custo do serviço de telecomunicações;

2. Se for exercido o direito de oposição, as entidades que promovam o envio de mensagens publicitárias devem manter uma lista actualizada, por si ou por organismos que as representem, de titulares que manifestaram a sua oposição ao envio de tais mensagens.

3. A Agência de Protecção de Dados apoia a constituição de listas de titulares de dados que manifestem a sua oposição à recepção de mensagens publicitárias.

4. O responsável pelo tratamento de dados pessoais para os fins constantes deste artigo deve informar o destinatário:

a) Sobre a procedência dos seus dados pessoais, no caso de os mesmos terem origem em fontes acessíveis ao público;

b) De que os seus dados serão comunicados a destinatários para fins de marketing directo ou utilizados por conta de terceiros, caso o titular dos dados tenha consentido, observando-se nesse caso os requisitos aplicáveis à comunicação de dados constantes do artigo 24.º.

c) Sobre a identidade do responsável pelo tratamento, sendo proibido o envio de publicidade oculta ou que dissimule a identidade da pessoa em nome de quem é efectuada a comunicação.

Artigo 21.º

(Legitimidade para o tratamento de dados relativos a actividades ilícitas, crimes e contravenções)

1. Os dados pessoais constantes da presente disposição têm a natureza de dados especiais, aplicando-se o regime previsto no artigo 17.º da presente lei.
2. A criação e a manutenção de registos centrais relativos a pessoas suspeitas de actividades ilícitas, infracções penais, contraordenações, condenações penais, decisões que apliquem medidas de segurança, coimas e sanções acessórias só podem ser mantidas por serviços públicos com essa competência legal, observando normas procedimentais e de protecção de dados previstas em diploma legal.
3. O tratamento de dados pessoais relativos a suspeitas de actividades ilícitas, infracções penais, contraordenações, condenações penais, decisões que apliquem medidas de segurança, coimas e sanções acessórias e infracção disciplinar pode ser definido por lei ou autorizado pela Agência de Protecção de Dados, observadas as normas de protecção de dados e de segurança da informação, quando tal tratamento for necessário à execução de finalidades legítimas do seu responsável, desde que não prevaleçam os direitos, liberdades e garantias do titular dos dados.
4. O tratamento de dados pessoais para fins de investigação policial deve limitar-se ao necessário para a prevenção de um perigo concreto ou repressão de uma infracção determinada, para o exercício de competência previstas em disposição legal e ainda nos termos de acordo, tratado ou convenção internacional de que Angola seja parte.

Artigo 22.º

(Legitimidade para o tratamento de dados pessoais resultantes de gravações de chamadas na relação contratual)

1. É admitida a gravação de chamadas, quando haja consentimento do titular dos dados e a mesma seja realizada no contexto de práticas comerciais lícitas, com a finalidade de comprovar uma transacção comercial ou qualquer outra comunicação estabelecida no âmbito de uma relação contratual.
4. As situações de emergência com intervenção de serviços públicos devem ter previsão legal ou autorização geral da Agência de Protecção de Dados.
5. Sem prejuízo do prazo de prescrição estipulado pela lei, a gravação da chamada deve ser mantida pelo período de tempo que tenha sido estipulado no acordo.

Artigo 23.º

(Legitimidade para o tratamento de dados de crédito e solvabilidade)

1. A realização do tratamento de dados relativos a crédito e solvabilidade, só deve ocorrer com o consentimento do titular dos dados e este tem o direito de não ser avaliado por meios ou mecanismos integralmente automatizados que possam definir perfis negativos, através da utilização, especialmente, de meios de inteligência artificial.
2. A pedido do titular dos dados, o responsável pelo tratamento que elabore um sistema de pontuação e/ou classificação com base no comportamento de crédito das pessoas deve comunicar detalhadamente ao respectivo titular qual a fórmula, as variáveis consideradas, o procedimento e as informações levadas em conta, ou ainda o algoritmo utilizado e sua composição.
3. Se for negada ao titular dos dados a celebração de um contrato, solicitação de emprego, serviço, crédito comercial ou financeiro com base em um relatório

de crédito, é obrigatório informar tal situação ao titular, dando-lhe uma cópia do referido relatório e indicar a empresa que o produziu.

4. As regras sobre a autorização, recolha, armazenamento e gestão de informações pessoais sobre cumprimento e incumprimento de obrigações creditícias constam de legislação especial.

SECÇÃO III

Comunicação e Interconexão de Dados Pessoais

Artigo 24.º

(Comunicação de dados)

1. Os dados pessoais tratados por organismos da Administração Pública não podem ser comunicados a outras entidades, organismos, serviços que tenham competências materiais distintas, salvo nas seguintes circunstâncias:

- a) Quando tal comunicação for permitida por disposição legal ou aprovada pela Agência de Protecção de Dados;
- b) Quando a comunicação tenha por objecto o tratamento posterior dos dados para fins históricos ou estatísticos.

2. Os dados pessoais tratados por entidades privadas podem ser comunicados desde que tenham sido garantidos os direitos de informação, se verifique uma das condições de legitimidade estabelecidas na presente lei.

Artigo 25.º

(Interconexão de dados pessoais)

1. A interconexão de dados pessoais que não esteja estabelecida em disposição legal pode ser realizada, mediante solicitação à Agência de Protecção de Dados pelo responsável pelo tratamento dos dados ou em conjunto pelos responsáveis correspondentes.

2. A interconexão de dados pessoais deve ser necessária e adequada à prossecução das finalidades legais ou estatutárias e de interesses legítimos dos responsáveis dos tratamentos, não implicar discriminação ou diminuição dos direitos, liberdades e garantias fundamentais dos titulares dos dados, ter em conta o tipo de dados objecto de interconexão e ser rodeada de adequadas medidas de segurança.

Capítulo III

Direitos dos Titulares dos Dados e Tratamentos por Sistema de Inteligência Artificial

SECÇÃO I

Direitos dos Titulares dos Dados

Artigo 26.º

(Direito de informação)

1. Quando os dados pessoais forem recolhidos junto do titular dos dados, o responsável pelo tratamento informa-o, aquando da recolha desses dados pessoais, do seguinte:

- a) Da identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
- b) Dos contactos do encarregado de protecção de dados, a existir;
- c) Das finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
- d) Dos destinatários ou categorias de destinatários dos dados pessoais, se os houver;
- f) Sobre a existência de transferência internacional de dados;

g) Da existência e condições do direito de acesso de actualização, oposição, rectificação ou apagamento;

h) Das consequências da recolha dos dados sem o consentimento do titular ou, em caso de incapacidade deste, pelo seu representante legal;

i) Do prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;

j) O direito de apresentar reclamação a uma autoridade de controlo.

2. Caso os dados pessoais não sejam recolhidos directamente do titular dos dados, o responsável pelo tratamento deve prestar-lhe a informação referida no momento do registo dos dados ou o mais tardar no prazo de trinta dias após a sua recolha, salvo se dele já for conhecida.

3. A obrigação de informação pode ser dispensada mediante disposição legal ou deliberação da Agência de Protecção de Dados, nos seguintes casos:

a) Por motivos de segurança do Estado e prevenção ou investigação criminal;

b) Quando a lei determinar expressamente o registo dos dados ou a sua divulgação.

4. No caso de recolha de dados em redes abertas, considera-se prestado o direito de informação através da publicação e disponibilização de políticas de privacidade que sejam de fácil acesso e incluam:

a) As informações descritas no n.º 1 do presente artigo;

b) A informação de que os seus dados pessoais podem circular na rede sem condições de segurança, correndo o risco de serem vistos e utilizados por terceiros não autorizados.

5. Quando o responsável pelo tratamento de dados pessoais tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja

aquele para o qual os dados tenham sido recolhidos, fornece ao titular dos dados informações sobre esse fim, podendo ser exercido o direito de oposição.

6. De acordo com o princípio da transparência, a informação deve ser prestada de maneira clara, precisa e objectiva em particular quando tenha como destinatários menores e pessoas com necessidades especiais.

Artigo 27.º

(Direito de acesso)

1. O titular dos dados tem o direito de solicitar e obter confirmação do responsável pelo tratamento se os seus dados pessoais estão a ser tratados ou não, e, em caso afirmativo, o direito de acesso a eles, bem como de conhecer qualquer informação relacionada às condições gerais e específicas do seu tratamento.

2. Para efeitos de exercício do direito de acesso, o titular dos dados tem o direito de obter as seguintes informações sobre o tratamento dos seus dados:

a) As finalidades do tratamento dos dados;

b) As categorias dos dados pessoais em questão;

c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;

d) O prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;

e) A forma de exercer o direito de rectificação ou apagamento ou do direito de se opor a esse tratamento.

2. O exercício do direito de acesso deve ser efectuado livremente, sem restrições, demoras ou custos excessivos.

3. Sempre que o titular dos dados apresentar o pedido por meios electrónicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato electrónico de uso corrente.

4. Verificam-se limites no acesso a dados pessoais quando esteja em causa a:

- a) Defesa nacional;
- b) Segurança do Estado;
- c) Prevenção ou investigação criminal;
- d) Segredo de justiça.

Artigo 28.º

(Direito de rectificação)

1. O titular dos dados tem o direito de obter, sem demora, do responsável pelo tratamento a rectificação dos seus dados pessoais, se estes se mostrarem imprecisos, falsos, incorrectos, incompletos ou não estiverem actualizados.

2. No âmbito de um tratamento de dados pessoais, o titular dos dados pode exercer o direito de rectificação a qualquer momento.

3. Independentemente do exercício do direito de rectificação, o responsável pelo tratamento tem a obrigação de manter os dados pessoais exactos e completos.

Artigo 29.º

(Direito de apagamento)

1. O titular dos dados pessoais tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora, nos seguintes casos:

- a) Sempre que se verifique a falta de necessidade superveniente relativamente ao tratamento originário;

- b) O titular dos dados pessoais retire o consentimento, com respeito pelo princípio da boa-fé;
- c) O titular dos dados pessoais exerça o direito de oposição;
- d) Os dados pessoais forem tratados ilicitamente;
- e) Verificar-se imposição legal.

3. O presente no número anterior não se aplica quando os dados pessoais se revelem necessários para:

- a) O exercício e direitos fundamentais, tais como a liberdade de expressão e de informação;
- b) Cumprimento de obrigação legal;
- c) Por motivos de interesse público no domínio da saúde pública, nomeadamente em caso de pandemias;
- d) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Artigo 30.º

(Direito à limitação do tratamento)

1. O titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma das seguintes situações:
 - a) Contestar a exactidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exactidão;
 - b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização;
 - c) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;

d) Se tiver oposto ao tratamento nos termos da presente lei, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

2. Quando o tratamento tiver sido limitado nos termos do n.º 1, os dados pessoais só podem, à excepção da conservação, ser objecto de tratamento com o consentimento do titular, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou colectiva, ou por motivos ponderosos de interesse público.

3. O titular dos dados que tiver obtido a limitação do tratamento nos termos do n.º 1 é informado pelo responsável pelo tratamento antes de ser anulada a limitação ao referido tratamento.

Artigo 31.º

(Direito de portabilidade)

1. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se:

- a) O tratamento se basear no consentimento dado nos termos da presente lei; e
- b) O tratamento for realizado por meios automatizados.

2. Para efeitos do exercício do direito de portabilidade previsto no n.º 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos directamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.

3. O exercício do direito de portabilidade não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento.

4. O direito de portabilidade não prejudica os direitos e as liberdades de terceiros.

Artigo 32.º

(Direito de oposição)

1. O titular dos dados tem o direito de se opor, salvo disposição legal em contrário, ao tratamento de dados pessoais não baseados no seu consentimento.

2. O responsável pelo tratamento deve fazer cessar o tratamento dos dados pessoais, a não ser que apresente razões importantes e legítimas, fundamentando a prevalência sobre os direitos do titular dos dados.

2. Sempre que os dados pessoais forem objecto de tratamento para efeitos de comercialização directa, o titular tem o direito de se opor, em qualquer momento e gratuitamente, quer se trate do tratamento inicial quer do tratamento posterior.

Artigo 33.º

(Decisões individuais automatizadas)

1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado ou semi-automatizado, que produza efeitos na sua esfera jurídica.

2. O número anterior não se aplica se a decisão:

a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; ou

b) For baseada no consentimento explícito do titular dos dados.

3. O responsável pelo tratamento deve fornecer, sempre que solicitado, informações claras, completas e adequadas sobre os critérios e procedimentos utilizados para a decisão automatizada ou semi-automatizada, respeitando os segredos comerciais e industriais.

Artigo 34.º

(Dados pessoais de pessoas falecidas)

1. Os dados pessoais das pessoas falecidas são protegidos nos termos da presente lei.
2. Os direitos de acesso, rectificação e apagamento dos dados pessoais das pessoas falecidas podem ser exercidos por quem a pessoa falecida haja designado para o efeito ou, na sua falta, pelos respetivos herdeiros.
3. O titular dos dados pode igualmente, nos termos legais aplicáveis, deixar determinada a impossibilidade de exercício dos direitos referidos no número anterior após a sua morte.

Artigo 35.º

(Direito do titular dos dados em casos especiais)

Os direitos de informação, de acesso, de rectificação, de apagamento e de limitação do tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, detecção, investigação ou repressão de infracções penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública são exercidos nos termos da lei processual penal, demais legislações aplicáveis e da presente lei.

SECÇÃO II

Tratamento de Dados Pessoais por Sistema de Inteligência Artificial

Artigo 36.º

(Práticas proibidas)

É proibida a implementação e o uso de sistema de inteligência artificial que:

- a) Use métodos que induzam as pessoas a adoptar comportamentos que comprometam a sua privacidade, a integridade dos seus dados pessoais, ou que violem os princípios previstos na presente lei;
- b) Explore vulnerabilidades específicas de certos grupos de pessoas, como aquelas relacionadas à idade, deficiência física ou mental, com o objectivo de induzi-las a fornecer, expor ou partilhar dados pessoais de maneira que comprometa a sua privacidade ou a respectiva segurança;
- c) Utilize dados pessoais para avaliar ou classificar pessoas singulares, com base no seu comportamento social ou em aspectos da sua personalidade, e que conduzam ao seu tratamento ilegítimo, prejudicial ou desfavorável, tendo em conta o contexto em que os dados foram originalmente gerados ou recolhidos.

Artigo 37.º

(Direitos dos titulares dos dados afectados por sistema de inteligência artificial)

Sem prejuízo de outros direitos previstos na presente lei, os titulares de dados afectados por sistemas de inteligência artificial têm os seguintes direitos:

- a) Receber, antes da sua utilização, informações claras e adequadas sobre as características e funcionalidades do sistema;
- b) Solicitar explicação sobre as decisões, recomendações ou previsões tomadas pelo sistema;
- c) Contestar as decisões ou as previsões do sistema que produzam efeitos jurídicos ou que impactem de maneira significativa os seus interesses;
- d) Exigir a participação humana em decisões do sistema tendo em consideração o contexto e o estado do desenvolvimento tecnológico;
- e) Receber um tratamento justo e igual, sendo proibido a implementação e o uso de sistema que possa acarretar qualquer tipo de discriminação.

Artigo 38.º

(Responsabilidade das entidades que produzem, fornecem ou operem sistema de inteligência artificial)

Sem prejuízo do disposto em legislação especial, as entidades que produzem, fornecem ou operem sistemas de inteligência artificial estão sujeitos às seguintes responsabilidades:

- a) Estabelecer estruturas de governança e adoptar práticas de gestão de dados que previnam e mitiguem potenciais situações discriminatórias,

garantindo a legalidade e legitimidade dos tratamentos conforme previsto na presente lei;

- b) Garantir que o sistema foi concebido e desenvolvido de modo a informar os usuários de que estão a interagir com um sistema de inteligência artificial, excepto se essa informação for evidente para qualquer usuário;
- c) Assegurar a transparência quanto às medidas de governança adoptadas no desenvolvimento e emprego do sistema;
- d) Assegurar-se de que foram adoptadas as medidas adequadas de segurança da informação desde a concepção até a operação dos sistemas;
- e) Utilizar dados provenientes de fontes seguras, que sejam exactas, pertinentes e actualizadas;
- f) Assegurar a explicação dos resultados do sistema, proporcionando aos titulares dos dados informações sobre o funcionamento do modelo, a lógica e os critérios relevantes para a produção de resultados, e, mediante solicitação, fornecer informações que permitam a interpretação dos resultados gerados, respeitando o sigilo industrial e comercial.

Capítulo IV

Segurança e Confidencialidade do Tratamento dos Dados Pessoais

SECÇÃO I

Segurança dos Dados

Artigo 39.º

(Protecção de dados desde a concepção e por defeito)

1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos dele decorrentes para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento

como no próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas à aplicar com eficácia os princípios da protecção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente diploma e proteja os direitos dos titulares dos dados.

2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento.

3. A obrigação referida no número anterior, aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade, em especial, essas medidas devem assegurar que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

Artigo 40.º

(Segurança dos dados pessoais)

1. O responsável pelo tratamento e o subcontratado aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

- a) A pseudonimização e a cifragem dos dados pessoais;
- b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
- c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
- d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

2. A avaliação do nível de segurança adequado, deve tomar em conta designadamente, os riscos apresentados pelo tratamento.

3. A determinação de medidas organizativas e técnicas deve, designadamente, considerar os seguintes elementos:

- a) Garantir a segurança da informação e a resistência dos sistemas e serviços;
- b) Classificar a informação de acordo com o nível de confidencialidade e sensibilidade e adoptar as medidas organizativas e técnicas adequadas à classificação;
- c) Definir políticas de gestão de palavras-passe seguras, impondo requisitos para o tamanho, a composição, o armazenamento e a frequência com que uma palavra-passe precisa de ser alterada;
- d) Adoptar sistemas de aviso que permitam identificar situações de acesso, tentativas ou utilização indevida;
- e) Definir, na fase de concepção, as melhores práticas de segurança de informação a adoptar, quer em fase de desenvolvimento de software, quer em fase de testes de aceitação;
- f) Realizar auditorias de segurança e avaliações de vulnerabilidade;
- g) Desenhar e organizar os sistemas e a infraestrutura por forma a segmentar ou isolar os sistemas e as redes de dados;
- h) Encriptar com código, ao qual só o destinatário tenha acesso, os e-mails ou anexos enviados que contenham dados pessoais.

Artigo 41.º

(Dever de notificar a violação de dados pessoais à Agência de Protecção de Dados)

1. No caso de ocorrer uma violação de dados pessoais, designadamente, a destruição, a perda, a alteração, a divulgação, o acesso não autorizados ou outro incidente de segurança dos dados, o responsável pelo tratamento notifica à Agência de Protecção de Dados, no prazo de 72 horas, após ter conhecimento da situação.
2. Nos casos em que não seja possível efectuar a notificação no prazo indicado no número anterior, o responsável pelo tratamento deve indicar os motivos do atraso.
4. A notificação a que se refere o n.º 1 é confidencial e deve, no mínimo:
 - a) Descrever a natureza da violação de dados pessoais, incluindo, se possível e adequado, as categorias e o número aproximado de titulares dos dados afetados;
 - b) Descrever as consequências prováveis da violação de dados pessoais;
 - c) Descrever as medidas adoptadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, nomeadamente, se for caso disso, para atenuar os seus eventuais efeitos negativos.
5. Nos casos em que não seja possível serem prestadas em simultâneo, as informações referidas no número anterior podem ser fornecidas posteriormente à notificação, sem demora injustificada.
6. O responsável pelo tratamento documenta qualquer violação de dados pessoais, incluindo os factos com ela relacionados, os seus efeitos e as medidas de reparação adoptadas, de modo a permitir à Agência de Protecção de Dados verificar o cumprimento do disposto no presente artigo.
7. Nos casos de subcontratação, os subcontratados notificam o responsável pelo tratamento de qualquer violação de dados pessoais de que tenha conhecimento, sem demora injustificada.

Artigo 42.º

(Comunicação de uma violação de dados pessoais ao titular dos dados)

1. Caso se verifique uma violação de dados pessoais susceptível de resultar num elevado risco para os direitos, liberdades e garantias do titular dos dados, o responsável pelo tratamento comunica-lhe a violação, sem demora injustificada.
2. A comunicação ao titular dos dados descreve, numa linguagem clara e simples, a natureza da violação dos dados pessoais e inclui as informações e as medidas referidas nas alíneas b) e c) do n.º 4 do artigo anterior.
3. A comunicação é dispensada nos casos em que:
 - a) O responsável pelo tratamento tiver adoptado medidas de protecção adequadas, tanto tecnológicas como organizativas, e estas tiverem sido aplicadas aos dados afectados pela violação de dados pessoais;
 - b) O responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que a concretização do elevado risco referido no número 1 deixou de ser provável; ou
 - c) Implicar um esforço desproporcionado, devendo, neste caso, o responsável pelo tratamento informar os titulares dos dados de outra forma igualmente eficaz, nomeadamente através de comunicação pública.
4. Se o responsável pelo tratamento não tiver comunicado a violação de dados pessoais ao titular dos dados, a Agência de Protecção de Dados, caso considere que da violação de dados pessoais resulta um elevado risco para os seus direitos, liberdades e garantias, pode exigir ao responsável que proceda a essa comunicação.

Artigo 43.º

(Avaliação de impacto de tratamentos de dados)

1. Se o responsável pelo tratamento pretender realizar algum tipo de tratamento de dados que, pela sua natureza, alcance, contexto ou finalidades, possa representar um alto risco para os direitos e liberdades dos titulares dos dados, deve realizar, antes da implementação do tratamento, uma avaliação de impacto das operações de tratamento sobre a protecção de dados pessoais.
2. A realização de uma avaliação de impacto sobre a protecção de dados a que se refere o n.º 1 é obrigatória, nomeadamente em caso de:
 - a) Avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfís, sendo com base nela adoptadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afectem significativamente de forma similar;
 - b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o n.º 1 do artigo 17.º, ou de dados pessoais relacionados com condenações penais e infracções a que se refere o artigo 21.º; ou
 - c) Controlo sistemático de zonas acessíveis ao público em grande escala.
3. Ao efectuar uma avaliação de impacto sobre a protecção de dados, o responsável pelo tratamento solicita parecer do encarregado da protecção de dados, nos casos em que este tenha sido designado.
4. A Agência de Protecção de Dados elabora e torna pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto sobre a protecção de dados por força do n.º 1.

5. A Agência de Protecção de Dados pode também elaborar e tornar pública uma lista dos tipos de operações de tratamento em relação aos quais não é obrigatória uma análise de impacto sobre a protecção de dados.

6. A avaliação inclui, pelo menos:

a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;

b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;

c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o n.º 1; e

d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a protecção dos dados pessoais e a demonstrar a conformidade com o presente diploma, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

7. Se se revelar necessário, o responsável pelo tratamento solicita a opinião dos titulares dos dados ou dos seus representantes sobre o tratamento previsto, sem prejuízo da defesa dos interesses comerciais ou públicos ou da segurança das operações de tratamento.

8. Se necessário, o responsável pelo tratamento procede a um controlo para avaliar se o tratamento é realizado em conformidade com a avaliação de impacto sobre a protecção de dados, pelo menos quando haja uma alteração dos riscos que as operações de tratamento representam.

9. O responsável pelo tratamento ou, se for caso disso, o seu representante, deve, no momento da notificação do tratamento, comunicar à Agência de

Protecção de Dados o resultado da avaliação de impacto de protecção de dados que se refere o n.º 1.

SECÇÃO II

Encarregado de Protecção de Dados

Artigo 44.º

(Designação do encarregado da protecção de dados)

1. O responsável pelo tratamento e o subcontratado designam um Encarregado da Protecção de Dados sempre que:

a) O tratamento for efectuado por uma autoridade ou um organismo público, exceptuando os Tribunais e o Ministério Público no exercício das suas competências processuais;

b) As actividades principais do responsável pelo tratamento ou do subcontratado consistam em operações de tratamento que, devido à natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou

c) As actividades principais do responsável pelo tratamento ou do subcontratado consistam em operações de tratamento em grande escala de categorias de dados especiais previstos na presente lei e de dados relacionados com condenações penais e infracções a que se refere a presente lei.

3. Um grupo empresarial pode designar um único encarregado da protecção de dados desde que o mesmo seja facilmente acessível a partir de cada estabelecimento.

4. Quando o responsável pelo tratamento ou o subcontratado for uma autoridade ou um organismo público, pode ser designado um único encarregado da protecção de dados para várias dessas autoridades ou organismos, tendo em conta a respetiva estrutura organizacional e dimensão.

5. O Encarregado de Protecção de Dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de protecção de dados, bem como na sua capacidade para desempenhar as funções referidas na presente lei.
6. O Encarregado da Protecção de Dados pode ser um elemento do pessoal da entidade responsável pelo tratamento ou do subcontratado, ou exercer as suas funções com base num contrato de prestação de serviços.
7. O responsável pelo tratamento comunica à Agência de Protecção de Dados os contactos do Encarregado da Protecção de Dados.
8. O Encarregado de Protecção de Dados deve estar inscrito na Agência de Protecção de Dados, conforme estabelecido nas directrizes definidas por esta entidade.

Artigo 45.º

(Posição do encarregado de protecção de dados)

1. O responsável pelo tratamento e o subcontratado asseguram que o encarregado da protecção de dados seja envolvido, de forma adequada e em tempo útil, em todas as questões relacionadas com a protecção de dados pessoais.
2. O responsável pelo tratamento e o subcontratado apoiam o encarregado da protecção de dados no exercício das funções, fornecendo-lhe os recursos necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento.
3. O responsável pelo tratamento e o subcontratado asseguram que o encarregado da protecção de dados não recebe instruções relativamente ao exercício das suas funções.

4. O encarregado não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratado pelo facto de exercer as suas funções.
5. O encarregado da protecção de dados informa directamente a direcção ao mais alto nível do responsável pelo tratamento ou do subcontratado.
6. Os titulares dos dados podem contactar o encarregado da protecção de dados sobre todas as questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos direitos que lhe são conferidos pelo presente diploma.
7. O encarregado da protecção de dados está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções.
8. O encarregado da protecção de dados pode exercer outras funções e atribuições, devendo o responsável pelo tratamento ou o subcontratado assegurar que essas funções e atribuições não resultem num conflito de interesses.

Artigo 46.º

(Funções do encarregado de protecção de dados)

1. O encarregado da protecção de dados tem, pelo menos, as seguintes funções:
 - a) Informar e aconselhar o responsável pelo tratamento ou o subcontratado, bem como os trabalhadores que tratam os dados, a respeito das suas obrigações nos termos da presente lei;
 - b) Controlar a conformidade das políticas do responsável pelo tratamento ou do subcontratado relativas à protecção de dados pessoais com a presente lei, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;
 - c) Prestar aconselhamento, quando tal for solicitado, no que respeita à avaliação de impacto sobre a protecção de dados e controla a sua realização nos termos da presente lei;

- d) Cooperar com a Agência de Protecção de Dados;
- e) Servir como ponto de contacto para a Agência de Protecção de Dados sobre questões relacionadas com o tratamento de dados pessoais efetuado;
2. No desempenho das suas funções, o encarregado da protecção de dados tem em devida consideração os riscos associados às operações de tratamento, levando em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

Artigo 47.º

(Dever de sigilo)

1. Os responsáveis pelo tratamento, os subcontratados, bem como qualquer outra pessoa que, no exercício das suas funções, tenha acesso aos dados pessoais, ficam obrigados a sigilo profissional, mesmo após o termo das suas funções.
2. O disposto no número anterior aplica-se aos membros da Agência de Protecção de Dados, bem como aos funcionários, agentes ou técnicos que aí exerçam funções.
3. O disposto nos números anteriores não exclui o dever de transmitir informações obrigatórias, nos termos legais.

SECÇÃO III

Relações entre Intervenientes no Tratamento de Dados

Artigo 48.º

(Relação entre o responsável pelo tratamento e subcontratado)

1. O responsável pelo tratamento deve considerar os riscos para os titulares dos dados e garantir os seus direitos tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados.

2. Nos termos do número anterior devem ser aplicadas as medidas técnicas e organizativas que forem adequadas para garantir e demonstrar a realização do tratamento com respeito pela presente lei.
3. Atendendo à natureza de um tratamento de dados pessoais, e à definição de finalidade e de meios para a sua concretização, podem existir dois ou mais responsáveis pelo tratamento, que actuam como responsáveis conjuntos, acordando as responsabilidades de cada um para o cumprimento da presente lei, e para garantir o respeito pelos direitos do titular dos dados.
4. O responsável pelo tratamento pode recorrer, por via contratual, a subcontratado que apresente garantias adequadas para a execução de medidas técnicas e organizativas para assegurar o cumprimento da presente lei e a defesa dos direitos do titular dos dados.
5. O tratamento por subcontratado pode estar determinado na lei.
6. O subcontratado pode contratar outro subcontratado, desde que para tal esteja autorizado pelo responsável pelo tratamento.

Artigo 49.º

(Conteúdo do contrato ou de acto normativo)

O contrato ou outro acto normativo deve prever para o subcontratado, designadamente, as seguintes obrigações:

- a) Tratar os dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento;
- b) Assegurar que as pessoas autorizadas a tratar os dados pessoais assumam um compromisso formal ou legal de confidencialidade;
- c) Garantir todas as exigências impostas pela presente lei no que respeita a medidas técnicas e organizacionais;
- d) Devolver ou apagar os dados pessoais findo o contrato;

e) Apagar as cópias existentes, a menos que a conservação dos dados seja exigida por lei;

f) Disponibilizar ao responsável pelo tratamento as informações necessárias para demonstrar o cumprimento das obrigações previstas no presente artigo e não se opor à realização de auditorias e inspeções, conduzidas pelo responsável pelo tratamento ou por auditor por este mandatado;

g) Se tal ocorrer na prossecução do contrato, informar imediatamente o responsável pelo tratamento de que uma instrução seja, na sua interpretação, violadora da presente lei.

8. O recurso à subcontratação não altera o facto de o responsável pelo tratamento deter a responsabilidade global pela protecção dos dados pessoais.

Artigo 50.º

(Confidencialidade do tratamento)

Qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratado, bem como o próprio subcontratado, tenha acesso a dados pessoais, não pode proceder ao seu tratamento sem instruções do responsável pelo tratamento, salvo por força de obrigações legais.

Capítulo V

Transferência Internacional de Dados

Artigo 51.º

(Regra geral sobre as transferências internacionais de dados)

1. As transferências de dados pessoais para fora do território nacional, podem ocorrer verificando-se uma das seguintes circunstâncias:

a) Se o Estado ou organização internacional receptor fornecer um nível adequado de protecção de dados;

b) Se a entidade exportadora dos dados fornecer garantias apropriadas para o tratamento dos dados pessoais, em conformidade com as condições mínimas e suficientes estabelecidas na presente lei;

c) Se ocorrer umas das situações excepcionais descritas no artigo 53.º da presente lei.

2. O ónus da prova para demonstrar que a transferência internacional está em conformidade com o disposto na presente lei recai, em todos os casos, sobre a entidade exportadora dos dados.

3. A transferência de dados pessoais que constitua medida necessária à protecção da segurança do Estado, da defesa, da segurança pública e da prevenção, investigação e repressão das infracções penais é regida por disposições legais específicas ou pelas convenções, tratados e acordos internacionais de que a República de Angola seja parte.

Artigo 52.º

(Transferências internacionais de dados com base em uma decisão adequada)

1. As transferências de dados pessoais que sejam ou venham a ser objecto de tratamento para um Estado ou organização internacional só serão realizadas se, sem prejuízo das outras disposições da presente lei, as condições estabelecidas forem respeitadas pelo responsável pelo tratamento e pelo subcontratado.

2. Compete à Agência de Protecção de Dados decidir se um Estado ou organização internacional dispõe de um nível de protecção de dados pessoais, levando em consideração os seguintes elementos:

a) As circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados, em especial, a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projectados, os países de origem e de

destino final, as regras em vigor no país em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas no referido Estado.

b) A existência de regras sobre a garantia do Estado de Direito, sobre a tutela dos direitos fundamentais, bem como a existência e o efetivo funcionamento de uma autoridade de controlo independente ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de protecção de dados, e adoptadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo de outros Estados;

c) Os compromissos internacionais assumidos pelo referido Estado ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à protecção de dados pessoais.

Artigo 53.º

(Transferências internacionais de dados com base em garantias adequadas)

1. Na ausência de uma decisão de adequação, as garantias adequadas podem ser obtidas pelos seguintes meios:

a) Um instrumento juridicamente vinculativo e exigível entre autoridades ou organismos públicos da República de Angola e outros Estados ou organizações internacionais, contendo os princípios, direitos e obrigações estabelecidos nesta lei;

b) Um acordo internacional bilateral ou multilateral, entre a República de Angola e outros Estados ou organizações internacionais, que contenha os princípios, obrigações e direitos estabelecidos nesta lei, e que permita

transferências de entidades privadas ou públicas estabelecidas em Angola para entidades privadas e ou públicas estabelecidas em outros países;

c) Acordos ou convénios que reconheçam expressamente os princípios, direitos e obrigações previstas nesta lei, que podem assumir as seguintes formas:

- i. Cláusulas contratuais modelo, previamente aprovadas pela Agência de Protecção de Dados;
- ii. Normas corporativas vinculantes, aprovadas pela Agência de Protecção de Dados e aplicáveis a todos os membros de um grupo económico nos termos definidos na presente lei;

2. Para efeitos do disposto do presente artigo, o acordo ou mecanismo que instrumentaliza a transferência internacional deve reconhecer que a parte exportadora está sujeita à jurisdição da Agência de Protecção de Dados e aos tribunais competentes da República de Angola e garantir que a parte importadora esteja sujeita à jurisdição de uma ou mais autoridades de supervisão independentes, para que os titulares de dados tenham os instrumentos legais eficazes para proteger os seus direitos.

Artigo 54.º

(Situações excepcionais)

1. Nas situações em que não haja uma decisão de adequação ou em que não exista instrumentos de garantias adequadas, as transferências internacionais de dados podem ser realizadas, excepcionalmente, nas seguintes circunstâncias:

a) Se o titular dos dados tiver explicitamente dado o seu consentimento à transferência, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas;

- b) A transferência for necessária para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido do titular dos dados;
- c) A transferência for necessária para a celebração ou execução de um contrato, celebrado no interesse do titular dos dados, entre o responsável pelo seu tratamento e outra pessoa singular ou colectiva;
- d) A transferência for necessária por importantes razões de interesse público;
- e) A transferência for necessária à declaração, ao exercício ou à defesa de um direito num processo judicial;
- f) A transferência for necessária para proteger interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento.

2. As excepções descritas no presente artigo não podem ser usadas para realizar transferências internacionais de forma regular ou habitual.

Capítulo VI

Autoridade Nacional para a Fiscalização de Protecção de Dados Pessoais

Artigo 55.º

(Objetivos da fiscalização)

A fiscalização da protecção de dados pessoais visa acompanhar, avaliar e controlar a actividade dos órgãos ou serviços legalmente competentes para o seu tratamento, velando pelo cumprimento da Constituição e da lei, particularmente do regime de direitos, liberdades e garantias fundamentais dos cidadãos.

Artigo 56.º

(Natureza)

1. A fiscalização da protecção de dados pessoais é assegurada pela Agência de Protecção de Dados, abreviadamente APD, que reveste a natureza de entidade administrativa independente, doptada de personalidade jurídica, com autonomia financeira, administrativa e patrimonial.
2. A APD é regulada por lei própria.

Artigo 57.º

(Atribuições genéricas)

No exercício da actividade de regulação, controlo e supervisão dos tratamentos de dados pessoais, a Agência de Protecção de Dados tem as seguintes atribuições:

- a) Fiscalizar o cumprimento e fazer aplicar o disposto na presente lei;
- b) Emitir parecer sobre quaisquer iniciativas legislativas e medidas regulamentares que envolvam matéria de protecção de dados pessoais
- c) Representar a República de Angola junto de organizações internacionais responsáveis pela área da protecção de dados pessoais;
- d) Apreciar as reclamações, queixas ou petições dos particulares;
- e) Obter acesso às instalações do responsável pelo tratamento e do subcontratante, incluindo os equipamentos e meios de tratamento de dados pessoais;
- f) Efectuar inspecções às entidades públicas e privadas com vista a avaliar o tratamento de dados pessoais;
- g) Emitir ordens, directrizes, comunicações e outros actos administrativos para garantir o tratamento adequado dos dados pessoais e os direitos dos titulares;

- h) Promover a sensibilização e a compreensão do público relativamente aos riscos, às regras, às garantias e aos direitos associados ao tratamento de dados pessoais;
- i) Apoiar as entidades públicas e privadas na elaboração de estudos, programas e projectos sobre a aplicação e controlo da legislação sobre protecção de dados pessoais;
- j) Promover a criação de procedimentos de certificação em matéria de protecção de dados, bem como selos e marcas de protecção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratados com a presente lei.
- k) Promover a implementação dos códigos de conduta no âmbito da protecção de dados pessoais;
- l) Prestar informações aos titulares de dados, se tal lhe for solicitado, sobre o exercício dos seus direitos nos termos da presente lei;
- m) Garantir as publicações, em suporte de papel e, ou, digital, que sejam consideradas úteis para a difusão da matéria dos dados pessoais, designadamente o boletim anual, legislação sobre protecção de dados, campanhas publicitárias de divulgação sobre protecção de dados pessoais;
- n) Promover formação e incorporação de conteúdos educativos relacionados ao tratamento de dados, privacidade e autodeterminação informativa;
- o) Solicitar informações aos responsáveis pelo tratamento, encarregados de protecção de dados e representantes, os quais devem fornecer os antecedentes, documentos, programas ou outros elementos relativos ao tratamento de dados solicitados;
- p) Desenvolver estratégias para prevenir a violência digital relacionada à defesa da privacidade e ao tratamento de dados, bem como promover, organizar e desenvolver programas voltados para a protecção de dados pessoais de

crianças e adolescentes na internet, jogos eletrônicos e outras plataformas digitais;

q) Sugerir aos órgãos legislativos competentes alterações à legislação sobre protecção de dados pessoais;

r) Autorizar e registar o tratamento de dados pessoais, nos termos da presente lei.

s) Aplicar coimas e sanções acessórias;

t) Exercer outras atribuições conferidas por lei.

Capítulo VII

Controlo Prévio dos Tratamentos de Dados Pessoais

Artigo 58.º

(Dever de notificação)

1. O responsável pelo tratamento de dados, ou seu representante quando aplicável, deve notificar a Agência de Protecção de Dados antes de iniciar qualquer tratamento de dados pessoais.

2. Excepto no caso de tratamento sujeitos a autorização, a Agência de Protecção de Dados deve se pronunciar sobre a notificação do responsável pelo tratamento no prazo de 10 dias após a sua recepção, findo este período se entende que o tratamento foi devidamente notificado.

3. A Agência de Protecção de Dados pode autorizar a simplificação ou a isenção da notificação para determinadas categorias de tratamento que, atendendo à especificidade dos dados, não sejam susceptíveis de pôr em causa os direitos, garantias e liberdades fundamentais dos titulares dos dados, e tendo em conta critérios de celeridade, economia e eficiência.

4. A decisão de isenção deve, entre outros aspectos, especificar as finalidades do tratamento, os dados ou categorias de dados a tratar, a categoria ou categorias de titulares dos dados, os destinatários ou categorias de destinatários a quem podem ser comunicados os dados e o período de conservação dos dados.

5. Estão isentos de notificação os tratamentos cuja única finalidade seja a manutenção de registos que se destinem a informação do público e possam ser consultados pelo público em geral ou por qualquer pessoa que provar um interesse legítimo.

Artigo 59.º

(Tratamentos de dados sujeitos à autorização)

1. Salvo se disposto em contrário por outro diploma legal, carecem de autorização da Agência de Protecção de Dados:

- a) O tratamento dos dados pessoais relativos a dados especiais;
- b) O tratamento dos dados pessoais relativos ao crédito e à solvabilidade dos seus titulares;
- c) As operações de comunicação, interconexão e transferências de dados pessoais prevista na presente lei;
- d) A utilização de dados pessoais para fins não determinantes da recolha;
- e) Os tratamentos de dados pessoais resultantes da gravação de chamadas para fins comerciais.

2. O diploma legal que autorizar os tratamentos a que se refere o número anterior carece de prévio parecer da Agência de Protecção de Dados.

3. É dispensada a obtenção de autorização da Agência de Protecção de Dados se o tratamento decorrer de diploma legal, bastando neste caso proceder a mera notificação, salvo se indicado em contrário em legislação específica.

Artigo 60.º

(Conteúdo dos pedidos de parecer, notificação e autorização da notificação)

Os pedidos de parecer e de autorização, bem como as notificações remetidas à Agência de Protecção de Dados devem conter as seguintes informações:

- a) O nome e o endereço do responsável pelo tratamento e, se for caso, do seu representante;
- b) A ou as finalidades do tratamento;
- c) A descrição da ou das categorias de titulares dos dados ou das categorias de dados pessoais que lhes respeitem;
- d) Os destinatários ou as categorias de destinatários a quem os dados podem ser comunicados e em que condições;
- e) A entidade encarregada do processamento da informação, se não for o próprio responsável do tratamento;
- f) As eventuais interconexões de tratamentos de dados pessoais;
- g) O tempo de conservação dos dados pessoais;
- h) A forma e as condições como os titulares dos dados podem ter conhecimento ou fazer corrigir os dados pessoais que lhes respeitem;
- i) As transferências de dados previstas para países terceiros;
- j) A descrição geral que permita avaliar de forma preliminar a adequação das medidas tomadas para garantir a segurança de tratamentos de interconexão.

Artigo 61.º

(Indicações obrigatórias)

As autorizações e os registos das notificações de tratamentos de dados pessoais emitidos pela Agência de Protecção de Dados devem, pelo menos, indicar:

- a) O responsável do ficheiro e, se for caso disso, o seu representante;
- b) As categorias de dados pessoais tratados;
- c) A ou as finalidades a que se destinam os dados e as categorias de entidades a quem podem ser transmitidos;
- d) A forma de exercício do direito de acesso e de rectificação;
- e) As eventuais interconexões de tratamentos de dados pessoais;
- f) As transferências de dados previstas para outros países.

Artigo 62.º

(Publicidade dos tratamentos)

1. O tratamento dos dados pessoais, quando não for objecto de diploma legal e dever ser autorizado ou notificado, consta de registo na Agência de Protecção de Dados aberto à consulta por qualquer pessoa.
2. O registo contém as informações enumeradas no artigo 61.º da presente lei.
3. O responsável por tratamento de dados não sujeito a notificação está obrigado a prestar, de forma adequada, a qualquer pessoa que lho solicite.
4. O disposto no presente artigo não se aplica a tratamentos cuja única finalidade seja a manutenção de registos que, nos termos de disposições legislativas ou regulamentares, se destinem à informação do público e se

encontrem abertos à consulta do público em geral ou de qualquer pessoa que possa provar um interesse legítimo.

5. A Agência de Protecção de Dados deve indicar no seu relatório anual todos os pareceres e autorizações elaborados ou concedidas ao abrigo da presente lei.

Artigo 63.º

(Códigos de conduta)

1. A Agência de Protecção de Dados estimula a criação de códigos de conduta que se destinam a contribuir, em função das características dos distintos sectores de actividade, para a boa execução das normas sobre protecção de dados.

2. É incentivada a participação de representantes dos direitos titulares dos dados na elaboração e aplicação dos códigos de conduta.

3. Os códigos de conduta devem ser registados na Agência de Protecção de Dados.

4. Cabe à Agência de Protecção de Dados emitir pareceres e recomendações para que os responsáveis pela criação dos códigos de conduta efectuem as correcções necessárias.

Capítulo VIII

Procedimentos e Sanções

SECÇÃO I

Processo Sancionatório

Artigo 64.º

(Prestação de informações)

1. Para efeitos de aplicação da presente lei, a Agência de Protecção de Dados pode solicitar, por escrito, a qualquer entidade pública ou privada, todas as

informações necessárias.

2. O pedido referido no número anterior deve ser instruído com os seguintes elementos:

- a) A base jurídica, a qualidade em que o destinatário é solicitado a transmitir o requerido e o objectivo do pedido;
- b) O prazo para o fornecimento do requerido;
- c) A menção de que o destinatário deve identificar, de maneira fundamentada, as informações que considera confidenciais, por motivo de segredos de negócio, juntando, nesse caso, uma cópia não confidencial dos documentos, ficheiros ou mensagens que contenham tais informações, expurgada das mesmas e incluindo descrição concisa da informação omitida que permita apreender o sentido da mesma;
- d) A indicação de que o incumprimento do pedido constitui contraordenação, nos termos da presente lei.

3. Os pedidos de informação efectuados pela Agência de Protecção de Dados devem ser respondidos em prazo não superiores a 10 dias úteis, salvo se, por decisão fundamentada, for fixado prazo diferente.

Artigo 65.º

(Notificações)

1. A notificações são feitas por carta registada, dirigidas ao domicílio do destinatário ou ao seu mandatário judicial.
2. A notificação ao arguido do acto processual que lhe impute a prática de contraordenação, bem como da decisão que lhe aplique coima, sanção acessória ou alguma medida cautelar, é feita nos termos do número anterior ou, quando o arguido não seja encontrado ou se recuse a receber a notificação, por anúncio publicado num dos jornais do país.

Artigo 66.º

(Abertura de inquérito)

1. Sempre que, por qualquer via, a Agência de Protecção de Dados tome conhecimento de práticas que violem as normas da presente lei obriga-se à abertura de inquérito, notificando a parte visada, e a promover as diligências de investigação necessárias ao seu apuramento e responsabilização dos respectivos agentes.
2. A realização de diligências investigativas previstas no número anterior pode ser dispensada quando houver evidências substanciais da ocorrência da infracção, devendo, neste caso, iniciar-se imediatamente o procedimento sancionatório correspondente.
3. Qualquer pessoa, física ou jurídica, que tiver notícia de uma prática que viole as disposições da presente lei pode denunciá-la à Agência de Protecção de Dados.

Artigo 67.º

(Tramitação do processo de inquérito)

1. O inquérito deve ser realizado no prazo determinado por instrutivo interno da Agência de Protecção de Dados.
2. A Agência de Protecção de Dados deve dar conhecimento a entidade alvo de inquérito sobre o seu objecto, finalidade e duração.
3. O inquérito deve ser realizado sob sigilo, com vista à salvaguarda das investigações e do prestígio da entidade alvo.
4. No exercício de poderes de inquérito, a Agência de Protecção de Dados pode:
 - a) Solicitar a exibição ou o envio de documentos e dados necessários para a realização exitosa do inquérito;

b) Aceder às instalações, bem como aos equipamentos físicos e digitais utilizados para o tratamento de dados.

c) Solicitar, no decurso das diligências a que se referem as alíneas anteriores, a qualquer representante ou trabalhador da empresa, esclarecimentos necessários ao desenvolvimento das diligências.

Artigo 68.º

(Medidas cautelares)

1. Nos casos em que se considere que a continuação de um tratamento de dados pessoais pode afectar gravemente os princípios previstos na presente lei ou causar prejuízos aos direitos dos titulares dos dados, pode a Agência de Protecção de Dados, no respeito pelo princípio da proporcionalidade, em qualquer momento da investigação ordenar a suspensão do tratamento, bem como o bloqueio ou a eliminação dos dados.

2. As adopção das medidas cautelares previstas no número anterior têm um prazo de duração não superior a 90 dias, salvo prorrogação devidamente fundamentada, sempre que seja necessário e adequado, até à sua revogação ou até à decisão final do processo.

Artigo 69.º

(Deliberação sobre o relatório de inquérito)

1. A conclusão do inquérito dá-se com a elaboração do relatório final, o qual deve conter as constatações, conclusões e recomendações sobre os factos inquiridos.

2. Recebido o relatório final de inquérito, deve ser tomada uma das seguintes decisões:

a) Abertura do processo sancionatório através de notificação, com o envio na nota de acusação.

b) Arquivamento do processo quando não se verifique indícios de ilicitude.

Artigo 70.º

(Instrução do processo sancionatório)

1. Notificado da acusação, o arguido dispõe do prazo de 15 dias úteis, para se pronunciar por escrito sobre os factos que lhe são imputados, devendo juntar os documentos probatórios de que disponha e arrolar testemunhas, até ao máximo de três por cada infração, para serem ouvidos, em dia a designar pela Agência de Protecção de Dados.
2. A falta de comparência do arguido não obsta a que o processo de contraordenação siga os seus termos.

Artigo 71.º

(Prescrição)

1. O procedimento para aplicação das sanções previstas na presente lei prescreve no prazo de 5 (cinco) anos.
2. O prazo de prescrição das coimas e sanções acessórias é de cinco anos a contar do dia em que a decisão administrativa se tornar definitiva ou do dia em que a decisão judicial transitar em julgado.

SECÇÃO II

Contraordenações e Coimas

Artigo 72.º

(Aplicação das Coimas)

1. A aplicação das coimas previstas na presente lei compete à Agência de Protecção de Dados.

2. A deliberação da Agência de Protecção de Dados, depois de homologadas pelo seu Presidente, constitui título executivo, no caso de não ser impugnada no prazo legal.

3. As deliberações da Agência de Protecção de Dados são públicas.

Artigo 73.º

(Contraordenações e coimas)

1. Sem prejuízo de outras sanções que se mostrem aplicáveis, constituem contraordenações punidas com coimas definidas no n.º 2 do presente artigo as seguintes situações:

- a) Não designar representante nos termos previstos no n. 3 do artigo 3.º;
- b) Violação dos princípios previstos nos artigos 6.º, 7.º, 8.º, 9.º, 10.º, 11.º e 12.º;
- c) Violação das regras do consentimento previstas nos artigos 15.º e 16.º;
- d) Violação dos artigos 17.º, sobre tratamento de dados especiais;
- e) Violação das regras sobre os tratamentos de dados pessoais previstos nos 18.º, 19.º, 20.º, 21.º, 22.º e 23.º;
- f) Violação dos artigos 24.º e 25.º, sobre a comunicação e interconexão de dados pessoais;
- g) Violação do artigo 26.º, 27.º, 28.º, 29.º, 30.º, 31.º, 32.º, 33.º e 34.º sobre os direitos dos titulares dos dados pessoais;
- h) Violação do estabelecido nos artigos 36.º, 37.º e 38.º, sobre tratamento de dados pessoais por sistema de inteligência artificial;
- i) Violação do artigo 39.º, sobre protecção de dados desde a concepção e por defeito;
- J) Violação do artigo 40.º, sobre a segurança de dados pessoais;

- k) Violação do artigo 41.º sobre o dever de notificar a violação de dados pessoais à Agência de Protecção de Dados;
- l) Violação do artigo 42.º sobre o dever de comunicação de uma violação de dados pessoais ao titular dos dados;
- m) Violação do artigo 43.º, sobre avaliação de impacto de tratamentos de dados;
- n) Violação do artigo 44.º, sobre a designação do encarregado da protecção de dados;
- o) Violação do n.º 1 do artigo 47.º sobre o dever de sigilo;
- p) Violação dos artigos 53.º e 54.º sobre transferências internacionais de dados;
- q) Violação do artigo 58.º sobre o dever de notificação;
- r) Violação do artigo 59.º sobre o tratamento sujeitos à autorização;
- s) Violação ou não acatamento das medidas cautelares previstas no artigo 68.º e de outras orientações emanadas pela Agência de Protecção de Dados nos termos da presente lei.

2. As contraordenações referidas no número anterior são punidas com coima de:

- a) De Kz 150 000,00 (Cento e cinquenta mil Kwanzas) a 5 000 000,00 (Cinco milhões de Kwanzas), no caso de pessoas singulares;
- a) De Kz 5 000 000,00 (Cinco milhões de Kwanzas) a 500 000 000,00 (Quinhentos milhões de Kwanzas), no caso de pessoas colectivas e meras associações de facto.

3. Tratando-se de violação de dados pessoais a coima é agravada no dobro dos respectivos limites

4. A coima é paga de uma vez só e pelo valor integral, sem prejuízo de a Agência de Protecção de Dados poder autorizar o pagamento faseado, sempre que a situação económica do visado, fundadamente, o justifique.

5. Nos casos de pagamento faseado, a última prestação não pode ir além dos três anos subsequentes ao carácter definitivo da decisão, e a falta de pagamento de uma prestação implica o vencimento de todas as outras, podendo, dentro dos limites referidos, os prazos e os planos de pagamento inicialmente estabelecidos serem alterados quando motivos supervenientes o justificarem.

6. A tentativa e a negligência são puníveis.

Artigo 74.º

(Pagamento voluntário da coima)

1. É admissível o pagamento voluntário da coima, devendo, em tais circunstâncias, ter-se em consideração o seguinte:

a) O pagamento da coima no prazo de duas semanas, sem contestação judicial, implica a redução para metade do valor decidido pela Agência de Protecção de Dados;

b) Tratando-se de dados especiais, o pagamento da coima no prazo de duas semanas, sem contestação judicial, implica a redução para dois terços do valor decidido pela Agência de Protecção de Dados.

Artigo 75.º

(Destino das receitas cobradas)

O montante das importâncias cobradas como resultado da aplicação das coimas reverte 70% para a Agência de Protecção de Dados e 30% para a Conta única do Tesouro.

Artigo 76.º

(Medidas corretivas)

Para além da aplicação de coimas, a Agência de Protecção de Dados pode recorrer aos seguintes meios de correcção para garantir a aplicação da presente lei:

- a) Advertir o responsável pelo tratamento ou ao subcontratado no sentido de que as operações de tratamento previstas são susceptíveis de violar as disposições da presente lei;
- b) Repreender o responsável pelo tratamento ou ao subcontratado sempre que as operações de tratamento tiverem violado as disposições da presente lei, mas não exista gravidade para a aplicação de coima;
- c) Ordenar ao responsável pelo tratamento ou ao subcontratado que satisfaça os pedidos de exercício de direitos apresentados pelo titular dos dados nos termos da presente lei.

Artigo 77.º

(Legislação subsidiária)

Em tudo o que não seja contrário ao disposto na presente secção, aplicam-se, subsidiariamente, as normas do Código do Procedimento Administrativo e as da Lei sobre o Regime Geral das Contra-ordenações, bem como a demais legislação pertinente.

SECÇÃO II

Crimes

Artigo 78.º

(Legitimidade da Agência de Protecção de Dados)

A Agência de Protecção de Dados tem legitimidade para intervir em processos judiciais no caso de violação das disposições da presente lei, e deve denunciar

ao Ministério Público as infracções penais de que tiver conhecimento, no exercício das suas funções e por causa delas, bem como praticar os actos cautelares necessários e urgentes para assegurar os meios de prova.

Artigo 79.º

(Utilização de dados de forma incompatível com a finalidade da recolha)

Quem utilizar dados pessoais tratados ao abrigo da presente lei de forma incompatível com a finalidade determinante da respetiva recolha é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.

Artigo 80.º

(Interconexão ilegal de dados)

Quem, intencionalmente, promover ou efectuar uma interconexão ilegal de dados pessoais tratados ao abrigo da presente lei, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.

Artigo 81.º

(Acesso indevido)

1. Quem, sem a devida autorização ou justificação, aceder, por qualquer modo, a dados pessoais é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
2. A pena é também agravada para o dobro nos seus limites quando o acesso:
 - a) For conseguido através de violação de regras técnicas de segurança;
 - b) Tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial; ou
 - c) O acesso indevido respeitar a dados especiais.

Artigo 82.º

(Desvio de dados)

1. Quem copiar, subtrair, ceder ou transferir, a título oneroso ou gratuito, dados pessoais sem previsão legal ou consentimento, independentemente da finalidade prosseguida, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2. A pena é também agravada para o dobro nos seus limites quando o acesso:

- a) For conseguido através de violação de regras técnicas de segurança;
- b) Tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial; ou
- c) O acesso indevido respeitar a dados especiais.

Artigo 83.º

(Viciação ou destruição de dados)

1. Quem, sem a devida autorização ou justificação, apagar, destruir, danificar, ocultar, suprimir ou modificar dados pessoais, tornando-os inutilizáveis ou afectando o seu potencial de utilização, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.

2. A pena é agravada para o dobro nos seus limites se o dano produzido for particularmente grave.

3. Nas situações previstas nos números anteriores, se o agente actuar com negligência é punido com pena de prisão:

- a) Até 1 ano ou multa até 120 dias, no caso previsto no n.º 1;
- b) Até 2 anos ou multa até 240 dias, no caso previsto no n.º 2.

Artigo 84.º

(Inserção de dados falsos)

1. Quem inserir ou facilitar a inserção de dados pessoais falsos, com a intenção de obter vantagem indevida para si ou para terceiro, ou para causar prejuízo, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.
2. A pena é agravada para o dobro nos seus limites se da inserção referida no número anterior resultar um prejuízo efectivo.

Artigo 85.º

(Violação do dever de sigilo)

1. Quem, obrigado a sigilo profissional nos termos da lei, sem justa causa e sem o devido consentimento, revelar ou divulgar no todo ou em parte dados pessoais é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
2. A pena é agravada para o dobro nos seus limites se o agente:
 - a) For funcionário público ou equiparado, nos termos da lei penal;
 - b) For encarregado de protecção de dados;
 - c) For determinado pela intenção de obter qualquer vantagem patrimonial ou outro benefício ilegítimo;
 - d) Puser em perigo a reputação, a honra ou a intimidade da vida privada de terceiros.
3. A negligência é punível com pena de prisão até 6 meses ou com pena de multa até 60 dias.

Artigo 86.º

(Desobediência)

1. Quem não cumprir as obrigações previstas na presente lei, depois de ultrapassado o prazo que tiver sido fixado pela Agência de Protecção de Dados para o respetivo cumprimento, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2. A pena é agravada para o dobro nos seus limites se, depois de notificado para o efeito, o agente:

- a) Não interromper, cessar ou bloquear o tratamento ilícito de dados;
- b) Não proceder ao apagamento ou destruição dos dados quando legalmente exigível, ou findo o prazo de conservação fixado nos termos da presente lei; ou
- c) Recusar, sem justa causa, a colaboração que lhe for exigida.

Artigo 87.º

(Punibilidade da tentativa)

Nos crimes previstos na presente secção, a tentativa é sempre punível.

Artigo 88.º

(Concurso de infracções)

1. Se o mesmo facto constituir simultaneamente crime e contraordenação, o agente é sempre punido a título de crime.
2. Quando se verifique concurso de crime e contraordenação, ou quando, pelo mesmo facto, uma pessoa deva responder a título de crime e outra a título de contraordenação, o processamento da contraordenação cabe às autoridades competentes para o processo criminal, nos termos do regime geral.

Artigo 89.º

(Sanções acessórias)

1. Conjuntamente com as sanções aplicadas pode ser ordenada, acessoriamente, a proibição temporária ou definitiva do tratamento, o bloqueio, o apagamento ou a destruição total ou parcial dos dados.
2. Tratando-se de crimes, ou de multas os Tribunais podem acessoriamente determinar a publicidade da condenação.

Artigo 90.º

(Revogação)

É revogada a Lei n.º 22/11, de 17 de Junho.

Artigo 91.º

(Dúvidas e omissões)

As dúvidas e omissões resultantes da interpretação e aplicação da presente Lei são resolvidas pela Assembleia Nacional.

Artigo 92.º

(Entrada em vigor)

A presente lei entra em vigor à data da sua aprovação.

Vista e aprovada pela Assembleia Nacional, em Luanda, aos ____ de _____ de 2025.

A Presidente da Assembleia Nacional

Carolina Cerqueira

Promulgada aos ____ de _____ de 2025.

Publique-se.

O Presidente da República

João Manuel Gonçalves Lourenço