



Anteprojecto da Lei das TI



Anteprojecto da Lei das Tecnologias de Informação da República de Angola

Índice

Título I

Comércio Electrónico

CAPÍTULO I – Objecto e Âmbito	Pág. 8
CAPÍTULO II – Prestadores de Serviço da Sociedade de Informação	Pág. 9
CAPÍTULO III – Responsabilidade dos Prestadores de Serviços em Rede	Pág. 13
CAPÍTULO IV – Comunicações Publicitárias em Rede e Marketing Directo	Pág. 17
CAPÍTULO V – Contratação Electrónica	Pág. 20
CAPÍTULO VI – Entidades de Supervisão e Regime Sancionatório	Pág. 24
CAPÍTULO VII – Disposições Finais	Pág. 29

Título II

Documentos electrónicos e Assinatura Digital

CAPÍTULO I – Documentos e Actos Jurídicos Electrónicos	Pág. 30
CAPÍTULO II – Assinaturas Electrónicas Qualificadas	Pág. 35
CAPÍTULO III – Certificação	Pág. 36
○ SECCÃO I – Acesso à Actividade de Certificação	Pág. 36
○ SECCÃO II – Exercício da Actividade	Pág. 45
○ SECCÃO III – Certificados	Pág. 49
CAPÍTULO IV – Fiscalização	Pág. 53
CAPÍTULO V – Disposições Finais	Pág. 55



Título III

Protecção Jurídica de Dados Pessoais

CAPÍTULO I – Disposições Gerais	Pág. 55
CAPÍTULO II – Tratamento de Dados Pessoais	Pág. 59
o SECÇÃO I – Qualidade dos Dados e Legitimidade do seu Tratamento	Pág. 59
o SECÇÃO II – Direito do Titular dos Dados	Pág.63
o SECÇÃO III – Segurança e Confidencialidade do Tratamento	Pág. 68
CAPÍTULO III – Transferência de Dados Pessoais	Pág. 72
CAPÍTULO IV – Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de protecção de Dados ou Autoridade de Protecção de Dados Pessoais	Pág. 74
o SECÇÃO I – Natureza e Atribuições	Pág. 74
o SECÇÃO II – Notificação	Pág. 78
CAPÍTULO V – Códigos de Conduta	Pág. 82
CAPÍTULO VI - Tutela Administrativa e Jurisdicional	Pág. 83
o SECÇÃO I – Tutela Administrativa e Jurisdicional	Pág. 83
o SECÇÃO II – Contra-ordenações	Pág.84
o SECÇÃO III – Crimes	Pág.86
CAPÍTULO VII – Disposições finais	Pág. 90

Título IV

Protecção da Privacidade no Sector das Comunicações Electrónicas

CAPÍTULO I – Objecto e Âmbito	Pág. 91
CAPÍTULO II – Segurança e Confidencialidade	Pág. 93
CAPÍTULO III – Regime Sancionatório	Pág. 102



Título V

Protecção Jurídica de Programa de Computador

CAPÍTULO I – Âmbito e Objecto	Pág. 103
CAPÍTULO II – Direitos do Autor	Pág. 104
CAPÍTULO III – Direitos do Utente	Pág. 106
CAPÍTULO IV – Disposições Comuns	Pág. 108
CAPÍTULO V – Disposições Finais e Transitórias	Pág. 109

Título VI

Protecção Jurídica de Bases de Dados

CAPÍTULO I – Objecto e Âmbito de Aplicação	Pág. 111
CAPÍTULO II – Direito de Autor	Pág. 112
CAPÍTULO III – Protecção Especial do Fabricante de Bases de Dados	Pág. 115
CAPÍTULO IV – Disposições Comuns	Pág. 118
CAPÍTULO V – Disposições Finais e Transitórias	Pág. 119

Título VII

Criminalidade Informática

CAPÍTULO I – Disposições Gerais	Pág. 120
CAPÍTULO II – Dos Crimes ligados à Informática	Pág. 123
○ SECÇÃO I – Crimes relativos à Confidencialidade, Integridade e Disponibilidade de Dados e Sistemas Informáticos	Pág. 123
○ SECÇÃO II – Crimes Informáticos	Pág. 126
○ SECÇÃO III – Crimes Relacionados com o Conteúdo	Pág. 127
CAPÍTULO III – Penas	Pág. 129
CAPÍTULO IV – Disposições Finais	Pág. 133



Exposição de Motivos do Anteprojecto da Lei das Tecnologias de Informação

A CNTI – Comissão Nacional de Tecnologias de Informação, no âmbito das suas atribuições, que contemplam a promoção da Sociedade da Informação na República de Angola, entendeu que deveria impulsionar a criação de uma Lei que regulasse a matéria das Tecnologias de Informação e Comunicação (TIC).

Como é do conhecimento geral, tem sido uma preocupação constante da CNTI – Comissão Nacional de Tecnologias de Informação contribuir de forma muito activa para a criação de infra-estruturas relacionadas com as TIC. Neste sentido, procedeu-se à criação do Portal da República de Angola, dos Portais dos Órgãos do Estado e dos Portais de Apoio ao Cidadão e às Empresas.

A promoção da inserção da República de Angola na Sociedade de Informação é um projecto há muito impulsionado pela CNTI – Comissão Nacional de Tecnologias de Informação, projecto este que se encontra estruturado através do PASI – Plano de Acção para a Sociedade de Informação e PAGE – Plano de Acção para a Governação Electrónica.

Ora, é neste âmbito que se promove, que se dá um primeiro passo, no sentido da criação de uma legislação que contemple a protecção jurídica de matérias como o comércio electrónico, os documentos electrónicos e a assinatura digital, a protecção jurídica de dados pessoais, a protecção da privacidade no sector das comunicações electrónicas, a protecção jurídica de programas de computador, a protecção jurídica de bases de dados e a criminalidade informática.

Estas matérias não esgotam a regulamentação da Sociedade de Informação, matéria esta que se encontra em constante evolução.

Contudo, abarca os principais temas respeitantes à Sociedade de Informação.



A regulamentação das normas aplicáveis à Sociedade de Informação, é necessariamente uma matéria cuja visão tem de ser global, ou seja, tem de ter em atenção os princípios que vigoram neste âmbito na comunidade internacional.

Assim, na elaboração deste Anteprojecto de Lei foram consideradas as normas da União Europeia e dos Estados Unidos da América sobre esta matéria, bem como foi consultada legislação de diversos países, nomeadamente a Legislação Indiana.

O Anteprojecto da Lei das Tecnologias de Informação está estruturado em sete títulos, que por sua vez estão subdivididos em capítulos.

O Título I é relativo ao Comércio Electrónico tendo como objecto a regulação do regime jurídico dos prestadores da sociedade de informação e da contratação por via electrónica, no que concerne às obrigações dos prestadores de serviços incluindo aqueles que actuam como intermediários na transacção de conteúdos pelas redes de telecomunicações, as comunicações comerciais por via electrónica, a informação prévia e posterior à celebração de contratos electrónicos, as condições sobre a sua validade e eficácia e o regime sancionatório aplicável aos prestadores de serviços da sociedade de informação.

Estão excluídos do âmbito de aplicação do Título I a matéria fiscal, a disciplina da concorrência, o regime de tratamento de dados pessoais e da protecção da privacidade, o patrocínio judiciário, os jogos de fortuna, a actividade notarial ou equiparadas, a protecção da saúde e da segurança pública. Estas matérias estão excluídas do âmbito de aplicação do presente Anteprojecto Lei por razões de segurança.

O Título I encontra-se subdividido sete capítulos, a saber: objecto e âmbito, prestadores de serviço da sociedade da informação, responsabilidade dos prestadores de serviços em rede, comunicações publicitárias em rede e marketing directo, contratação electrónica, entidades de supervisão e regime sancionatório, e disposições finais.



O **Título II** é relativo aos documentos electrónicos e à assinatura digital tendo como objecto a regulação da validade, da eficácia e do valor probatório dos documentos electrónicos, da assinatura electrónica, e regulação da actividade de certificação de entidades certificadas estabelecidas na República de Angola.

Este Título encontra-se subdividido nos seguintes capítulos: documentos e actos jurídicos electrónicos, assinaturas electrónicas qualificadas, certificação, fiscalização e disposições finais.

O **Título III** é relativo à protecção jurídica de dados pessoais e tem por objecto garantir a protecção, no que concerne ao tratamento de dados pessoais, das liberdades públicas e dos direitos fundamentais das pessoas singulares, em especial a sua honra e a sua intimidade pessoal e familiar.

Este Título encontra-se subdividido nos seguintes capítulos: disposições gerais, tratamento de dados pessoais, transferência de dados pessoais, autoridade de protecção de dados angolana, códigos de conduta, tutela administrativa e jurisdicional e disposições finais.

O **Título IV** versa sobre a protecção da privacidade no sector das comunicações electrónicas, é no fundo um complemento do título anterior, visa a protecção do tratamento de dados pessoais no contexto de redes e serviços de comunicações electrónicas.

Está subdividido em três capítulos, a saber: objecto e âmbito, segurança e confidencialidade e regime sancionatório.

O **Título V** é relativo à Protecção Jurídica de Programa de Computador e visa aplicar aos programas de computador as regras sobre autoria e titularidade vigentes para o direito de autor.

É um título que se encontra subdividido em cinco capítulos, a saber: âmbito e objecto, direitos do autor, direitos do utente, disposições comuns, disposições finais e transitórias.



O **Título VI** é relativo à Protecção Jurídica de Bases de Dados e visa, à semelhança do que sucede no título anterior, atribuir às bases de dados uma protecção idêntica à vigente para os direitos de autor, em função do grau de originalidade das mesmas. Esta protecção é muito relevante em termos económicos e em termos de protecção do investimento financeiro, daqueles que utilizam consideráveis recursos técnicos, humanos e financeiros para a criação de bases de dados.

Este título encontra-se subdividido em cinco capítulos, a saber: objecto e âmbito de aplicação, direitos de autor, protecção especial do fabricante de bases de dados, disposições comuns, e disposições finais e transitórias.

Por último, mas não de somenos importância, temos o **Título VII** relativo à Criminalidade Informática, elaborado com base na Lei da Criminalidade Informática Portuguesa, na Convenção sobre o Cibercrime, assinada em Budapeste em 23 de Novembro de 2001, no Protocolo Adicional à Convenção sobre o Cibercrime e na Decisão Quadro da União Europeia n.º 2005/222/JAI.

Neste Título criminaliza-se a divulgação de pornografia infantil através de sistema ou rede informática, em respeito ao Protocolo Facultativo à Declaração Universal dos Direitos da Criança das Nações Unidas relativo à venda de crianças, prostituição infantil e pornografia infantil. Matéria que aliás é contemplada no Anteprojecto de Código Penal.

Estando o mesmo subdividido em quatro capítulos, a saber: disposições gerais, dos crimes ligados à informática, penas e disposições finais.

Luanda, 11 de Abril de 2007



Título I

Comércio Electrónico

Capítulo I

Objecto e âmbito

Artigo 1.º

Objecto

O objecto do presente título consiste na regulação do regime jurídico dos prestadores de serviços da sociedade de informação e da contratação por via electrónica, no que concerne às obrigações dos prestadores de serviços incluindo aqueles que actuam como intermediários na transacção de conteúdos pelas redes de telecomunicações, as comunicações comerciais por via electrónica, a informação prévia e posterior à celebração de contratos electrónicos, as condições sobre a sua validade e eficácia e o regime sancionatório aplicável aos prestadores de serviços da sociedade de informação.

Artigo 2.º

Âmbito

1. Estão fora do âmbito do presente diploma:

- a) A matéria fiscal;
- b) A disciplina da concorrência;
- c) O regime do tratamento de dados pessoais e da protecção da privacidade;
- d) O patrocínio judiciário;
- e) Os jogos de fortuna, incluindo lotarias e apostas, em que é feita uma aposta em dinheiro;
- f) A actividade notarial ou equiparadas, enquanto caracterizadas pela fé pública ou por outras manifestações de poderes públicos;



- g) A protecção da saúde e da segurança pública, incluindo a salvaguarda da defesa nacional;
- h) Normas aplicáveis à protecção do consumidor.

Capítulo II

Prestadores de serviços da sociedade da informação

Artigo 3.º

Princípio da liberdade de exercício

1. Entende-se por «**serviço da sociedade da informação**» qualquer serviço prestado à distância por via electrónica, mediante remuneração ou pelo menos no âmbito de uma actividade económica na sequência de pedido individual do destinatário.
2. Não constituem serviços de radiodifusão os serviços prestados através de radiodifusão sonora ou televisiva.
3. A actividade de prestador de serviços da sociedade da informação não depende de autorização prévia, mas depende de registo junto do Órgão do Governo Responsável pela Política de Telecomunicações.
4. Exceptua-se o disposto no domínio das telecomunicações, bem como todo o regime de autorização que não vise especial e exclusivamente os serviços da sociedade da informação.
5. O disposto no presente diploma não exclui a aplicação da legislação vigente que com ele seja compatível, nomeadamente no que respeita ao regime dos contratos celebrados à distância e não prejudica o nível de protecção dos consumidores, incluindo investidores, resultante da restante legislação nacional.



Artigo 4.º

Prestadores de serviços estabelecidos na República de Angola

1. Os prestadores de serviços da sociedade da informação estabelecidos na República de Angola ficam integralmente sujeitos à lei angolana relativa à actividade que exercem.
2. Um prestador de serviços que exerça uma actividade económica no país mediante um estabelecimento efectivo considera-se estabelecido na República de Angola seja qual for a localização da sua sede, não configurando a mera disponibilidade de meios técnicos adequados à prestação do serviço, só por si, um estabelecimento efectivo.
3. O prestador estabelecido em vários locais considera-se estabelecido, para efeitos do n.º 1, no local em que tenha o centro das suas actividades relacionadas com o serviço da sociedade da informação.
4. Os prestadores intermediários de serviços em rede que pretendam exercer estavelmente a actividade na República de Angola devem previamente proceder à inscrição junto da entidade de supervisão central.
5. Os prestadores intermediários de serviços em rede são os que prestam serviços técnicos para o acesso, disponibilização e utilização de informações ou serviços em linha independentes da geração da própria informação ou serviço.

Artigo 5.º

Serviços de Origem Estrangeira

Os serviços de origem estrangeira estão sujeitos à aplicação geral da lei angolana.



Artigo 6.º

Exclusões

Estão fora do âmbito de aplicação do n.º 1 do artigo 4.º:

- a) A propriedade intelectual, incluindo a protecção das bases de dados e das topografias dos produtos semicondutores;
- b) A actividade seguradora, quanto a seguros obrigatórios, alcance e condições da autorização da entidade seguradora e empresas em dificuldades ou em situação irregular;
- c) A matéria disciplinada por legislação escolhida pelas partes no uso da autonomia privada;
- d) Os contratos celebrados com consumidores, no que respeita às obrigações deles emergentes;
- e) A validade dos contratos em função da observância de requisitos legais de forma, em contratos relativos a direitos reais sobre imóveis;
- f) A permissibilidade do envio de mensagens publicitárias não solicitadas por correio electrónico.

Artigo 7.º

Providências restritivas

1. Os tribunais e outras entidades competentes, nomeadamente as entidades de supervisão, podem restringir a circulação de um determinado serviço da sociedade da informação proveniente de outro Estado Estrangeiro se lesar ou ameaçar gravemente:

- a) A dignidade humana ou a ordem pública, incluindo a protecção de menores e a repressão do incitamento ao ódio fundado na raça, no sexo, na religião ou na nacionalidade, nomeadamente por razões de prevenção ou repressão de crimes ou de ilícitos de mera ordenação social;



- b) A saúde pública;
- c) A segurança pública, nomeadamente na vertente da segurança e defesa nacionais;
- d) Os consumidores, incluindo os investidores.

2. As providências tomadas devem ser proporcionais aos objectivos a tutelar.

3. O disposto no número anterior não prejudica a realização de diligências judiciais, incluindo a instrução e demais actos praticados no âmbito de uma investigação criminal ou de um ilícito de mera ordenação social.

Artigo 8.º

Disponibilização permanente de informações

1. Os prestadores de serviços devem disponibilizar permanentemente em linha, em condições que permitam um acesso fácil, gratuito e directo, elementos completos de identificação que incluam, nomeadamente:

- a) Nome ou denominação social;
- b) Endereço geográfico em que se encontra estabelecido e endereço electrónico, em termos de permitir uma comunicação directa;
- c) Inscrições do prestador em registos públicos e respectivos números de registo;
- d) Número de identificação fiscal.

2. Se o prestador exercer uma actividade sujeita a um regime de autorização prévia, deve disponibilizar a informação relativa à entidade que a concedeu.

3. Se o prestador exercer uma profissão regulamentada deve também indicar o título profissional e o Estado em que foi concedido, a entidade profissional em que se encontra inscrito, bem como referenciar as regras profissionais que disciplinam o acesso e o exercício dessa profissão.

4. Se os serviços prestados implicarem custos para os destinatários além dos custos dos serviços de telecomunicações, incluindo ónus fiscais ou despesas de entrega, estes devem ser objecto de informação clara anterior à utilização dos serviços.



Capítulo III

Responsabilidade dos prestadores de serviços em rede

Artigo 9.º

Princípio da equiparação

A responsabilidade dos prestadores de serviços em rede está sujeita ao regime comum, nomeadamente em caso de associação de conteúdos, com as especificações constantes dos artigos seguintes.

Artigo 10.º

Ausência de um dever geral de vigilância dos prestadores intermediários de serviços

Os prestadores intermediários de serviços em rede não estão sujeitos a uma obrigação geral de vigilância sobre as informações que transmitem ou armazenam ou de investigação de eventuais ilícitos praticados no seu âmbito.

Artigo 11.º

Deveres comuns dos prestadores intermediários dos serviços

Cabe aos prestadores intermediários de serviços a obrigação para com as entidades competentes:

- a) De informar de imediato quando tiverem conhecimento de actividades ilícitas que se desenvolvam por via dos serviços que prestam;
- b) De satisfazer os pedidos de identificar os destinatários dos serviços com quem tenham acordos de armazenagem;
- c) De cumprir prontamente as determinações destinadas a prevenir ou pôr termo a uma infracção, nomeadamente no sentido de remover ou impossibilitar o acesso a uma informação;
- d) De fornecer listas de titulares de sítios que alberguem, quando lhes for pedido.



Artigo 12.º

Responsabilidade dos operadores de redes e provedores de acessos

1. O prestador intermediário de serviços que prossiga apenas a actividade de transmissão de informações em rede, ou de facultar o acesso a uma rede de comunicações, sem estar na origem da transmissão nem ter intervenção no conteúdo das mensagens transmitidas nem na selecção destas ou dos destinatários, é isento de toda a responsabilidade pelas informações transmitidas.
2. A irresponsabilidade mantém-se ainda que o prestador realize a armazenagem meramente tecnológica das informações no decurso do processo de transmissão, exclusivamente para as finalidades de transmissão e durante o tempo necessário para esta.

Artigo 13.º

Responsabilidade dos prestadores de serviços que realizam cópia temporal dos dados solicitados pelos usuários

1. O prestador intermediário de serviços de transmissão de comunicações em rede que não tenha intervenção no conteúdo das mensagens transmitidas nem na selecção destas ou dos destinatários e respeite as condições de acesso à informação é isento de toda a responsabilidade pela armazenagem temporária e automática, exclusivamente para tornar mais eficaz e económica a transmissão posterior a nova solicitação de destinatários do serviço.
2. Passa, porém, a aplicar-se o regime comum de responsabilidade se o prestador não proceder segundo as regras usuais do sector:
 - a) Na actualização da informação;
 - b) No uso da tecnologia, aproveitando-a para obter dados sobre a utilização da informação.



3. As regras comuns passam também a ser aplicáveis se chegar ao conhecimento do prestador que a informação foi retirada da fonte originária ou o acesso tornado impossível ou ainda que um tribunal ou entidade administrativa com competência sobre o prestador que está na origem da informação ordenou essa remoção ou impossibilidade de acesso com exequibilidade imediata e o prestador não a retirar ou impossibilitar imediatamente o acesso.

Artigo 14.º

Responsabilidade dos prestadores de serviços de alojamento ou armazenagem de dados

1. O prestador intermediário do serviço de armazenagem em servidor só é responsável, nos termos comuns, pela informação que armazena se tiver conhecimento de actividade ou informação cuja ilicitude for manifesta e não retirar ou impossibilitar logo o acesso a essa informação.
2. Há responsabilidade civil sempre que, perante as circunstâncias que conhece, o prestador do serviço tenha ou deva ter consciência do carácter ilícito da informação.
3. Aplicam-se as regras comuns de responsabilidade sempre que o destinatário do serviço actuar subordinado ao prestador ou for por ele controlado.

Artigo 15.º

Responsabilidade dos prestadores intermediários de serviços de associação de conteúdos

Os prestadores intermediários de serviços de associação de conteúdos em rede, por meio de instrumentos de busca, hiperconexões ou processos análogos que permitam o acesso a conteúdos ilícitos estão sujeitos a regime de responsabilidade correspondente ao estabelecido no artigo anterior.



Artigo 16.º

Solução provisória de litígios

1. Nos casos contemplados nos artigos 14.º e 15.º, o prestador intermediário de serviços, se a ilicitude não for manifesta, não é obrigado a remover o conteúdo contestado ou a impossibilitar o acesso à informação só pelo facto de um interessado arguir uma violação.
2. Nos casos previstos no número anterior, qualquer interessado pode recorrer à entidade de supervisão respectiva, que deve dar uma solução provisória em quarenta e oito horas e logo a comunica electronicamente aos intervenientes.
3. Quem tiver interesse jurídico na manutenção daquele conteúdo em linha pode nos mesmos termos recorrer à entidade de supervisão contra uma decisão do prestador de remover ou impossibilitar o acesso a esse conteúdo, para obter a solução provisória do litígio.
4. O procedimento perante a entidade de supervisão será especialmente regulamentado.
5. A entidade de supervisão pode a qualquer tempo alterar a composição provisória do litígio estabelecida.
6. Qualquer que venha a ser a decisão, nenhuma responsabilidade recai sobre a entidade de supervisão e tão-pouco recai sobre o prestador intermediário de serviços por ter ou não retirado o conteúdo ou impossibilitado o acesso a mera solicitação, quando não for manifesto se há ou não ilicitude.
7. A solução definitiva do litígio é realizada nos termos e pelas vias comuns.
8. O recurso a estes meios não prejudica a utilização pelos interessados, mesmo simultânea, dos meios judiciais comuns.



Artigo 17.º

Relação com o direito à informação

1. A associação de conteúdos não é considerada irregular unicamente por haver conteúdos ilícitos no sítio de destino, ainda que o prestador tenha consciência do facto.

2. A remissão é lícita se for realizada com objectividade e distanciamento, representando o exercício do direito à informação, sendo, pelo contrário, ilícita se representar uma maneira de tomar como próprio o conteúdo ilícito para que se remete.

3. A avaliação é realizada perante as circunstâncias do caso, nomeadamente:
 - a) A confusão eventual dos conteúdos do sítio de origem com os de destino;
 - b) O carácter automatizado ou intencional da remissão;
 - c) A área do sítio de destino para onde a remissão é efectuada.

Capítulo IV

Comunicações publicitárias em rede e marketing directo

Artigo 18.º

Âmbito

1. Não constituem comunicação publicitária em rede:
 - a) Mensagens que se limitem a identificar ou permitir o acesso a um operador económico ou identifiquem objectivamente bens, serviços ou a imagem de um operador, em colectâneas ou listas, particularmente quando não tiverem implicações financeiras, embora se integrem em serviços da sociedade da informação;
 - b) Mensagens destinadas a promover ideias, princípios, iniciativas ou instituições.

2. A comunicação publicitária pode ter somente por fim promover a imagem de um operador comercial, industrial, artesanal ou integrante de uma profissão regulamentada.



Artigo 19.º

Identificação e informação

Nas comunicações publicitárias prestadas à distância, por via electrónica, devem ser claramente identificados de modo a serem apreendidos com facilidade por um destinatário comum:

- a) A natureza publicitária, logo que a mensagem seja apresentada no terminal e de forma ostensiva;
- b) O anunciante;
- c) As ofertas promocionais, como descontos, prémios ou brindes, e os concursos ou jogos promocionais, bem como os condicionalismos a que ficam submetidos.

Artigo 20.º

Comunicações não solicitadas

1. O envio de mensagens para fins de marketing directo, cuja recepção seja independente de intervenção do destinatário, nomeadamente por via de aparelhos de chamada automática, aparelhos de telecópia ou por correio electrónico, carece de consentimento prévio do destinatário.
2. Exceptuam-se as mensagens enviadas a pessoas colectivas, ficando, no entanto, aberto aos destinatários o recurso ao sistema de opção negativa.
3. É também permitido ao fornecedor de um produto ou serviço, no que respeita aos mesmos ou a produtos ou serviços análogos, enviar publicidade não solicitada aos clientes com quem celebrou anteriormente transacções, se ao cliente 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.
4. Nos casos previstos nos números anteriores, o destinatário deve ter acesso a meios que lhe permitam a qualquer momento recusar, sem ónus e independentemente de justa causa, o envio dessa publicidade para futuro.



5. É proibido o envio de correio electrónico para fins de marketing directo, ocultando ou dissimulando a identidade da pessoa em nome de quem é efectuada a comunicação.
6. Cada comunicação não solicitada deve indicar um endereço e um meio técnico electrónico, de fácil identificação e utilização, que permita ao destinatário do serviço recusar futuras comunicações.
7. Às entidades que promovam o envio de comunicações publicitárias não solicitadas cuja recepção seja independente da intervenção do destinatário cabe manter, por si ou por organismos que as representem, uma lista actualizada de pessoas que manifestaram o desejo de não receber aquele tipo de comunicações.
8. É proibido o envio de comunicações publicitárias por via electrónica às pessoas constantes das listas prescritas no número anterior.

Artigo 21.º

Profissões regulamentadas

1. As comunicações publicitárias à distância por via electrónica em profissões regulamentadas são permitidas mediante o estrito cumprimento das regras deontológicas de cada profissão, nomeadamente as relativas à independência e honra e ao sigilo profissionais, bem como à lealdade para com o público e dos membros da profissão entre si.
2. Entende-se por profissão regulamentada a actividade profissional ou o conjunto das actividades profissionais cujo acesso ou exercício esteja subordinado à posse de um diploma, certificado ou atestado de competência emitido pela autoridade competente ou cujo exercício seja condicionado a um título profissional reservado a quem satisfaça certas condições de qualificação.



Capítulo V

Contratação electrónica

Artigo 22.º

Âmbito

As disposições deste capítulo são aplicáveis a todo o tipo de contratos celebrados por via electrónica ou informática, sejam ou não qualificáveis como comerciais.

Artigo 23.º

Liberdade de celebração

1. É livre a celebração de contratos por via electrónica, sem que a validade ou eficácia destes seja prejudicada pela utilização deste meio.
2. São excluídos do princípio da admissibilidade os negócios jurídicos:
 - a) Familiares e sucessórios;
 - b) Que exijam a intervenção de tribunais, entes públicos ou outros entes que exerçam poderes públicos, nomeadamente quando aquela intervenção condicione a produção de efeitos em relação a terceiros e ainda os negócios legalmente sujeitos a reconhecimento ou autenticação notariais;
 - c) Reais imobiliários, com excepção do arrendamento;
 - d) De caução e de garantia, quando não se integrem na actividade profissional de quem as presta.
3. Só tem de aceitar a via electrónica para a celebração de um contrato quem se tiver vinculado a proceder dessa forma.
4. São proibidas cláusulas contratuais gerais que imponham a celebração por via electrónica dos contratos com consumidores.



Artigo 24.º

Forma

1. As declarações emitidas por via electrónica satisfazem a exigência legal de forma escrita quando contidas em suporte que ofereça as mesmas garantias de fidedignidade, inteligibilidade e conservação.
2. O documento electrónico vale como documento assinado quando satisfizer os requisitos sobre assinatura electrónica e certificação constantes do Título II da presente lei.

Artigo 25.º

Dispositivos de identificação e correcção de erros

O prestador de serviços em rede que celebre contratos por via electrónica deve disponibilizar aos destinatários dos serviços, salvo acordo em contrário das partes que não sejam consumidores, meios técnicos eficazes que lhes permitam identificar e corrigir erros de introdução, antes de formular uma ordem de encomenda.

Artigo 26.º

Informações prévias

1. O prestador de serviços em rede que celebre contratos em linha deve facultar aos destinatários, antes de ser dada a ordem de encomenda, informação mínima inequívoca que inclua:
 - a) O processo de celebração do contrato;
 - b) O arquivamento ou não do contrato pelo prestador de serviço e a acessibilidade àquele pelo destinatário;
 - c) A língua ou línguas em que o contrato pode ser celebrado;
 - d) Os meios técnicos que o prestador disponibiliza para poderem ser identificados e corrigidos erros de introdução que possam estar contidos na ordem de encomenda;
 - e) Os termos contratuais e as cláusulas gerais do contrato a celebrar;



- f) Os códigos de conduta de que seja subscritor e a forma de os consultar electronicamente.

2. O disposto no número anterior é derrogável por acordo em contrário das partes que não sejam consumidores.

Artigo 27.º

Informação posterior à celebração do contrato

1. Logo que receba uma ordem de encomenda por via exclusivamente electrónica, o prestador de serviços deve acusar a recepção igualmente por meios electrónicos, salvo acordo em contrário com a parte que não seja consumidora.
2. É dispensado o aviso de recepção da encomenda nos casos em que há a imediata prestação em linha do produto ou serviço.
3. O aviso de recepção deve conter a identificação fundamental do contrato a que se refere.
4. O prestador satisfaz o dever de acusar a recepção se enviar a comunicação para o endereço electrónico que foi indicado ou utilizado pelo destinatário do serviço.
5. A encomenda torna-se definitiva com a confirmação do destinatário, dada na sequência do aviso de recepção, reiterando a ordem emitida.

Artigo 28.º

Contratos celebrados por meio de comunicação individual

Os artigos 25.º a 27.º não são aplicáveis aos contratos celebrados exclusivamente por correio electrónico ou outro meio de comunicação individual equivalente.



Artigo 29.º

Apresentação dos termos contratuais e cláusulas gerais

1. Os termos contratuais e as cláusulas gerais, bem como o aviso de recepção, devem ser sempre comunicados de maneira que permita ao destinatário armazená-los e reproduzi-los.
2. A ordem de encomenda, o aviso de recepção e a confirmação da encomenda consideram-se recebidos logo que os destinatários tenham a possibilidade de aceder a eles.

Artigo 30.º

Proposta contratual e convite a contratar

1. A oferta de produtos ou serviços em linha representa uma proposta contratual quando contiver todos os elementos necessários para que o contrato fique concluído com a simples aceitação do destinatário, representando, caso contrário, um convite a contratar.
2. O mero aviso de recepção da ordem de encomenda não tem significado para a determinação do momento da conclusão do contrato.

Artigo 31.º

Contratação sem intervenção humana

1. À contratação celebrada exclusivamente por meio de computadores, sem intervenção humana, é aplicável o regime comum, salvo quando este pressupuser uma actuação.
2. São aplicáveis as disposições sobre erro:
 - a) Na formação da vontade, se houver erro de programação;
 - b) Na declaração, se houver defeito de funcionamento da máquina;
 - c) Na transmissão, se a mensagem chegar deformada ao seu destino.



3. A outra parte não pode opor-se à impugnação por erro sempre que lhe fosse exigível que dele se apercebesse, nomeadamente pelo uso de dispositivos de detecção de erros de introdução.

Artigo 32.º

Solução de litígios por via electrónica

É permitido o funcionamento em rede de formas de solução extrajudicial de litígios entre prestadores e destinatários de serviços da sociedade da informação, com observância das disposições concernentes à validade e eficácia dos documentos referidas no presente capítulo.

Capítulo VI

Entidades de supervisão e regime sancionatório

Artigo 33.º

Entidade de supervisão central

1. É instituída uma entidade de supervisão central com atribuições em todos os domínios regulados pelo presente título, salvo nas matérias em que lei especial atribua competência sectorial a outra entidade.

2. As funções de entidade de supervisão central serão exercidas pelo Órgão do Governo responsável pela Política de Telecomunicações.

Artigo 34.º

Atribuições e competência

1. As entidades de supervisão funcionam como organismos de referência para os contactos que se estabeleçam no seu domínio, fornecendo, quando requeridas, informações aos destinatários, aos prestadores de serviços e ao público em geral.

2. Cabe às entidades de supervisão, além das atribuições gerais já assinaladas e das que lhes forem especificamente atribuídas:



- a) Adoptar as providências restritivas previstas no artigo 7.º;
- b) Elaborar regulamentos e dar instruções sobre práticas a ser seguidas para cumprimento do disposto no presente diploma;
- c) Fiscalizar o cumprimento do preceituado sobre o comércio electrónico;
- d) Instaurar e instruir processos contra-ordenacionais e, bem assim, aplicar as sanções previstas;
- e) Determinar a suspensão da actividade dos prestadores de serviços em face de graves irregularidades e por razões de urgência.

3. A entidade de supervisão central tem competência em todas as matérias que a lei atribua a um órgão administrativo sem mais especificação e nas que lhe forem particularmente cometidas.

4. Cabe designadamente à entidade de supervisão central, além das atribuições gerais já assinaladas, quando não couberem a outro órgão:

- a) Publicitar em rede os códigos de conduta mais significativos de que tenha conhecimento;
- b) Publicitar outras informações, nomeadamente decisões judiciais neste domínio;
- c) Em geral, desempenhar a função de entidade permanente de contacto com os outros Estados.

Artigo 35.º

Contra-ordenação

1. Constitui contra-ordenação sancionável com coima de Kz 280.000,00 a Kz 5.600.000,00 a prática dos seguintes actos pelos prestadores de serviços:

- a) A não disponibilização ou a prestação de informação aos destinatários regulada nos artigos 8.º, 11.º, 19.º, 20.º, n.º 6, e 26.º, n.º 1, do presente diploma;
- b) O envio de comunicações não solicitadas, com inobservância dos requisitos legais previstos no artigo 20.º;



- c) A não disponibilização aos destinatários, quando devido, de dispositivos de identificação e correcção de erros de introdução, tal como previsto no artigo 25.º;
- d) A omissão de pronto envio do aviso de recepção da ordem de encomenda previsto no artigo 27.º;
- e) A não comunicação dos termos contratuais, cláusulas gerais e avisos de recepção previstos no artigo 29.º, de modo que permita aos destinatários armazená-los e reproduzi-los;
- f) A não prestação de informações solicitadas pela entidade de supervisão.

2. Constitui contra-ordenação sancionável com coima de Kz 560.000,00 a Kz 11.200.000,00 a prática dos seguintes actos pelos prestadores de serviços:

- a) A desobediência à determinação da entidade de supervisão ou de outra entidade competente de identificar os destinatários dos serviços com quem tenham acordos de transmissão ou de armazenagem, tal como previsto na alínea b) do artigo 11.º;
- b) O não cumprimento de determinação do tribunal ou da autoridade competente de prevenir ou pôr termo a uma infracção nos termos da alínea c) do artigo 11.º;
- c) A omissão de informação à autoridade competente sobre actividades ilícitas de que tenham conhecimento, praticadas por via dos serviços que prestam, tal como previsto na alínea a) do artigo 11.º;
- d) A não remoção ou impedimento do acesso a informação que armazenem e cuja ilicitude manifesta seja do seu conhecimento, tal como previsto nos artigos 14.º e 15.º;
- e) A não remoção ou impedimento do acesso a informação que armazenem, se, nos termos do artigo 13.º, n.º 3, tiverem conhecimento que foi retirada da fonte, ou o acesso tornado impossível, ou ainda que um tribunal ou autoridade administrativa da origem ordenou essa remoção ou impossibilidade de acesso para ter exequibilidade imediata;
- f) A prática com reincidência das infracções previstas no n.º 1.



3. Constitui contra-ordenação sancionável com coima de Kz 280.000,00 a Kz 11.200.000,00 a prestação de serviços de associação de conteúdos, nas condições da alínea e) do n.º 2, quando os prestadores de serviços não impossibilitem a localização ou o acesso a informação ilícita.
4. A negligência é sancionável nos limites da coima aplicável às infracções previstas no n.º 1.
5. A prática da infracção por pessoa colectiva agrava em um terço os limites máximo e mínimo da coima.

Artigo 36.º

Sanções acessórias

1. Às contra-ordenações acima previstas pode ser aplicada a sanção acessória de perda a favor do Estado dos bens usados para a prática das infracções.
2. Em função da gravidade da infracção, da culpa do agente ou da prática reincidente das infracções, pode ser aplicada, simultaneamente com as coimas previstas no n.º 2 do artigo anterior, a sanção acessória de interdição do exercício da actividade pelo período máximo de seis anos e, tratando-se de pessoas singulares, da inibição do exercício de cargos sociais em empresas prestadoras de serviços da sociedade da informação durante o mesmo período.
3. A aplicação de medidas acessórias de interdição do exercício da actividade e, tratando-se de pessoas singulares, da inibição do exercício de cargos sociais em empresas prestadoras de serviços da sociedade da informação por prazo superior a dois anos será obrigatoriamente decidida judicialmente por iniciativa oficiosa da própria entidade de supervisão.
4. Pode dar-se adequada publicidade à punição por contra-ordenação, bem como às sanções acessórias aplicadas nos termos do presente diploma.



Artigo 37.º

Providências provisórias

1. A entidade de supervisão a quem caiba a aplicação da coima pode determinar, desde que se revelem imediatamente necessárias, as seguintes providências provisórias:

- a) A suspensão da actividade e o encerramento do estabelecimento que é suporte daqueles serviços da sociedade da informação, enquanto decorre o procedimento e até à decisão definitiva;
- b) A apreensão de bens que sejam veículo da prática da infracção.

2. Estas providências podem ser determinadas, modificadas ou levantadas em qualquer momento pela própria entidade de supervisão, por sua iniciativa ou a requerimento dos interessados e a sua legalidade pode ser impugnada em juízo.

Artigo 38.º

Destino das coimas

O montante das coimas cobradas reverte para o Estado e para a entidade que as aplicou na proporção de 60 % e 40 %, respectivamente.

Artigo 39.º

Regras aplicáveis

1. O regime sancionatório estabelecido não prejudica os regimes sancionatórios especiais vigentes.
2. A entidade competente para a instauração, instrução e aplicação das sanções é a entidade de supervisão central ou as sectoriais, consoante a natureza das matérias.
3. É aplicável subsidiariamente o regime geral das contra-ordenações.



Capítulo VII

Disposições finais

Artigo 40.º

Códigos de conduta

1. As entidades de supervisão estimularão a criação de códigos de conduta pelos interessados e a sua difusão por estes por via electrónica.
2. Será incentivada a participação das associações e organismos que têm a seu cargo os interesses dos consumidores na formulação e aplicação de códigos de conduta, sempre que estiverem em causa os interesses destes. Quando houver que considerar necessidades específicas de associações representativas de deficientes visuais ou outros, estas deverão ser consultadas.
3. Os códigos de conduta devem ser publicitados em rede pelas próprias entidades de supervisão.

Artigo 41.º

Impugnação

As entidades de supervisão e o Ministério Público têm legitimidade para impugnar em juízo os códigos de conduta aprovados em domínio abrangido por este diploma que extravasem das finalidades da entidade que os emitiu ou tenham conteúdo contrário a princípios gerais ou regras vigentes.



Título II

Documentos Electrónicos e Assinatura Digital

Capítulo I

Documentos e actos jurídicos electrónicos

Artigo 42.º

Objecto

O presente diploma regula a validade, eficácia e valor probatório dos documentos electrónicos, a assinatura electrónica e a actividade de certificação de entidades certificadoras estabelecidas na República de Angola.

Artigo 43.º

Definições

Para os fins do presente título, entende-se por:

- a) **Documento electrónico:** documento elaborado mediante processamento electrónico de dados;
- b) **Assinatura electrónica:** resultado de um processamento electrónico de dados susceptível de constituir objecto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento electrónico;
- c) **Assinatura electrónica avançada:** assinatura electrónica que preenche os seguintes requisitos:
 - i. Identifica de forma unívoca o titular como autor do documento;
 - ii. A sua aposição ao documento depende apenas da vontade do titular;
 - iii. É criada com meios que o titular pode manter sob seu controlo exclusivo;
 - iv. A sua conexão com o documento permite detectar toda e qualquer alteração superveniente do conteúdo deste;



- d) **Assinatura digital:** modalidade de assinatura electrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento electrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento electrónico foi alterado depois de aposta a assinatura;
- e) **Chave privada:** elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento electrónico, ou se decifra um documento electrónico previamente cifrado com a correspondente chave pública;
- f) **Chave pública:** elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento electrónico pelo titular do par de chaves assimétricas, ou se cifra um documento electrónico a transmitir ao titular do mesmo par de chaves;
- g) **Assinatura electrónica qualificada:** assinatura digital ou outra modalidade de assinatura electrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura;
- h) **Dados de criação de assinatura:** conjunto único de dados, como chaves privadas, utilizado pelo titular para a criação de uma assinatura electrónica;
- i) **Dispositivo de criação de assinatura:** suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura;
- j) **Dispositivo seguro de criação de assinatura:** dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados, que:
 - i. Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada;



- ii. Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis;
 - iii. Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros;
 - iv. Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura;
-
- l) **Dados de verificação de assinatura:** conjunto de dados, como chaves públicas, utilizado para verificar uma assinatura electrónica;
 - m) **Credenciação:** acto pelo qual é reconhecido a uma entidade que o solicite e que exerça a actividade de entidade certificadora o preenchimento dos requisitos definidos no presente diploma para os efeitos nele previstos;
 - n) **Entidade certificadora:** entidade ou pessoa singular ou colectiva que cria ou fornece meios para a criação e verificação das assinaturas, emite os certificados, assegura a respectiva publicidade e presta outros serviços relativos a assinaturas electrónicas;
 - o) **Certificado:** documento electrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular;
 - p) **Certificado qualificado:** certificado que contém os elementos referidos no artigo 69.º;
 - q) **Titular:** pessoa singular ou colectiva identificada num certificado como a detentora de um dispositivo de criação de assinatura;
 - r) **Produto de assinatura electrónica:** suporte lógico, dispositivo de equipamento ou seus componentes específicos, destinados a ser utilizados na prestação de serviços de assinatura electrónica qualificada por uma entidade certificadora ou na criação e verificação de assinatura electrónica qualificada;
 - s) **Validação cronológica:** declaração de entidade certificadora que atesta a data e hora da criação, expedição ou recepção de um documento electrónico;
 - t) **Endereço electrónico:** identificação de um equipamento informático adequado para receber e arquivar documentos electrónicos.



Artigo 44.º

Forma e força probatória

1. O documento electrónico satisfaz o requisito legal de forma escrita quando o seu conteúdo seja susceptível de representação como declaração escrita.
2. Quando lhe seja aposta uma assinatura electrónica qualificada, o documento electrónico com o conteúdo referido no número anterior tem a força probatória de documento particular assinado, nos termos do artigo 376.º do Código Civil.
3. Quando lhe seja aposta uma assinatura electrónica qualificada, o documento electrónico cujo conteúdo não seja susceptível de representação como declaração escrita tem a força probatória prevista no artigo 368.º do Código Civil e no 249.º do Código de Processo Penal.
4. O disposto nos números anteriores não obsta à utilização de outro meio de comprovação da autoria e integridade de documentos electrónicos, incluindo outras modalidades de assinatura electrónica, desde que tal meio seja adoptado pelas partes ao abrigo de válida convenção sobre prova ou seja aceite pela pessoa a quem for oposto o documento.

Artigo 45.º

Cópias de documentos

As cópias de documentos electrónicos, sobre idêntico ou diferente tipo de suporte, são válidas e eficazes nos termos gerais de direito e têm a força probatória atribuída às cópias fotográficas pelo n.º 2 do artigo 387.º do Código Civil e pelo artigo 249.º do Código de Processo Penal, se forem observados os requisitos aí previstos.

Artigo 46.º

Documentos electrónicos dos organismos públicos

1. Os organismos públicos podem emitir documentos electrónicos com assinatura electrónica qualificada aposta em conformidade com as normas do presente diploma.



2. Nas operações relativas à criação, emissão, arquivo, reprodução, cópia e transmissão de documentos electrónicos que formalizem actos administrativos através de sistemas informáticos, incluindo a sua transmissão por meios de telecomunicações, os dados relativos ao organismo interessado e à pessoa que tenha praticado cada acto administrativo devem ser indicados de forma a torná-los facilmente identificáveis e a comprovar a função ou cargo desempenhado pela pessoa signatária de cada documento.

Artigo 47.º

Comunicação de documentos electrónicos

1. O documento electrónico comunicado por um meio de telecomunicações considera-se enviado e recebido pelo destinatário se for transmitido para o endereço electrónico definido por acordo das partes e neste for recebido.

2. São oponíveis entre as partes e a terceiros a data e a hora da criação, da expedição ou da recepção de um documento electrónico que contenha uma validação cronológica emitida por uma entidade certificadora.

3. A comunicação do documento electrónico, ao qual seja aposta assinatura electrónica qualificada, por meio de telecomunicações que assegure a efectiva recepção equivale à remessa por via postal registada e, se a recepção for comprovada por mensagem de confirmação dirigida ao remetente pelo destinatário que revista idêntica forma, equivale à remessa por via postal registada com aviso de recepção.

4. Os dados e documentos comunicados por meio de telecomunicações consideram-se em poder do remetente até à recepção pelo destinatário.



5. Os operadores que assegurem a comunicação de documentos electrónicos por meio de telecomunicações não podem tomar conhecimento do seu conteúdo, nem duplicá-los por qualquer meio ou ceder a terceiros qualquer informação, ainda que resumida ou por extracto, sobre a existência ou sobre o conteúdo desses documentos, salvo quando se trate de informação que, pela sua natureza ou por indicação expressa do seu remetente, se destine a ser tornada pública.

Capítulo II

Assinaturas electrónicas qualificadas

Artigo 48.º

Assinatura electrónica qualificada

1. A aposição de uma assinatura electrónica qualificada a um documento electrónico equivale à assinatura autógrafa dos documentos com forma escrita sobre suporte de papel e cria a presunção de que:

- a) A pessoa que após a assinatura electrónica qualificada é o titular desta ou é representante, com poderes bastantes, da pessoa colectiva titular da assinatura electrónica qualificada;
- b) A assinatura electrónica qualificada foi aposta com a intenção de assinar o documento electrónico;
- c) O documento electrónico não sofreu alteração desde que lhe foi aposta a assinatura electrónica qualificada.

2. A assinatura electrónica qualificada deve referir-se inequivocamente a uma só pessoa singular ou colectiva e ao documento ao qual é aposta.

3. A aposição de assinatura electrónica qualificada substitui, para todos os efeitos legais, a aposição de selos, carimbos, marcas ou outros sinais identificadores do seu titular.



4. A aposição de assinatura electrónica qualificada que conste de certificado que esteja revogado, caduco ou suspenso na data da aposição ou não respeite as condições dele constantes equivale à falta de assinatura.

Artigo 49.º

Obtenção dos dados de assinatura e certificado

Quem pretenda utilizar uma assinatura electrónica qualificada deve, nos termos do n.º 1 do artigo 68.º, gerar ou obter os dados de criação e verificação de assinatura, bem como obter o respectivo certificado emitido por entidade certificadora nos termos deste diploma.

Capítulo III

Certificação

Secção I

Acesso à actividade de certificação

Artigo 50.º

Acesso à actividade de certificação

1. O exercício da actividade de entidade certificadora depende de autorização prévia do Órgão do Governo responsável pela Política de Informática.

2. A credenciação e o registo estão sujeitos ao pagamento de taxas em função dos custos associados às tarefas administrativas, técnicas, operacionais e de fiscalização correspondentes, nos termos a fixar por despacho do Ministério da Ciência e da Tecnologia, que constituem receita do Órgão do Governo responsável pela Política de Informática.



Artigo 51.º

Entidade competente para a credenciação

A credenciação de entidades certificadoras para efeitos do presente diploma compete ao Órgão do Governo responsável pela Política de Informática.

Artigo 52.º

Credenciação da entidade certificadora

1. É concedida a credenciação a entidades certificadoras de assinaturas electrónicas qualificadas, mediante pedido apresentado ao Órgão do Governo responsável pela Política de Informática, que satisfaçam os seguintes requisitos:

- a) Estejam dotadas de capital e meios financeiros adequados;
- b) Dêem garantias de absoluta integridade e independência no exercício da actividade de certificação e assinaturas electrónicas qualificadas;
- c) Disponham de recursos técnicos e humanos que satisfaçam os padrões de segurança e de eficácia que sejam previstos na regulamentação a que se refere o artigo 77.º;
- d) Mantenham contrato de seguro válido para cobertura adequada da responsabilidade civil emergente da actividade de certificação.

2. A credenciação é válida pelo período de três anos, podendo ser objecto de renovação por períodos de igual duração.

Artigo 53.º

Pedido de credenciação

1. O pedido de credenciação de entidade certificadora deve ser instruído com os seguintes documentos:

- a) Estatutos da pessoa colectiva e, tratando-se de sociedade, contrato de sociedade ou, tratando-se de pessoa singular, a respectiva identificação e domicílio;



- b) Tratando-se de sociedade, relação de todos os sócios, com especificação das respectivas participações, bem como dos membros dos órgãos de administração e de fiscalização, e, tratando-se de sociedade anónima, relação de todos os accionistas com participações significativas, directas ou indirectas;
- c) Declarações subscritas por todas as pessoas singulares e colectivas referidas no n.º 1 do artigo 55.º de que não se encontram em nenhuma das situações indiciadoras de inidoneidade referidas no respectivo n.º 2;
- d) Prova do substrato patrimonial e dos meios financeiros disponíveis, e designadamente, tratando-se de sociedade, da realização integral do capital social;
- e) Descrição da organização interna e plano de segurança;
- f) Demonstração dos meios técnicos e humanos exigidos nos termos do diploma regulamentar a que se refere a alínea c) do n.º 1 do artigo 52.º, incluindo certificados de conformidade dos produtos de assinatura electrónica emitidos por organismo reconhecido de certificação acreditado pelo Órgão do Governo responsável pela Política de Informática;
- g) Designação do auditor de segurança;
- h) Programa geral da actividade prevista para os primeiros três anos;
- i) Descrição geral das actividades exercidas nos últimos três anos ou no tempo decorrido desde a constituição, se for inferior, e balanço e contas dos exercícios correspondentes;
- j) Comprovação de contrato de seguro válido para cobertura adequada da responsabilidade civil emergente da actividade de certificação.

2. Se à data do pedido a pessoa colectiva não estiver constituída, o pedido será instruído, em substituição do previsto na alínea a) do número anterior, com os seguintes documentos:

- a) Acta da reunião em que foi deliberada a constituição;
- b) Projecto de estatutos ou contrato de sociedade;
- c) Declaração de compromisso, subscrita por todos os fundadores, de que no acto de constituição, e como condição dela, estará integralmente realizado o substrato patrimonial exigido por lei.



3. As declarações previstas na alínea c) do n.º 1, poderão ser entregues em momento posterior ao pedido, nos termos e prazo que o Órgão do Governo responsável pela Política de Informática fixar.
4. Consideram-se como participações significativas, para os efeitos do presente diploma, as que igualem ou excedam 10% do capital da sociedade anónima.
5. O pedido de renovação de credenciação deve ser instruído com os seguintes documentos:
 - a) Programa geral da actividade prevista para os próximos três anos;
 - b) Descrição geral das actividades exercidas nos últimos três anos, balanço e contas dos exercícios correspondentes;
 - c) Declaração que todos os elementos referidos no n.º 1 deste artigo e nos n.ºs 2 e 3 do artigo 72.º não sofreram alteração desde a sua apresentação ao Órgão do Governo responsável pela Política de Informática.

Artigo 54.º

Requisitos patrimoniais

1. As entidades certificadoras privadas, que sejam pessoas colectivas, devem estar dotadas de capital social no valor mínimo de Kz 22.500.000,00 ou, não sendo pessoas colectivas, do substrato patrimonial equivalente.
2. O substrato patrimonial, e designadamente o capital social mínimo de sociedade, encontrar-se-á sempre integralmente realizado à data da credenciação, se a pessoa colectiva estiver já constituída, ou será sempre integralmente realizado com a constituição da pessoa colectiva, se esta ocorrer posteriormente.
3. As entidades certificadoras que sejam pessoas singulares devem ter e manter durante toda a sua actividade um património, livre de quaisquer ónus, de valor equivalente ao previsto no n.º 1.



Artigo 55.º

Requisitos de idoneidade

1. A pessoa singular e, no caso de pessoa colectiva, os membros dos órgãos de administração e fiscalização, os empregados, e representantes das entidades certificadoras com acesso aos actos e instrumentos de certificação, os sócios da sociedade e, tratando-se de sociedade anónima, os accionistas com participações significativas serão sempre pessoas de reconhecida idoneidade.

2. Entre outras circunstâncias atendíveis, considera-se indiciador de falta de idoneidade o facto de a pessoa ter sido:

- a) Condenada, no País ou no estrangeiro, por crime de furto, roubo, burla, burla informática e nas comunicações, extorsão, abuso de confiança, infidelidade, falsificação, falsas declarações, insolvência dolosa, insolvência negligente, favorecimento de credores, emissão de cheques sem provisão, abuso de cartão de garantia ou de crédito, apropriação ilegítima de bens do sector público ou cooperativo, administração danosa em unidade económica do sector público ou cooperativo, usura, suborno, corrupção, recepção não autorizada de depósitos ou outros fundos reembolsáveis, prática ilícita de actos ou operações inerentes à actividade seguradora ou dos fundos de pensões, branqueamento de capitais, abuso de informação, manipulação do mercado de valores mobiliários ou crime previsto na Lei das Sociedades Comerciais;
- b) Declarada, por sentença nacional ou estrangeira, falida ou insolvente ou julgada responsável por falência ou insolvência de empresa por ela dominada ou de cujos órgãos de administração ou fiscalização tenha sido membro;
- c) Sujeita a sanções, no País ou no estrangeiro, pela prática de infracções às normas legais ou regulamentares que regem as actividades de produção, autenticação, registo e conservação de documentos, e designadamente as do notariado, dos registos públicos, do funcionalismo judicial, das bibliotecas públicas, e da certificação de assinaturas electrónicas qualificadas.



3. A falta dos requisitos de idoneidade previstos no presente artigo constitui fundamento de recusa e de revogação da credenciação, nos termos da alínea c) do n.º 1 do artigo 58.º e da alínea f) do n.º 1 do artigo 60.º.

Artigo 56.º

Seguro obrigatório de responsabilidade civil

O Ministro da Ciência e da Tecnologia definirá, por portaria, as características do contrato de seguro de responsabilidade civil a que se refere a alínea d) do artigo 52.º

Artigo 57.º

Decisão

1. O Órgão do Governo responsável pela Política de Informática poderá solicitar dos requerentes informações complementares e proceder, por si ou por quem para o efeito designar, às averiguações, inquirições e inspecções que entenda necessárias para a apreciação do pedido.

2. A decisão sobre o pedido de credenciação ou sua renovação deve ser notificada aos interessados no prazo de três meses a contar da recepção do pedido ou, se for o caso, a contar da recepção das informações complementares solicitadas ou da conclusão das diligências que entenda necessárias, não podendo no entanto exceder o prazo de seis meses sobre a data da recepção daquele.

3. O Órgão do Governo responsável pela Política de Informática poderá incluir na credenciação condições adicionais desde que necessárias para assegurar o cumprimento das disposições legais e regulamentares aplicáveis ao exercício da actividade pela entidade certificadora.

4. A credenciação é inscrita no registo a que se refere o artigo 50.º e é publicada no Diário da República.



Artigo 58.º

Recusa de credenciação

1. A credenciação é recusada sempre que:

- a) O pedido não estiver instruído com todas as informações e documentos necessários;
- b) A instrução do pedido enfermar de inexactidões ou falsidades;
- c) O Órgão do Governo responsável pela Política de Informática não considerar demonstrado algum dos requisitos enumerados nos artigos 52.º e seguintes.

2. Se o pedido estiver deficientemente instruído, o Órgão do Governo responsável pela Política de Informática, antes de recusar a credenciação, notificará o requerente, dando-lhe prazo razoável para suprir a deficiência.

Artigo 59.º

Caducidade da credenciação

1. A credenciação caduca nos seguintes casos:

- a. Quando a actividade de certificação não seja iniciada no prazo de 12 meses após a recepção da notificação da credenciação;
- b. Quando, tratando-se de pessoa colectiva, esta seja dissolvida, sem prejuízo dos actos necessários à respectiva liquidação;
- c. Quando, tratando-se de pessoa singular, esta faleça ou seja declarada interdita ou inabilitada;
- d. Quando, findo o prazo de validade, a credenciação não tenha sido objecto de renovação.

2. A caducidade da credenciação é inscrita no registo a que se refere o artigo 50.º e é publicada no Diário da República.



Artigo 60.º

Revogação da credenciação

1. A credenciação é revogada, sem prejuízo de outras sanções aplicáveis nos termos da lei, quando se verifique alguma das seguintes situações:

- a) Se tiver sido obtida por meio de falsas declarações ou outros expedientes ilícitos;
- b) Se deixar de se verificar algum dos requisitos enumerados no artigo 52.º;
- c) Se a entidade cessar a actividade de certificação ou a reduzir para nível insignificante por período superior a 12 meses;
- d) Se ocorrerem irregularidades graves na administração, organização ou fiscalização interna da entidade;
- e) Se no exercício da actividade de certificação ou de outra actividade social forem praticados actos ilícitos que lesem ou ponham em perigo a confiança do público na certificação;
- f) Se supervenientemente se verificar alguma das circunstâncias de inidoneidade referidas no artigo 55.º em relação a qualquer das pessoas a que alude o seu n.º 1;
- g) Se os certificados do organismo de certificação referidos na alínea f) do n.º 1 do artigo 53.º tiverem sido revogados.

2. A revogação da credenciação compete ao Órgão do Governo responsável pela Política de Informática, em decisão fundamentada que será notificada à entidade no prazo de oito dias úteis.

3. A decisão de revogação é inscrita no registo a que se refere o artigo 50.º e publicada no Diário da República.

Artigo 61.º

Anomalias nos órgãos de administração e fiscalização

1. Se por qualquer motivo deixarem de estar preenchidos os requisitos legais e estatutários do normal funcionamento dos órgãos de administração ou fiscalização, o Órgão do Governo responsável pela Política de Informática fixará prazo para ser regularizada a situação.



2. Não sendo regularizada a situação no prazo fixado, será revogada a credenciação nos termos do artigo anterior.

Artigo 62.º

Comunicação de alterações

Devem ser comunicadas ao Órgão do Governo responsável pela Política de Informática, no prazo de 30 dias, as alterações das entidades certificadoras que emitem certificados qualificados relativas a:

- a) Firma ou denominação;
- b) Objecto;
- c) Local da sede, salvo se a mudança ocorrer dentro do mesmo concelho ou para concelho limítrofe;
- d) Substrato patrimonial ou património, desde que se trate de uma alteração significativa;
- e) Estrutura de administração e de fiscalização;
- f) Limitação dos poderes dos órgãos de administração e fiscalização;
- g) Cisão, fusão e dissolução.

Artigo 63.º

Registo de alterações

1. O registo das pessoas referidas no n.º 1 do artigo 55.º deve ser solicitado ao Órgão do Governo responsável pela Política de Informática no prazo de 15 dias após assumirem qualquer das qualidades nele referidas, mediante pedido da entidade certificadora ou dos interessados, juntamente com as provas de que se encontram preenchidos os requisitos definidos no mesmo artigo, e sob pena da credenciação ser revogada.



2. Poderão a entidade certificadora ou os interessados solicitar o registo provisório, antes da assunção por estes de qualquer das qualidades referidas no n.º 1 do artigo 55.º, devendo a conversão em definitivo ser requerida no prazo de 30 dias a contar da designação, sob pena de caducidade.
3. Em caso de recondução, será esta averbada no registo, a pedido da entidade certificadora ou dos interessados.
4. O registo é recusado em caso de inidoneidade, nos termos do artigo 55.º, e a recusa é comunicada aos interessados e à entidade certificadora, a qual deve tomar as medidas adequadas para que aqueles cessem imediatamente funções ou deixem de estar para com a pessoa colectiva na relação prevista no mesmo artigo, seguindo-se no aplicável o disposto no artigo 61.º
5. Sem prejuízo do que resulte de outras disposições legais aplicáveis, a falta de registo não determina por si só invalidade dos actos jurídicos praticados pela pessoa em causa no exercício das suas funções.

Secção II

Exercício da actividade

Artigo 64.º

Deveres da entidade certificadora que emite certificados qualificados

Compete à entidade certificadora que emite certificados qualificados:

- a) Estar dotada dos requisitos patrimoniais estabelecidos no artigo 54.º;
- b) Oferecer garantias de absoluta integridade e independência no exercício da actividade de certificação;
- c) Demonstrar a fiabilidade necessária para o exercício da actividade de certificação;
- d) Manter um contrato de seguro válido para a cobertura adequada da responsabilidade civil emergente da actividade de certificação, nos termos previstos no artigo 56.º;



- e) Dispor de recursos técnicos e humanos que satisfaçam os padrões de segurança e eficácia, nos termos do diploma regulamentar;
- f) Utilizar sistemas e produtos fiáveis protegidos contra qualquer modificação e que garantam a segurança técnica dos processos para os quais estejam previstos;
- g) Adoptar medidas adequadas para impedir a falsificação ou alteração dos dados constantes dos certificados e, nos casos em que a entidade certificadora gere dados de criação de assinaturas, garantir a sua confidencialidade durante o processo de criação;
- h) Utilizar sistemas fiáveis de conservação dos certificados, de forma a que:
 - i. Os certificados só possam ser consultados pelo público nos casos em que tenha sido obtido o consentimento do seu titular;
 - ii. Apenas as pessoas autorizadas possam inserir dados e alterações aos certificados;
 - iii. A autenticidade das informações possa ser verificada;
 - iv. Quaisquer alterações de carácter técnico susceptíveis de afectar os requisitos de segurança sejam imediatamente detectáveis;
- i) Verificar rigorosamente a identidade dos requerentes titulares dos certificados e, tratando-se de representantes de pessoas colectivas, os respectivos poderes de representação, bem como, quando aplicável, as qualidades específicas a que se refere a alínea i) do n.º 1 do artigo 69;
- j) Conservar os elementos que comprovem a verdadeira identidade dos requerentes titulares de certificados com pseudónimo;
- k) Informar os requerentes, por forma escrita, de modo completo e claro, sobre o processo de emissão de certificados qualificados e os termos e condições exactos de utilização do certificado qualificado, incluindo eventuais restrições à sua utilização;
- l) Cumprir as regras de segurança para tratamento de dados pessoais estabelecidas na legislação respectiva;
- m) Não armazenar ou copiar dados de criação de assinaturas do titular a quem a entidade certificadora tenha oferecido serviços de gestão de chaves;
- n) Assegurar o funcionamento de um serviço que:



- i. Permita a consulta, de forma célere e segura, do registo informático dos certificados emitidos, revogados, suspensos ou caducados;
 - ii. Garanta, de forma imediata e segura, a revogação, suspensão ou caducidade dos certificados;
-
- o) Proceder à publicação imediata da revogação ou suspensão dos certificados, nos casos previstos no presente diploma;
 - p) Assegurar que a data e hora da emissão, suspensão e revogação dos certificados possam ser determinadas através de validação cronológica;
 - q) Conservar os certificados que emitir, por um período não inferior a 20 anos.

Artigo 65.º

Protecção de dados

1. As entidades certificadoras só podem coligir dados pessoais necessários ao exercício das suas actividades e obtê-los directamente das pessoas interessadas na titularidade dos dados de criação e verificação de assinatura e respectivos certificados, ou de terceiros junto dos quais aquelas pessoas autorizem a sua colecta.
2. Os dados pessoais coligidos pela entidade certificadora não poderão ser utilizados para outra finalidade que não seja a de certificação, salvo se outro uso for consentido expressamente por lei ou pela pessoa interessada.
3. As entidades certificadoras e o Órgão do Governo responsável pela Política de Informática respeitarão as normas legais vigentes sobre a protecção, tratamento e circulação dos dados pessoais.
4. As entidades certificadoras comunicarão à autoridade judiciária, sempre que esta o ordenar nos termos legalmente previstos, os dados relativos à identidade dos titulares de certificados que sejam emitidos com pseudónimo, sempre com respeito pelo disposto no artigo 217.º do Código de Processo Penal.



Artigo 66.º

Responsabilidade civil

1. A entidade certificadora é civilmente responsável pelos danos sofridos pelos titulares dos certificados e por terceiros, em consequência do incumprimento dos deveres que lhe incumbem por força do presente diploma e da sua regulamentação, excepto se provar que não actuou de forma dolosa ou negligente.

2. São nulas as convenções de exoneração e limitação da responsabilidade prevista no n.º 1.

Artigo 67.º

Cessação da actividade

1. No caso de pretender cessar voluntariamente a sua actividade, a entidade certificadora que emite certificados qualificados deve comunicar essa intenção ao Órgão do Governo responsável pela Política de Informática e às pessoas a quem tenha emitido certificados que permaneçam em vigor, com a antecipação mínima de três meses, indicando também qual a entidade certificadora à qual é transmitida a sua documentação ou a revogação dos certificados no termo daquele prazo, devendo neste último caso, quando seja credenciada, colocar a sua documentação à guarda do Órgão do Governo responsável pela Política de Informática.

2. A entidade certificadora que emite certificados qualificados que se encontre em risco de decretação de falência, de processo de recuperação de empresa ou de cessação da actividade por qualquer outro motivo alheio à sua vontade deve informar imediatamente o Órgão do Governo responsável pela Política de Informática.

3. No caso previsto no número anterior, se a entidade certificadora vier a cessar a sua actividade, o Órgão do Governo responsável pela Política de Informática promoverá a transmissão da documentação daquela para outra entidade certificadora ou, se tal transmissão for impossível, a revogação dos certificados emitidos e a conservação dos elementos de tais certificados pelo prazo em que deveria fazê-lo a entidade certificadora.



4. A cessação da actividade de entidade certificadora que emite certificados qualificados é inscrita no registo a que se refere o artigo 50.º e publicada no Diário da República.

Secção III

Certificados

Artigo 68.º

Emissão dos certificados qualificados

1. A entidade certificadora emite, a pedido de uma pessoa singular ou colectiva interessada e a favor desta, os dados de criação e de verificação de assinatura ou, se tal for solicitado, coloca à disposição os meios técnicos necessários para que esta os crie, devendo sempre verificar, por meio legalmente idóneo e seguro, a identidade e, quando existam, os poderes de representação da requerente.
2. A entidade certificadora emite, a pedido do titular, uma ou mais vias do certificado e do certificado complementar.
3. A entidade certificadora deve tomar medidas adequadas para impedir a falsificação ou alteração dos dados constantes dos certificados e assegurar o cumprimento das normas legais e regulamentares aplicáveis recorrendo a pessoal devidamente habilitado.
4. A entidade certificadora fornece aos titulares dos certificados as informações necessárias para a utilização correcta e segura das assinaturas, nomeadamente as respeitantes:
 - a) Às obrigações do titular do certificado e da entidade certificadora;
 - b) Ao procedimento de aposição e verificação de assinatura;
 - c) À conveniência de os documentos aos quais foi aposta uma assinatura serem novamente assinados quando ocorrerem circunstâncias técnicas que o justifiquem.



5. A entidade certificadora organizará e manterá permanentemente actualizado um registo informático dos certificados emitidos, suspensos ou revogados, o qual estará acessível a qualquer pessoa para consulta, inclusivamente por meio de telecomunicações, e será protegido contra alterações não autorizadas.

Artigo 69.º

Conteúdo dos certificados qualificados

1. O certificado qualificado deve conter, pelo menos, as seguintes informações:

- a) Nome ou denominação do titular da assinatura e outros elementos necessários para uma identificação inequívoca e, quando existam poderes de representação, o nome do seu representante ou representantes habilitados, ou um pseudónimo do titular, claramente identificado como tal;
- b) Nome e assinatura electrónica avançada da entidade certificadora, bem como indicação do país onde se encontra estabelecida;
- c) Dados de verificação de assinatura correspondentes aos dados de criação de assinatura detidos pelo titular;
- d) Número de série do certificado;
- e) Início e termo de validade do certificado;
- f) Identificadores de algoritmos utilizados na verificação de assinaturas do titular e da entidade certificadora;
- g) Indicação de o uso do certificado ser ou não restrito a determinados tipos de utilização, bem como eventuais limites do valor das transacções para as quais o certificado é válido;
- h) Limitações convencionais da responsabilidade da entidade certificadora, sem prejuízo do disposto no n.º 2 do artigo 66.º;
- i) Eventual referência a uma qualidade específica do titular da assinatura, em função da utilização a que o certificado estiver destinado;
- j) Indicação de que é emitido como certificado qualificado.



2. A pedido do titular podem ser incluídas no certificado ou em certificado complementar informações relativas a poderes de representação conferidos ao titular por terceiro, à sua qualificação profissional ou a outros atributos, mediante fornecimento da respectiva prova, ou com a menção de se tratar de informações não confirmadas.

Artigo 70.º

Suspensão e revogação dos certificados qualificados

1. A entidade certificadora suspende o certificado:

- a) A pedido do titular, devidamente identificado para o efeito;
- b) Quando existam fundadas razões para crer que o certificado foi emitido com base em informações erróneas ou falsas, que as informações nele contidas deixaram de ser conformes com a realidade ou que a confidencialidade dos dados de criação de assinatura não está assegurada.

2. A suspensão com um dos fundamentos previstos na alínea b) do número anterior será sempre motivada e comunicada prontamente ao titular, bem como imediatamente inscrita no registo do certificado, podendo ser levantada quando se verifique que tal fundamento não corresponde à realidade.

3. A entidade certificadora revogará o certificado:

- a) A pedido do titular, devidamente identificado para o efeito;
- b) Quando, após suspensão do certificado, se confirme que o certificado foi emitido com base em informações erróneas ou falsas, que as informações nele contidas deixaram de ser conformes com a realidade, ou que a confidencialidade dos dados de criação de assinatura não está assegurada;
- c) Quando a entidade certificadora cesse as suas actividades sem ter transmitido a sua documentação a outra entidade certificadora;
- d) Quando o Órgão do Governo responsável pela Política de Informática ordene a revogação do certificado por motivo legalmente fundado;



- e) Quando tomar conhecimento do falecimento, interdição ou inabilitação da pessoa singular ou da extinção da pessoa colectiva.
4. A decisão de revogação do certificado com um dos fundamentos previstos nas alíneas b), c) e d) do n.º 3 será sempre fundamentada e comunicada ao titular, bem como imediatamente inscrita.
5. A suspensão e a revogação do certificado são oponíveis a terceiros a partir da inscrição no registo respectivo, salvo se for provado que o seu motivo já era do conhecimento do terceiro.
6. A entidade certificadora conservará as informações referentes aos certificados durante um prazo não inferior a 20 anos a contar da suspensão ou revogação de cada certificado e facultá-las-á a qualquer interessado.
7. A revogação ou suspensão do certificado indicará a data e hora a partir das quais produzem efeitos, não podendo essa data e hora ser anteriores àquela em que essa informação for divulgada publicamente.
8. A partir da suspensão ou revogação de um certificado ou do termo do seu prazo de validade é proibida a emissão de certificado referente aos mesmos dados de criação de assinatura pela mesma ou outra entidade certificadora.

Artigo 71.º

Obrigações do titular

1. O titular do certificado deve tomar todas as medidas de organização e técnica que sejam necessárias para evitar danos a terceiros e preservar a confidencialidade da informação transmitida.
2. Em caso de dúvida quanto à perda de confidencialidade dos dados de criação de assinatura, o titular deve pedir a suspensão do certificado e, se a perda for confirmada, a sua revogação.



3. A partir da suspensão ou revogação de um certificado ou do termo do seu prazo de validade é proibida ao titular a utilização dos respectivos dados de criação de assinatura para gerar uma assinatura electrónica.

4. Sempre que se verificarem motivos que justifiquem a revogação ou suspensão do certificado, deve o respectivo titular efectuar, com a necessária celeridade e diligência, o correspondente pedido de suspensão ou revogação à entidade certificadora.

Capítulo IV

Fiscalização

Artigo 72.º

Deveres de informação das entidades certificadoras

1. As entidades certificadoras fornecem ao Órgão do Governo responsável pela Política de Informática, de modo pronto e exaustivo, todas as informações que ele lhes solicite para fins de fiscalização da sua actividade e facultam-lhe para os mesmos fins a inspecção dos seus estabelecimentos e o exame local de documentos, objectos, equipamentos de hardware e software e procedimentos operacionais, no decorrer dos quais o Órgão do Governo responsável pela Política de Informática poderá fazer as cópias e registos que sejam necessários.

2. As entidades certificadoras credenciadas devem comunicar sempre ao Órgão do Governo responsável pela Política de Informática, no mais breve prazo possível, todas as alterações relevantes que sobrevenham nos requisitos e elementos referidos nos artigos 53.º e 54.º

3. Até ao último dia útil de cada semestre, as entidades certificadoras credenciadas devem enviar ao Órgão do Governo responsável pela Política de Informática uma versão actualizada das relações referidas na alínea b) do n.º 1 do artigo 53.º.



Artigo 73.º

Auditor de segurança

1. As entidades certificadoras que emitam certificados qualificados devem ser auditadas por um auditor de segurança que cumpra os requisitos especificados na regulamentação a que se refere o artigo 77.º
2. O auditor de segurança elabora um relatório anual de segurança que envia ao Órgão do Governo responsável pela Política de Informática até 31 de Março de cada ano civil.

Artigo 74.º

Contabilistas e auditores externos

Os contabilistas ou peritos contabilistas ao serviço das entidades certificadoras e os auditores externos que, por imposição legal, prestem às mesmas entidades serviços de auditoria devem comunicar ao Órgão do Governo responsável pela Política de Informática as infracções graves às normas legais ou regulamentares relevantes para a fiscalização e que detectem no exercício das suas funções.

Artigo 75.º

Recursos

Nos recursos interpostos das decisões tomadas pelo Órgão do Governo responsável pela Política de Informática no exercício dos seus poderes de credenciação e fiscalização, presume-se, até prova em contrário, que a suspensão da eficácia determina grave lesão do interesse público.

Artigo 76.º

Colaboração das autoridades

O Órgão do Governo responsável pela Política de Informática poderá solicitar às autoridades policiais e judiciárias e a quaisquer outras autoridades e serviços públicos toda a colaboração ou auxílio que julgue necessários para a credenciação e fiscalização da actividade de certificação.



Capítulo V

Disposições finais

Artigo 77.º

Normas regulamentares

1. A regulamentação do presente título, nomeadamente no que se refere à criação de entidades certificadoras, às normas de carácter técnico e de segurança, constará de decreto regulamentar, a adoptar no prazo de 300 dias.
2. O Órgão do Governo responsável pela Política de Informática poderá emitir normas regulamentares relativas aos requisitos a que devem obedecer os documentos que recebam por via electrónica.

Título III

Protecção Jurídica de Dados Pessoais

Capítulo I

Disposições gerais

Artigo 78.º

Objecto

O presente título tem por objecto garantir a protecção, no que concerne ao tratamento de dados pessoais, das liberdades públicas e dos direitos fundamentais das pessoas singulares, em especial a sua honra e a sua intimidade pessoal e familiar



Artigo 79.º

Âmbito de Aplicação

1. O presente título aplica-se ao tratamento de dados pessoais registados em suporte físico e que sejam susceptíveis de tratamento, e a toda a modalidade de uso posterior desses dados pelos sectores público ou privado.
2. O presente título aplica-se ao tratamento de dados pessoais efectuado:
 - a) No âmbito das actividades de estabelecimento do responsável do tratamento situado em território angolano;
 - b) Fora do território nacional, em local onde a legislação angolana seja aplicável por força do direito internacional;
 - c) Por responsável que, não estando estabelecido no território nacional, recorra, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território nacional, salvo se esses meios só forem utilizados para trânsito através do território nacional.
3. O presente título aplica-se à videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas sempre que o responsável pelo tratamento esteja domiciliado ou sediado na República de Angola ou utilize um fornecedor de acesso a redes informáticas e telemáticas estabelecido em território angolano.
4. No caso referido na alínea c) do n.º 2, o responsável pelo tratamento deve designar, mediante comunicação à Autoridade de Protecção de Dados Angolana / Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais, um representante estabelecido na República de Angola, que o substitua em todos os seus direitos e obrigações, sem prejuízo da sua própria responsabilidade.
5. O disposto no número anterior aplica-se no caso de o responsável pelo tratamento estar abrangido por estatuto de extraterritorialidade, de imunidade ou por qualquer outro que impeça o procedimento criminal.



6. O presente título aplica-se ao tratamento e dados pessoais que tenham por objectivo a segurança pública, a defesa nacional e a segurança do Estado, sem prejuízo do disposto em normas especiais constantes de instrumentos de direito internacional a que a República de Angola se vincule e de legislação específica atinente aos respectivos sectores.

7. O presente título não se aplica ao tratamento de dados pessoais efectuado por pessoa singular no exercício de actividades exclusivamente pessoais ou domésticas.

Artigo 80.º

Definições

Para efeitos do presente título, entende-se por:

- a) «**Dados pessoais**»: qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;
- b) «**Tratamento de dados pessoais**» («tratamento»): qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;
- c) «**Ficheiro de dados pessoais**» («ficheiro»): qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;



- d) **«Responsável pelo tratamento»:** a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios do 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 os dados pessoais em causa;
- e) **«Subcontratante»:** a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento;
- f) **«Terceiro»:** a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, não sendo o titular dos dados, o responsável pelo tratamento, o subcontratante ou outra pessoa sob autoridade directa do responsável pelo tratamento ou do subcontratante, esteja habilitado a tratar os dados;
- g) **«Destinatário»:** a pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo a quem sejam comunicados dados pessoais, independentemente de se tratar ou não de um terceiro, sem prejuízo de não serem consideradas destinatários as autoridades a quem sejam comunicados dados no âmbito de uma disposição legal;
- h) **«Consentimento do titular dos dados»:** qualquer manifestação de vontade, livre, inequívoca, específica e informada, nos termos da qual o titular aceita que os seus dados pessoais sejam objecto de tratamento;
- i) **«Interconexão de dados»:** forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade.



Capítulo II

Tratamento de dados pessoais

Secção I

Qualidade dos dados e legitimidade do seu tratamento

Artigo 81.º

Qualidade dos dados

1. Os dados pessoais devem ser:

- a) Tratados de forma lícita e com respeito pelo princípio da boa fé;
- b) Recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com essas finalidades;
- c) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e posteriormente tratados;
- d) Exactos e, se necessário, actualizados, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou rectificados os dados inexactos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente;
- e) Conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior.

2. Mediante requerimento do responsável pelo tratamento, e caso haja interesse legítimo, a Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais pode autorizar a conservação de dados para fins históricos, estatísticos ou científicos por período superior ao referido na alínea e) do número anterior.

3. Cabe ao responsável pelo tratamento assegurar a observância do disposto nos números anteriores.



Artigo 82.º

Condições de legitimidade do tratamento de dados

O tratamento de dados pessoais só pode ser efectuado se o seu titular tiver dado de forma inequívoca o seu consentimento ou se o tratamento for necessário para:

- a) Execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração da vontade negocial efectuadas a seu pedido;
- b) Cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito;
- c) Protecção de interesses vitais do titular dos dados, se este estiver física ou legalmente incapaz de dar o seu consentimento;
- d) Execução de uma missão de interesse público em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;
- e) Prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos fundamentais do titular dos dados.

Artigo 83.º

Tratamento de dados sensíveis

1. É proibido o tratamento de dados pessoais referentes a convicções filosóficas, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos.



2. Mediante disposição legal, autorização da Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais ou quando o titular dos dados tiver dado o seu consentimento expresso pode ser permitido o tratamento dos dados referidos no número anterior quando por motivos de interesse público importante esse tratamento for indispensável ao exercício das atribuições legais ou estatutárias do seu responsável, sempre com garantias de não discriminação e com as medidas de segurança previstas no artigo 92.º.

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 filosófico ou religioso, no âmbito das suas actividades legítimas, sob condição de o tratamento respeitar apenas aos membros desse organismo ou às pessoas que com ele mantenham contactos periódicos ligados às suas finalidades, 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.



4. O tratamento dos dados referentes à saúde e à vida sexual, incluindo os dados genéticos, é permitido quando útil para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde, desde que o tratamento desses dados seja efectuado por um profissional de saúde obrigado a sigilo ou por outra pessoa sujeita igualmente a segredo profissional, seja notificado à Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais, e sejam garantidas medidas adequadas de segurança da informação.

Artigo 84.º

Suspeitas de actividades ilícitas, infracções penais e contra-ordenações

1. A criação e manutenção de registos centrais relativos a pessoas suspeitas de actividades ilícitas, infracções penais, contra-ordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias só pode ser mantida por serviços públicos com competência específica prevista na respectiva lei de organização e funcionamento, observando normas procedimentais e de protecção de dados previstas em diploma legal, com prévio parecer da Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais.

2. O tratamento de dados pessoais relativos a suspeitas de actividades ilícitas, infracções penais, contra-ordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias pode ser autorizado pela Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais, 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 fundamentais.

3. 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 competências previstas no respectivo estatuto orgânico ou noutra disposição legal e ainda nos termos de acordo ou convenção internacional de que a República de Angola seja parte.



Artigo 85.º

Interconexão de dados pessoais

1. A interconexão de dados pessoais que não esteja prevista em disposição legal está sujeita a autorização da Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais solicitada pelo responsável ou em conjunto pelos correspondentes responsáveis dos tratamentos.

2. A interconexão de dados pessoais deve ser adequada à prossecução das finalidades legais ou estatutárias e de interesses legítimos dos responsáveis dos tratamentos, não implicar discriminação ou diminuição dos direitos fundamentais dos titulares dos dados, ser rodeada de adequadas medidas de segurança e ter em conta o tipo de dados objecto de interconexão, nos termos do previsto no artigo 102.º da presente lei.

Secção II

Direitos do titular dos dados

Artigo 86.º

Informação em caso de recolha de dados junto da pessoa em causa

1. Quando recolher dados pessoais directamente do seu titular, o responsável pelo tratamento ou o seu representante deve prestar-lhe, salvo se já dele forem conhecidas, as seguintes informações:

- a) Identidade do responsável pelo tratamento e, se for caso disso, do seu representante;
- b) Finalidades do tratamento;
- c) Outras informações, tais como:
 - i. Os destinatários ou categorias de destinatários dos dados;
 - ii. O carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder;



iii. A existência e as condições do direito de acesso e de rectificação, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir ao seu titular um tratamento leal dos mesmos.

2. Os documentos que sirvam de base à recolha de dados pessoais devem conter as informações constantes do número anterior.

Artigo 87.º

Informação em caso de dados não recolhidos junto da pessoa em causa

1. Se os dados não forem recolhidos junto do seu titular, e salvo se dele já forem conhecidas, o responsável pelo tratamento, ou o seu representante, deve prestar-lhe as informações previstas no n.º 1 do artigo anterior no momento do registo dos dados ou, se estiver prevista a comunicação a terceiros, o mais tardar aquando da primeira comunicação desses dados.

2. No caso de recolha de dados em redes abertas, o titular dos dados deve ser informado, salvo se disso já tiver conhecimento, 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.

3. A obrigação de informação pode ser dispensada, mediante disposição legal ou deliberação da Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais, por motivos de segurança do Estado e prevenção ou investigação criminal, e, bem assim, quando, nomeadamente no caso do tratamento de dados com finalidades estatísticas, históricas ou de investigação científica, a informação do titular dos dados se revelar impossível ou implicar esforços desproporcionados ou ainda quando a lei determinar expressamente o registo dos dados ou a sua divulgação.



Artigo 88.º

Direito de acesso

1. O titular dos dados tem o direito de obter do responsável pelo tratamento, livremente e sem restrições, com periodicidade razoável e sem demoras ou custos excessivos:

- a) A confirmação de serem ou não tratados dados que lhe digam respeito, bem como informação sobre as finalidades desse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados;
- b) A comunicação, sob forma inteligível, dos seus dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem desses dados;
- c) O conhecimento da lógica subjacente ao tratamento automatizado dos dados que lhe digam respeito;
- d) A rectificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto no presente título, nomeadamente devido ao carácter incompleto ou inexacto desses dados;
- e) A notificação aos terceiros a quem os dados tenham sido comunicados de qualquer rectificação, apagamento ou bloqueio efectuado nos termos da alínea d), salvo se isso for comprovadamente impossível.

2. No caso de tratamento de dados pessoais relativos à segurança do Estado e à prevenção ou investigação criminal, o direito de acesso é exercido através da Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais ou de outra autoridade independente a quem a lei atribua a verificação do cumprimento da legislação de protecção de dados pessoais.

3. Nos casos previstos no n.º 2 se a comunicação dos dados ao seu titular puder prejudicar a segurança do Estado, a prevenção ou a investigação criminal, a Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais limita-se a informar o titular dos dados das diligências efectuadas.



4. O direito de acesso à informação relativa a dados da saúde, incluindo os dados genéticos, é exercido por intermédio de médico escolhido pelo titular dos dados.

5. No caso de os dados não serem utilizados para tomar medidas ou decisões em relação a pessoas determinadas, a lei pode restringir o direito de acesso nos casos em que manifestamente não exista qualquer perigo de violação dos direitos fundamentais do titular dos dados, designadamente do direito à vida privada, e os referidos dados forem exclusivamente utilizados para fins de investigação científica ou conservados sob forma de dados pessoais durante um período que não exceda o necessário à finalidade exclusiva de elaborar estatísticas.

Artigo 89.º

Direito de oposição do titular dos dados

O titular dos dados tem o direito de:

- a) Salvo disposição legal em contrário, e pelo menos nos casos referidos nas alíneas d) e e) do artigo 82.º, se opor em qualquer altura, por razões ponderosas e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objecto de tratamento, devendo, em caso de oposição justificada, o tratamento efectuado pelo responsável deixar de poder incidir sobre esses dados;
- b) Se opor, a seu pedido e gratuitamente, ao tratamento dos dados pessoais que lhe digam respeito previsto pelo responsável pelo tratamento para efeitos de *marketing* directo ou qualquer outra forma de prospecção, ou de ser informado, antes de os dados pessoais serem comunicados pela primeira vez a terceiros para fins de *marketing* directo ou utilizados por conta de terceiros, e de lhe ser expressamente facultado o direito de se opor, sem despesas, a tais comunicações ou utilizações.



Artigo 90.º

Decisões individuais automatizadas

1. Qualquer pessoa tem o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, designadamente a sua capacidade profissional, o seu crédito, a confiança de que é merecedora ou o seu comportamento.
2. Sem prejuízo do cumprimento das restantes disposições do presente título, uma pessoa pode ficar sujeita a uma decisão tomada nos termos do n.º 1, desde que tal ocorra no âmbito da celebração ou da execução de um contrato, e sob condição de o seu pedido de celebração ou execução do contrato ter sido satisfeito, ou de existirem medidas adequadas que garantam a defesa dos seus interesses legítimos, designadamente o seu direito de representação e expressão.
3. Pode ainda ser permitida a tomada de uma decisão nos termos do n.º 1 quando a Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais o autorize, definindo medidas de garantia da defesa dos interesses legítimos do titular dos dados.



Secção III

Segurança e confidencialidade do tratamento

Artigo 91.º

Segurança do tratamento

1. O responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito; estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.
2. O responsável pelo tratamento, em caso de tratamento por sua conta, deverá escolher um subcontratante que ofereça garantias suficientes em relação às medidas de segurança técnica e de organização do tratamento a efectuar, e deverá zelar pelo cumprimento dessas medidas.
3. A realização de operações de tratamento em subcontratação deve ser regida por um contrato ou acto jurídico que vincule o subcontratante ao responsável pelo tratamento e que estipule, designadamente, que o subcontratante apenas actua mediante instruções do responsável pelo tratamento e que lhe incumbe igualmente o cumprimento das obrigações referidas no n.º 1.
4. Os elementos de prova da declaração negocial, do contrato ou do acto jurídico relativos à protecção dos dados, bem como as exigências relativas às medidas referidas no n.º 1, são consignados por escrito em documento em suporte com valor probatório legalmente reconhecido.



Artigo 92.º

Medidas especiais de segurança

1. Os responsáveis pelo tratamento dos dados referidos no n.º 2 do artigo 83.º e no n.º 1 do artigo 84.º devem tomar as medidas adequadas para:

- a) Impedir o acesso de pessoa não autorizada às instalações utilizadas para o tratamento desses dados (controlo da entrada nas instalações);
- b) Impedir que suportes de dados possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada (controlo dos suportes de dados);
- c) Impedir a introdução não autorizada, bem como a tomada de conhecimento, a alteração ou a eliminação não autorizadas de dados pessoais inseridos (controlo da inserção);
- d) Impedir que sistemas de tratamento automatizados de dados possam ser utilizados por pessoas não autorizadas através de instalações de transmissão de dados (controlo da utilização);
- e) Garantir que as pessoas autorizadas só possam ter acesso aos dados abrangidos pela autorização (controlo de acesso);
- f) Garantir a verificação das entidades a quem possam ser transmitidos os dados pessoais através das instalações de transmissão de dados (controlo da transmissão);
- g) Garantir que possa verificar-se *a posteriori*, em prazo adequado à natureza do tratamento, a fixar na regulamentação aplicável a cada sector, quais os dados pessoais introduzidos quando e por quem (controlo da introdução);
- h) Impedir que, na transmissão de dados pessoais, bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada (controlo do transporte).

2. Tendo em conta a natureza das entidades responsáveis pelo tratamento e o tipo das instalações em que é efectuado, a Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais pode dispensar a existência de certas medidas de segurança, garantido que se mostre o respeito pelos direitos fundamentais dos titulares dos dados.



3. Os sistemas devem garantir a separação lógica entre os dados referentes à saúde e à vida sexual, incluindo os genéticos, dos restantes dados pessoais.

4. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais pode determinar que, nos casos em que a circulação em rede de dados pessoais referidos nos artigos 83.º e 84.º possa pôr em risco direitos fundamentais dos respectivos titulares, a transmissão seja cifrada.

Artigo 93.º

Tratamento por subcontratante

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

Artigo 94.º

Sigilo profissional

1. Os responsáveis do tratamento de dados pessoais, bem como as pessoas que, no exercício das suas funções, tenham conhecimento dos dados pessoais tratados, ficam obrigados a sigilo profissional, mesmo após o termo das suas funções.

2. Igual obrigação recai sobre os membros da Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais, mesmo após o termo do mandato.

3. O disposto nos números anteriores não exclui o dever do fornecimento das informações obrigatórias, nos termos legais, excepto quando constem de ficheiros organizados para fins estatísticos.



4. Os funcionários, agentes ou técnicos que exerçam funções de assessoria à Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais estão sujeitos à mesma obrigação de sigilo profissional.

Artigo 95.º

Cessação do Tratamento de Dados

1. Em caso de cessação, por qualquer causa, do tratamento de dados, o responsável pelo tratamento dos dados deve notificar previamente a Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais do seu destino.

2. Os dados podem ser:

- a) Destruídos;
- b) Cedidos a outro responsável pelo tratamento, desde que sejam destinados a um tratamento com finalidades análogas aquelas para que os dados foram inicialmente recolhidos;
- c) Conservados para fins exclusivamente pessoais e não destinados a uma comunicação sistemática ou à difusão;
- d) Conservados ou cedidos a outro responsável pelo tratamento para finalidades históricas, científicas ou de estatística, desde que em conformidade com as normas deste título.



Capítulo III

Transferência de dados pessoais

Artigo 96.º

Princípios

1. A transferência de dados pessoais para outro Estado que sejam objecto de tratamento ou que se destinem a sê-lo só pode realizar-se com o respeito das disposições do presente título e se o Estado para onde são transferidos assegurar um nível de protecção adequado.
2. A adequação do nível de protecção é apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, devem ser tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projectados, os países de origem e de destino final, as regras de direito, gerais ou sectoriais, em vigor no Estado em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse Estado.

Artigo 97.º

Derrogações

1. A transferência de dados pessoais para um Estado que não assegure um nível de protecção adequado na acepção do artigo anterior pode ser permitida pela Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais se o titular dos dados tiver dado de forma inequívoca o seu consentimento à transferência ou se essa transferência:
 - a) 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;
 - b) For necessária para a execução ou celebração de um contrato celebrado ou a celebrar, no interesse do titular dos dados, entre o responsável pelo tratamento e um terceiro; ou



- c) For necessária ou legalmente exigida para a protecção de um interesse público importante, ou para a declaração, o exercício ou a defesa de um direito num processo judicial; ou
- d) For necessária para proteger os interesses vitais do titular dos dados; ou
- e) For realizada a partir de um registo público que, nos termos de disposições legislativas ou regulamentares, se destine à informação do público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar um interesse legítimo, desde que as condições estabelecidas na lei para a consulta sejam cumpridas no caso concreto.

2. Sem prejuízo do disposto no n.º 1, a Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais pode autorizar uma transferência ou um conjunto de transferências de dados pessoais para um Estado que não assegure um nível de protecção adequado na acepção do artigo anterior, desde que o responsável pelo tratamento assegure mecanismos suficientes de garantia de protecção da vida privada e dos direitos fundamentais das pessoas, bem como do seu exercício, designadamente, mediante cláusulas contratuais adequadas.

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 e acordos internacionais em que a República de Angola é parte.



Capítulo IV

Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais

Secção I

Natureza, Atribuições e Competências

Artigo 98.º

Natureza

1. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais é uma entidade administrativa independente, cuja organização e funcionamento serão reguladas em sede própria.
2. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais, independentemente do direito nacional aplicável a cada tratamento de dados em concreto, exerce as suas competências em todo o território nacional.
3. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais coopera com as autoridades de controlo de protecção de dados de outros Estados na difusão do direito e das regulamentações nacionais em matéria de protecção de dados pessoais, bem como na defesa e no exercício dos direitos de pessoas residentes no estrangeiro.

Artigo 99.º

Atribuições

1. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais é a autoridade nacional que tem como atribuição controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de protecção de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei.



2. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais deve ser consultada sobre quaisquer disposições legais, bem como sobre instrumentos jurídicos em preparação em instituições internacionais, relativos ao tratamento de dados pessoais.

3. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais dispõe:

- a) De poderes de investigação e de inquérito, podendo aceder aos dados objecto de tratamento e recolher todas as informações necessárias ao desempenho das suas funções de controlo;
- b) De poderes de autoridade, designadamente o de ordenar o bloqueio, apagamento ou destruição dos dados, bem como o de proibir, temporária ou definitivamente, o tratamento de dados pessoais, ainda que incluídos em redes abertas de transmissão de dados a partir de servidores situados em território angolano;
- c) Do poder de emitir pareceres prévios aos tratamentos de dados pessoais, assegurando a sua publicitação.

4. Em caso de reiterado não cumprimento das disposições legais em matéria de dados pessoais, a Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais pode advertir ou censurar publicamente o responsável pelo tratamento, bem como suscitar a questão, de acordo com as respectivas competências, à Assembleia Nacional, ao Governo ou a outros órgãos ou autoridades.

5. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais 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.



6. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais é representada em juízo pelo Ministério Público e está isenta de custas nos processos em que intervenha.

Artigo 100.º

Competências

1. Compete em especial à Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais:

- a) Emitir parecer sobre disposições legais, bem como sobre instrumentos jurídicos em preparação em instituições internacionais, relativos ao tratamento de dados pessoais;
- b) Autorizar ou registar, consoante os casos, os tratamentos de dados pessoais;
- c) Autorizar excepcionalmente a utilização de dados pessoais para finalidades não determinantes da recolha, com respeito pelos princípios definidos no artigo 81.º;
- d) Autorizar a interconexão de tratamentos automatizados de dados pessoais;
- e) Autorizar a transferência de dados pessoais nos casos previstos no artigo 97.º;
- f) Fixar o tempo da conservação dos dados pessoais em função da finalidade, podendo emitir directivas para determinados sectores de actividade;
- g) Fazer assegurar o direito de acesso à informação, bem como do exercício do direito de rectificação e actualização;
- h) Autorizar a fixação de custos ou de periodicidade para o exercício do direito de acesso, bem como fixar os prazos máximos de cumprimento, em cada sector de actividade, das obrigações que, por força dos artigos 88.º a 90.º, incumbem aos responsáveis pelo tratamento de dados pessoais;
- i) Dar seguimento ao pedido efectuado por qualquer pessoa, ou por associação que a represente, para protecção dos seus direitos fundamentais no que diz respeito ao tratamento de dados pessoais e informá-la do resultado;
- j) Efectuar, a pedido de qualquer pessoa, a verificação da licitude de um tratamento de dados, sempre que esse tratamento esteja sujeito a restrições de acesso ou de informação, e informá-la da realização da verificação;



- k) Apreciar as reclamações, queixas ou petições dos particulares;
- l) Dispensar a execução de medidas de segurança, nos termos previstos no n.º 2 do artigo 92.º, podendo emitir directivas para determinados sectores de actividade;
- m) Assegurar a representação junto de instâncias comuns de controlo e em reuniões internacionais de entidades independentes de controlo da protecção de dados pessoais, bem como participar em reuniões internacionais no âmbito das suas competências;
- n) Deliberar sobre a aplicação de coimas;
- o) Promover e apreciar códigos de conduta;
- p) Promover a divulgação e esclarecimento dos direitos relativos à protecção de dados e dar publicidade periódica à sua actividade, nomeadamente através da publicação de um relatório anual;
- q) Exercer outras competências legalmente previstas.

2. No exercício das suas competências de emissão de directivas ou de apreciação de códigos de conduta, a Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais deve promover a audição das associações de defesa dos interesses em causa.

3. No exercício das suas funções, a Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais profere decisões com força obrigatória, passíveis de reclamação e de recurso para as Salas de Direito Administrativo dos Tribunais Provinciais.

4. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais pode sugerir à Assembleia Nacional as providências que entender úteis à prossecução das suas atribuições e ao exercício das suas competências.



Artigo 101.º

Dever de colaboração

1. As entidades públicas e privadas devem prestar a sua colaboração à Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais, facultando-lhe todas as informações que por esta, no exercício das suas competências, lhe forem solicitadas.
2. O dever de colaboração é assegurado, designadamente, quando a Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais tiver necessidade, para o cabal exercício das suas funções, de examinar o sistema informático e os ficheiros de dados pessoais, bem como toda a documentação relativa ao tratamento e transmissão de dados pessoais.
3. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais, bem como os técnicos por ela mandatados, têm direito de acesso aos sistemas informáticos que sirvam de suporte ao tratamento dos dados, bem como à documentação referida no número anterior, no âmbito das suas atribuições e competências.

Secção II

Notificação

Artigo 102.º

Obrigaç o de notifica o   Autoridade de Protec o de Dados Angolana/ Autoridade Nacional de Protec o de Dados ou Autoridade de Protec o de Dados Pessoais

1. O respons vel pelo tratamento ou, se for caso disso, o seu representante deve notificar a Autoridade de Protec o de Dados Angolana/ Autoridade Nacional de Protec o de Dados ou Autoridade de Protec o de Dados Pessoais antes da realiza o de um tratamento ou conjunto de tratamentos, total ou parcialmente automatizados, destinados   prossegu o de uma ou mais finalidades interligadas.



2. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais pode autorizar a simplificação ou a isenção da notificação para determinadas categorias de tratamentos que, atendendo aos dados a tratar, não sejam susceptíveis de pôr em causa os direitos fundamentais dos titulares dos dados e tenham em conta critérios de celeridade, economia e eficiência.

3. A autorização, que está sujeita a publicação no *Diário da República*, deve 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.

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

5. Os tratamentos não automatizados dos dados pessoais previstos no n.º 1 do artigo 83.º estão sujeitos a notificação quando tratados ao abrigo da alínea a) do n.º 3 do mesmo artigo.

Artigo 103.º

Controlo prévio

1. Carecem de autorização da Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais:

- a) O tratamento dos dados pessoais a que se referem o n.º 2 do artigo 83.º e o n.º 2 do artigo 84.º;
- b) O tratamento dos dados pessoais relativos ao crédito e à solvabilidade dos seus titulares;
- c) A interconexão de dados pessoais prevista no artigo 85.º;
- d) A utilização de dados pessoais para fins não determinantes da recolha.



2. Os tratamentos a que se refere o número anterior podem ser autorizados por diploma legal, não carecendo neste caso de autorização da Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais.

Artigo 104.º

Conteúdo dos pedidos de parecer ou de autorização e da notificação

Os pedidos de parecer ou de autorização, bem como as notificações, remetidos à Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais devem conter as seguintes informações:

- a) Nome e endereço do responsável pelo tratamento e, se for o caso, do seu representante;
- b) As finalidades do tratamento;
- c) Descrição da ou das categorias de titulares dos dados e dos dados ou categorias de dados pessoais que lhes respeitem;
- d) Destinatários ou categorias de destinatários a quem os dados podem ser comunicados e em que condições;
- e) Entidade encarregada do processamento da informação, se não for o próprio responsável do tratamento;
- f) Eventuais interconexões de tratamentos de dados pessoais;
- g) Tempo de conservação dos dados pessoais;
- h) Forma e condições como os titulares dos dados podem ter conhecimento ou fazer corrigir os dados pessoais que lhes respeitem;
- i) Transferências de dados previstas para países terceiros;
- j) Descrição geral que permita avaliar de forma preliminar a adequação das medidas tomadas para garantir a segurança do tratamento em aplicação dos artigos 91.º e 92.º.



Artigo 105.º

Indicações obrigatórias

1. Os diplomas legais referidos no n.º 2 do artigo 83.º e no n.º 1 do artigo 84.º, bem como as autorizações da Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais e os registos de tratamentos de dados pessoais 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) 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) Eventuais interconexões de tratamentos de dados pessoais;
- f) Transferências de dados previstas para outros países.

2. Qualquer alteração das indicações constantes do n.º 1 está sujeita aos procedimentos previstos nos artigos 102.º e 103.º.

Artigo 106.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 Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais, aberto à consulta por qualquer pessoa.

2. O registo contém as informações enumeradas nas alíneas a) a d) e i) do artigo 104.º.

3. O responsável por tratamento de dados não sujeito a notificação está obrigado a prestar, de forma adequada, a qualquer pessoa que lho solicite, pelo menos as informações referidas no n.º 1 do artigo 105.º



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 Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais deve publicar no seu relatório anual todos os pareceres e autorizações elaborados ou concedidas ao abrigo da presente lei, designadamente as autorizações previstas no n.º 2 do artigo 83.º e no n.º 2 do artigo 85.º.

Capítulo V

Códigos de conduta

Artigo 107.º

Códigos de conduta

1. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais apoia a elaboração de códigos de conduta destinados a contribuir, em função das características dos diferentes sectores, para a boa execução das disposições do presente título.

2. As associações profissionais e outras organizações representativas de categorias de responsáveis pelo tratamento de dados que tenham elaborado projectos de códigos de conduta podem submetê-los à apreciação da Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais.

3. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais pode declarar a conformidade dos projectos com as disposições legais e regulamentares vigentes em matéria de protecção de dados pessoais.



Capítulo VI

Tutela administrativa e jurisdicional

Secção I

Tutela administrativa e jurisdicional

Artigo 108.º

Tutela administrativa e jurisdicional

Sem prejuízo do direito de apresentação de queixa à Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais, qualquer pessoa pode, nos termos da lei, recorrer a meios administrativos ou jurisdicionais para garantir o cumprimento das disposições legais em matéria de protecção de dados pessoais.

Artigo 109.º

Responsabilidade civil

1. Qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro acto que viole disposições legais em matéria de protecção de dados pessoais tem o direito de obter do responsável a reparação pelo prejuízo sofrido.
2. O responsável pelo tratamento pode ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano lhe não é imputável.
3. Quando se trate de ficheiros de titularidade pública, a responsabilidade é exigida de acordo com a legislação do regime de responsabilidade da Administração Pública.
4. No caso de ficheiros de titularidade privada, a acção de indemnização será proposta nos tribunais ordinários.



Secção II

Contra-ordenações

Artigo 110.º

Legislação subsidiária

Às infracções previstas na presente secção é subsidiariamente aplicável o regime geral das contra-ordenações, com as adaptações constantes dos artigos seguintes.

Artigo 111.º

Cumprimento do dever omitido

Sempre que a contra-ordenação resulte de omissão de um dever, a aplicação da sanção e o pagamento da coima não dispensam o infractor do seu cumprimento, se este ainda for possível.

Artigo 112.º

Omissão ou defeituoso cumprimento de obrigações

1. As entidades que, por negligência, não cumpram a obrigação de notificação à Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais do tratamento de dados pessoais a que se referem os n.ºs 1 e 5 do artigo 102.º, prestem falsas informações ou cumpram a obrigação de notificação com inobservância dos termos previstos no artigo 104.º, ou ainda quando, depois de notificadas pela Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais, mantiverem o acesso às redes abertas de transmissão de dados a responsáveis por tratamento de dados pessoais que não cumpram as disposições da presente lei, praticam contra-ordenação punível com as seguintes coimas:

- a) Tratando-se de pessoa singular, no mínimo de Kz 28.000,00 e no máximo de Kz 280.000,00;
- b) Tratando-se de pessoa colectiva ou de entidade sem personalidade jurídica, no mínimo de Kz 168.000,00 e no máximo de Kz 1.680.000,00.



2. A coima é agravada para o dobro dos seus limites quando se trate de dados sujeitos a controlo prévio, nos termos do artigo 103.º

Artigo 113.º

Contra-ordenações

1. Praticam contra-ordenação punível com a coima mínima de Kz 56.000,00 e máxima de Kz 560.000,00, as entidades que não cumprirem alguma das seguintes disposições da presente lei:

- a) Designar representante nos termos previstos no n.º 5 do artigo 79.º;
- b) Observar as obrigações estabelecidas nos artigos 81.º, 86.º, 87.º, 88.º, 89.º, 90.º, 92.º, 93.º e 106.º, n.º 3.

2. A pena é agravada para o dobro dos seus limites quando não forem cumpridas as obrigações constantes dos artigos 82.º, 83.º, 84.º, 85.º, 96.º e 97.º.

Artigo 114.º

Concurso de infracções

1. Se o mesmo facto constituir, simultaneamente, crime e contra-ordenação, o agente é punido sempre a título de crime.

2. As sanções aplicadas às contra-ordenações em concurso são sempre cumuladas materialmente.

Artigo 115.º

Punição da negligência e da tentativa

1. A negligência é sempre punida nas contra-ordenações previstas no artigo 113.º

2. A tentativa é sempre punível nas contra-ordenações previstas nos artigos 112.º e 113.º.



Artigo 116.º

Aplicação das coimas

1. A aplicação das coimas previstas no presente título compete ao Coordenador da Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais, sob prévia deliberação da Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais.

2. A deliberação da Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais, depois de homologada pelo Coordenador, constitui título executivo, no caso de não ser impugnada no prazo legal.

Artigo 117.º

Destino das receitas cobradas

O montante das importâncias cobradas, em resultado da aplicação das coimas, reverte, em partes iguais, para o Estado e para a Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais.

Secção III

Crimes

Artigo 118.º

Não cumprimento de obrigações relativas a protecção de dados

1. É punido com prisão até um ano ou multa até 120 dias quem intencionalmente:

- a) Omitir a notificação ou o pedido de autorização a que se referem os artigos 102.º e 103.º;



- b) Fornecer falsas informações na notificação ou nos pedidos de autorização para o tratamento de dados pessoais ou neste proceder a modificações não consentidas pelo instrumento de legalização;
- c) Desviar ou utilizar dados pessoais, de forma incompatível com a finalidade determinante da recolha ou com o instrumento de legalização;
- d) Promover ou efectuar uma interconexão ilegal de dados pessoais;
- e) Depois de ultrapassado o prazo que lhes tiver sido fixado pela Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais para cumprimento das obrigações previstas na presente lei ou em outra legislação de protecção de dados, as não cumprir;
- f) Depois de notificado pela Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais para o não fazer, mantiver o acesso a redes abertas de transmissão de dados a responsáveis pelo tratamento de dados pessoais que não cumpram as disposições da presente lei.

2. A pena é agravada para o dobro dos seus limites quando se tratar de dados pessoais a que se referem os artigos 83.º e 84.

Artigo 119.º

Acesso indevido

1. Quem, sem a devida autorização, por qualquer modo, aceder a dados pessoais cujo acesso lhe está vedado, é punido com prisão até um ano ou multa até 120 dias.

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

- a) For conseguido através de violação de regras técnicas de segurança;
- b) Tiver possibilitado ao agente ou a terceiros o conhecimento de dados pessoais;
- c) Tiver proporcionado ao agente ou a terceiros, benefício ou vantagem patrimonial.

3. No caso do n.º 1 o procedimento criminal depende de queixa.



Artigo 120.º

Viciação ou destruição de dados pessoais

1. Quem, sem a devida autorização, apagar, destruir, danificar, suprimir ou modificar dados pessoais, tornando-os inutilizáveis ou afectando a sua capacidade de uso, é punido com prisão até dois anos ou multa até 240 dias.
2. A pena é agravada para o dobro nos seus limites se o dano produzido for particularmente grave.
3. Se o agente actuar com negligência, a pena é, em ambos os casos, de prisão até um ano ou multa até 120 dias.

Artigo 121.º

Desobediência qualificada

1. Quem, depois de notificado para o efeito, não interromper, cessar ou bloquear o tratamento de dados pessoais é punido com a pena correspondente ao crime de desobediência qualificada.
2. Na mesma pena incorre quem, depois de notificado:
 - a) Recusar, sem justa causa, a colaboração que concretamente lhe for exigida nos termos do artigo 101.º;
 - b) Não proceder ao apagamento, destruição total ou parcial de dados pessoais;
 - c) Não proceder à destruição de dados pessoais, findo o prazo de conservação previsto no artigo 81.º.



Artigo 122.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 prisão até dois anos ou multa até 240 dias.

2. A pena é agravada em metade dos seus limites se o agente:
 - a) For funcionário público ou equiparado, nos termos da lei penal;
 - b) For determinado pela intenção de obter qualquer vantagem patrimonial ou outro benefício ilegítimo;
 - c) Puser em perigo a reputação, a honra e consideração ou a intimidade da vida privada de outrem.

3. A negligência é punível com prisão até seis meses ou multa até 120 dias.

4. Fora dos casos previstos no n.º 2, o procedimento criminal depende de queixa.

Artigo 123.º

Punição da tentativa

Nos crimes previstos nas disposições anteriores, a tentativa é sempre punível.

Artigo 124.º

Pena acessória

1. Conjuntamente com as coimas e penas aplicadas pode, acessoriamente, ser ordenada:
 - a) A proibição temporária ou definitiva do tratamento, o bloqueio, o apagamento ou a destruição total ou parcial dos dados;
 - b) A publicidade da sentença condenatória;



- c) A advertência ou censura públicas do responsável pelo tratamento, nos termos do n.º 4 do artigo 99.º
2. A publicidade da decisão condenatória faz-se a expensas do condenado, na publicação periódica de maior expansão editada na área da comarca da prática da infracção ou, na sua falta, em publicação periódica da comarca mais próxima, bem como através da afixação de edital em suporte adequado, por período não inferior a 30 dias.
3. A publicação é feita por extracto de que constem os elementos da infracção e as sanções aplicadas, bem como a identificação do agente.

Capítulo VII

Disposições finais

Artigo 125.º

Disposição transitória

1. Os tratamentos de dados existentes em ficheiros manuais à data da entrada em vigor da presente lei devem cumprir o disposto nos artigos 83.º, 84.º, 86.º, 87.º e 88.º no prazo de cinco anos.
2. Em qualquer caso, o titular dos dados pode obter, a seu pedido e, nomeadamente, aquando do exercício do direito de acesso, a rectificação, o apagamento ou o bloqueio dos dados incompletos, inexactos ou conservados de modo incompatível com os fins legítimos prosseguidos pelo responsável pelo tratamento.
3. A Autoridade de Protecção de Dados Angolana/ Autoridade Nacional de Protecção de Dados ou Autoridade de Protecção de Dados Pessoais pode autorizar que os dados existentes em ficheiros manuais e conservados unicamente com finalidades de investigação histórica não tenham que cumprir os artigos 83.º, 84.º e 85.º, desde que não sejam em nenhum caso reutilizados para finalidade diferente.



Título IV

Protecção da Privacidade no Sector das Comunicações Electrónicas

Capítulo I

Objecto e Âmbito

Artigo 126.º

Objecto e âmbito de aplicação

1. O presente título é relativo ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas.
2. O presente título aplica-se ao tratamento de dados pessoais no contexto das redes e serviços de comunicações electrónicas acessíveis ao público, especificando e complementando as disposições do título anterior.
3. As disposições do presente título asseguram a protecção dos interesses legítimos dos assinantes que sejam pessoas colectivas na medida em que tal protecção seja compatível com a sua natureza.
4. As excepções à aplicação do presente título que se mostrem estritamente necessárias para a protecção de actividades relacionadas com a segurança pública, a defesa, a segurança do Estado e a prevenção, investigação e repressão de infracções penais são definidas em legislação especial.



Artigo 127.º

Definições

1. Para efeitos do presente título, entende-se por:

- a. «**Comunicação electrónica**» qualquer informação trocada ou enviada entre um número finito de partes mediante a utilização de um serviço de comunicações electrónicas acessível ao público;
- b. «**Assinante**» a pessoa singular ou colectiva que é parte num contrato com uma empresa que forneça redes e ou serviços de comunicações electrónicas acessíveis ao público para fornecimento desses serviços;
- c. «**Utilizador**» qualquer pessoa singular que utilize um serviço de comunicações electrónicas acessível ao público para fins privados ou comerciais, não sendo necessariamente assinante desse serviço;
- d. «**Dados de tráfego**» quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos da facturação da mesma;
- e. «**Dados de localização**» quaisquer dados tratados numa rede de comunicações electrónicas que indiquem a posição geográfica do equipamento terminal de um assinante ou de qualquer utilizador de um serviço de comunicações electrónicas acessível ao público;
- f. «**Serviços de valor acrescentado**» todos aqueles que requeiram o tratamento de dados de tráfego ou de dados de localização que não sejam dados de tráfego, para além do necessário à transmissão de uma comunicação ou à facturação da mesma;
- g. «**Chamada**» qualquer ligação estabelecida através de um serviço telefónico acessível ao público que permite uma comunicação bidireccional em tempo real;
- h. «**Consentimento**» por parte do utilizador ou assinante significa o consentimento dado pela pessoa a quem dizem respeito os dados, previsto no título anterior;



2. São excluídas da alínea a) do número anterior as informações enviadas no âmbito de um serviço de difusão ao público em geral, através de uma rede de comunicações electrónicas, que não possam ser relacionadas com o assinante de um serviço de comunicações electrónicas ou com qualquer utilizador identificável que receba a informação.

Capítulo II

Segurança e confidencialidade

Artigo 128.º

Segurança

1. As empresas que oferecem redes e as empresas que oferecem serviços de comunicações electrónicas devem colaborar entre si no sentido da adopção de medidas técnicas e organizacionais eficazes para garantir a segurança dos seus serviços e, se necessário, a segurança da própria rede.

2. As medidas referidas no número anterior devem ser adequadas à prevenção dos riscos existentes, tendo em conta a proporcionalidade dos custos da sua aplicação e o estado da evolução tecnológica.

3. Em caso de risco especial de violação da segurança da rede, as empresas que oferecem serviços de comunicações electrónicas acessíveis ao público devem gratuitamente informar os assinantes desse serviço da existência daquele risco, bem como das soluções possíveis para o evitar e custos prováveis das mesmas.

Artigo 129.º

Inviolabilidade das comunicações electrónicas

1. As empresas que oferecem redes e ou serviços de comunicações electrónicas devem garantir a inviolabilidade das comunicações e respectivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações electrónicas acessíveis ao público.



2. É proibida a escuta, a instalação de dispositivos de escuta, o armazenamento ou outros meios de interceptação ou vigilância de comunicações e dos respectivos dados de tráfego por terceiros sem o consentimento prévio e expresso dos utilizadores, com excepção dos casos previstos na lei.

3. O disposto no presente artigo não impede as gravações legalmente autorizadas de comunicações e dos respectivos dados de tráfego, quando realizadas no âmbito de práticas comerciais lícitas, para o efeito de prova de uma transacção comercial nem de qualquer outra comunicação feita no âmbito de uma relação contratual, desde que o titular dos dados tenha sido disso informado e dado o seu consentimento.

4. São autorizadas as gravações de comunicações de e para serviços públicos destinados a prover situações de emergência de qualquer natureza.

Artigo 130.º

Armazenamento e acesso à informação

1. A utilização das redes de comunicações electrónicas para o armazenamento de informações ou para obter acesso à informação armazenada no equipamento terminal de um assinante ou de qualquer utilizador é apenas permitida quando estejam reunidas as seguintes condições:

- a) Serem fornecidas ao assinante ou utilizador em causa informações claras e completas, nomeadamente sobre os objectivos do processamento, em conformidade com o disposto no título anterior;
- b) Ser dado ao assinante ou ao utilizador o direito de recusar esse processamento.

2. O disposto no número anterior e no n.º 1 do artigo 129.º não impede o armazenamento automático, intermédio e transitório ou o acesso estritamente necessários para:

- a) Efectuar ou facilitar a transmissão de uma comunicação através de uma rede de comunicações electrónicas;



- b) Fornecer um serviço no âmbito da sociedade da informação que tenha sido explicitamente solicitado pelo assinante ou por qualquer utilizador.

Artigo 131.º

Dados de tráfego

1. Sem prejuízo do disposto nos números seguintes, os dados de tráfego relativos aos assinantes e utilizadores tratados e armazenados pelas empresas que oferecem redes e ou serviços de comunicações electrónicas devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação.
2. É permitido o tratamento de dados de tráfego necessários à facturação dos assinantes e ao pagamento de interligações, designadamente:
 - a) Número ou identificação, endereço e tipo de posto do assinante;
 - b) Número total de unidades a cobrar para o período de contagem, bem como o tipo, hora de início e duração das chamadas efectuadas ou o volume de dados transmitidos;
 - c) Data da chamada ou serviço e número chamado;
 - d) Outras informações relativas a pagamentos, tais como pagamentos adiantados, pagamentos a prestações, cortes de ligação e avisos.
3. O tratamento referido no número anterior apenas é lícito até final do período durante o qual a factura pode ser legalmente contestada ou o pagamento reclamado.
4. As empresas que oferecem serviços de comunicações electrónicas podem tratar os dados referidos no n.º 1 na medida e pelo tempo necessários à comercialização de serviços de comunicações electrónicas ou ao fornecimento de serviços de valor acrescentado desde que o assinante ou o utilizador a quem os dados digam respeito tenha para tanto dado o seu prévio consentimento, o qual pode ser retirado a qualquer momento.



5. Nos casos previstos no n.º 2 e, antes de ser obtido o consentimento dos assinantes ou utilizadores, nos casos previstos no n.º 4, as empresas que oferecem serviços de comunicações electrónicas devem fornecer-lhes informações exactas e completas sobre o tipo de dados que são tratados, os fins e a duração desse tratamento, bem como sobre a sua eventual disponibilização a terceiros para efeitos da prestação de serviços de valor acrescentado.

6. O tratamento dos dados de tráfego deve ser limitado aos trabalhadores e colaboradores das empresas que oferecem redes e ou serviços de comunicações electrónicas acessíveis ao público encarregados da facturação ou da gestão do tráfego, das informações a clientes, da detecção de fraudes, da comercialização dos serviços de comunicações electrónicas acessíveis ao público, ou da prestação de serviços de valor acrescentado, restringindo-se ao necessário para efeitos das referidas actividades.

7. O disposto nos números anteriores não prejudica o direito de os tribunais e as demais autoridades competentes obterem informações relativas aos dados de tráfego, nos termos da legislação aplicável, com vista à resolução de litígios, em especial daqueles relativos a interligações ou à facturação.

Artigo 132.º

Dados de localização

1. Nos casos em que sejam processados dados de localização, para além dos dados de tráfego, relativos a assinantes ou utilizadores das redes públicas de comunicações ou de serviços de comunicações electrónicas acessíveis ao público, o tratamento destes dados é permitido apenas se os mesmos forem tornados anónimos.

2. É permitido o registo, tratamento e transmissão de dados de localização às organizações com competência legal para receber chamadas de emergência para efeitos de resposta a essas chamadas.



3. O tratamento de dados de localização é igualmente permitido na medida e pelo tempo necessário para a prestação de serviços de valor acrescentado, desde que seja obtido consentimento prévio por parte dos assinantes ou utilizadores.

4. As empresas que oferecem serviços de comunicações electrónicas acessíveis ao público devem, designadamente, informar os utilizadores ou assinantes, antes de obterem o seu consentimento, sobre o tipo de dados de localização que serão tratados, a duração e os fins do tratamento e a eventual transmissão dos dados a terceiros para efeitos de fornecimento de serviços de valor acrescentado.

5. As empresas que oferecem serviços de comunicações electrónicas acessíveis ao público devem garantir aos assinantes e utilizadores a possibilidade de, através de um meio simples e gratuito:

- a) Retirar a qualquer momento o consentimento anteriormente concedido para o tratamento dos dados de localização referidos nos números anteriores;
- b) Recusar temporariamente o tratamento desses dados para cada ligação à rede ou para cada transmissão de uma comunicação.

6. O tratamento dos dados de localização deve ser limitado aos trabalhadores e colaboradores das empresas que oferecem redes e ou serviços de comunicações electrónicas acessíveis ao público ou de terceiros que forneçam o serviço de valor acrescentado, devendo restringir-se ao necessário para efeitos da referida actividade.

Artigo 133.º

Facturação detalhada

1. Os assinantes têm o direito de receber facturas não detalhadas.



2. As empresas que oferecem redes e ou serviços de comunicações electrónicas acessíveis ao público devem conciliar os direitos dos assinantes que recebem facturas detalhadas com o direito à privacidade dos utilizadores autores das chamadas e dos assinantes chamados, nomeadamente submetendo à aprovação do Órgão do Governo responsável pela Política de Informática propostas quanto a meios que permitam aos assinantes um acesso anónimo ou estritamente privado a serviços de comunicações electrónicas acessíveis ao público.

3. As chamadas facultadas ao assinante a título gratuito, incluindo chamadas para serviços de emergência ou de assistência, não devem constar da facturação detalhada.

Artigo 134.º

Identificação da linha chamadora e da linha conectada

1. Quando for oferecida a apresentação da identificação da linha chamadora, as empresas que oferecem serviços de comunicações electrónicas acessíveis ao público devem garantir, linha a linha, aos assinantes que efectuem as chamadas e, em cada chamada, aos demais utilizadores a possibilidade de, através de um meio simples e gratuito, impedir a apresentação da identificação da linha chamadora.

2. Quando for oferecida a apresentação da identificação da linha chamadora, as empresas que oferecem serviços de comunicações electrónicas devem garantir ao assinante chamado a possibilidade de impedir, através de um meio simples e gratuito, no caso de uma utilização razoável desta função, a apresentação da identificação da linha chamadora nas chamadas de entrada.

3. Nos casos em que seja oferecida a identificação da linha chamadora antes de a chamada ser atendida, as empresas que oferecem serviços de comunicações electrónicas devem garantir ao assinante chamado a possibilidade de rejeitar, através de um meio simples, chamadas de entrada não identificadas.



4. Quando for oferecida a apresentação da identificação da linha conectada, as empresas que oferecem serviços de comunicações electrónicas devem garantir ao assinante chamado a possibilidade de impedir, através de um meio simples e gratuito, a apresentação da identificação da linha conectada ao utilizador que efectua a chamada.

5. As empresas que oferecem redes e ou serviços de comunicações electrónicas acessíveis ao público são obrigadas a disponibilizar ao público, e em especial aos assinantes, informações transparentes e actualizadas sobre as possibilidades referidas nos números anteriores.

Artigo 135.º

Excepções

1. As empresas que oferecem redes e ou serviços de comunicações electrónicas acessíveis ao público devem, quando tal for compatível com os princípios da necessidade, da adequação e da proporcionalidade, anular por um período de tempo não superior a 30 dias a eliminação da apresentação da linha chamadora, a pedido, feito por escrito e devidamente fundamentado, de um assinante que pretenda determinar a origem de chamadas não identificadas perturbadoras da paz familiar ou da intimidade da vida privada, caso em que o número de telefone dos assinantes chamadores que tenham eliminado a identificação da linha é registado e comunicado ao assinante chamado.

2. Nos casos previstos no número anterior, a anulação da eliminação da apresentação da linha chamadora deve ser precedida de parecer obrigatório por parte do Órgão do Governo responsável pela Política de Informática.

3. As empresas referidas no n.º 1 devem igualmente anular, numa base linha a linha, a eliminação da apresentação da linha chamadora bem como registar e disponibilizar os dados de localização de um assinante ou utilizador, no caso previsto no n.º 2 do artigo 132.º, por forma a disponibilizar esses dados às organizações com competência legal para receber chamadas de emergência para efeitos de resposta a essas chamadas.



4. Nos casos dos números anteriores, deve ser obrigatoriamente transmitida informação prévia ao titular dos referidos dados, sobre a transmissão dos mesmos, ao assinante que os requereu nos termos do n.º 1 ou aos serviços de emergência nos termos do n.º 3.

5. O dever de informação aos titulares dos dados deve ser exercido pelos seguintes meios:

- a) Nos casos do n.º 1, mediante a emissão de uma gravação automática antes do estabelecimento da chamada, que informe os titulares dos dados que, a partir daquele momento e pelo prazo previsto, o seu número de telefone deixa de ser confidencial nas chamadas efectuadas para o assinante que pediu a identificação do número;
- b) Nos casos do n.º 3, mediante a inserção de cláusulas contratuais gerais nos contratos a celebrar entre os assinantes e as empresas que fornecem redes e ou serviços de comunicações electrónicas, ou mediante comunicação expressa aos assinantes nos contratos já celebrados, que possibilitem a transmissão daquelas informações aos serviços de emergência.

6. A existência do registo e da comunicação a que se referem os n.ºs 1 e 3 devem ser objecto de informação ao público e a sua utilização deve ser restringida ao fim para que foi concedida.

Artigo 136.º

Reencaminhamento automático de chamadas

As empresas que oferecem redes e ou serviços de comunicações electrónicas acessíveis ao público devem assegurar aos assinantes a possibilidade de, através de um meio simples e gratuito, interromper o reencaminhamento automático de chamadas efectuado por terceiros para o seu equipamento terminal.



Artigo 137.º

Centrais digitais e analógicas

1. O disposto nos artigos 134.º, 135.º e 136.º é aplicável às linhas de assinante ligadas a centrais digitais e, sempre que tal seja tecnicamente possível e não exija esforço económico desproporcionado, às linhas de assinante ligadas a centrais analógicas.
2. Compete ao Órgão do Governo responsável pela Política de Telecomunicações, enquanto autoridade reguladora nacional, confirmar os casos em que seja tecnicamente impossível ou economicamente desproporcionado cumprir o disposto nos artigos 134.º, 135.º e 136.º do presente título e comunicar esse facto ao Órgão do Governo responsável pela Política de Informática.

Artigo 138.º

Listas de assinantes

1. Os assinantes devem ser informados, gratuitamente e antes da inclusão dos respectivos dados em listas, impressas ou electrónicas, acessíveis ao público ou que possam ser obtidas através de serviços de informação de listas, sobre:
 - a) Os fins a que as listas se destinam;
 - b) Quaisquer outras possibilidades de utilização baseadas em funções de procura incorporadas em versões electrónicas das listas.
2. Os assinantes têm o direito de decidir da inclusão dos seus dados pessoais numa lista pública e, em caso afirmativo, decidir quais os dados a incluir, na medida em que esses dados sejam pertinentes para os fins a que se destinam as listas, tal como estipulado pelo fornecedor.
3. Deve ser garantida aos assinantes a possibilidade de, sem custos adicionais, verificar, corrigir, alterar ou retirar os dados incluídos nas referidas listas.



4. Deve ser obtido o consentimento adicional expresso dos assinantes para qualquer utilização de uma lista pública que não consista na busca de coordenadas das pessoas com base no nome e, se necessário, num mínimo de outros elementos de identificação.

Capítulo III

Regime sancionatório

Artigo 139.º

Contra-ordenação

1. Constitui contra-ordenação punível com a coima mínima de Kz 168.000,00 e máxima de Kz 2.800.000,00:

- a) A não observância das regras de segurança impostas pelo artigo 128.º;
- b) A violação do dever de confidencialidade, a proibição de interceptação ou a vigilância das comunicações e dos respectivos dados de tráfego previstos no artigo 129.º;
- c) A não observância das condições de armazenamento e acesso à informação previstas no artigo 130.º.

2. Constitui contra-ordenação punível com a coima mínima de Kz 56.000,00 e máxima de Kz 2.240.000,00:

- a) A não observância das condições de tratamento e armazenamento de dados de tráfego e de dados de localização previstas nos artigos 131.º e 132.º;
- b) A violação das obrigações previstas nos n.os 1, 2 e 4 do artigo 132.º e nos artigos 134.º a 136.º;
- c) A criação, organização ou actualização de listas de assinantes em violação do disposto no artigo 138.º.

3. Quando praticadas por pessoas colectivas, as contra-ordenações previstas no n.º 1 são puníveis com coimas de Kz 560.000,00 a Kz 550.000.000,00 e as previstas no n.º 2 com coimas de Kz 280.000,00 a Kz 280.000.000,00.



4. A tentativa e a negligência são puníveis.

Artigo 140.º

Processamento e aplicação de coimas

1. Compete ao Órgão do Governo responsável pela Política de Informática a instauração, instrução e arquivamento de processos de contra-ordenação e a aplicação de coimas por violação do disposto no n.º 3 do artigo 129.º, nos artigos 130.º e 131.º, nos n.ºs 1 a 5 do artigo 132.º, nos n.os 2 e 4 do artigo 133.º, nos n.ºs 1 e 2 do artigo 135.º e no artigo 138.º;

2. A instauração e arquivamento de processos de contra-ordenação e a respectiva aplicação de coimas relativos aos restantes ilícitos previstos no artigo anterior são da competência do conselho de administração do Órgão do Governo responsável pela Política de Telecomunicações, cabendo a instrução dos mesmos aos respectivos serviços.

3. O montante das coimas reverte para o Estado em 55 % e para o Órgão do Governo responsável pela Política de Informática em 45 %.

Título V

Protecção Jurídica de Programa de Computador

Capítulo I

Âmbito e Objecto

Artigo 141.º

Âmbito

1. O presente título é relativo à protecção jurídica de programas de computador.

2. Os programas de computador são protegidos nos termos dos direitos de autor conforme definido na Lei n.º 4/90, de 10 de Março, e nos termos de tratados internacionais a que a República de Angola se vincule.



3. Os programas de computador são protegidos unicamente se forem originais, no sentido de serem uma criação intelectual do seu autor.
4. Para efeitos de protecção, equipara-se ao programa de computador o material de concepção preliminar daquele programa.

Artigo 142.º

Objecto

1. A protecção atribuída ao programa de computador incide sobre a sua expressão, sob qualquer forma, salvo aquelas criadas com a intenção de causar danos a um sistema informático.
2. Esta tutela não prejudica a liberdade das ideias e dos princípios que estão na base de qualquer elemento do programa ou da sua interoperabilidade, como a lógica, os algoritmos ou a linguagem de programação.

Capítulo II

Direitos do Autor

Artigo 143.º

Autoria

1. Aplicam-se ao programa de computador as regras sobre autoria e titularidade vigentes para o direito de autor.
2. O programa que for realizado no âmbito de uma empresa presume-se obra colectiva.
3. Quando um programa de computador for criado por um empregado no exercício das suas funções, ou segundo instruções emanadas do dador de trabalho, ou por encomenda, pertencem ao destinatário do programa os direitos a ele relativos, salvo estipulação em contrário ou se outra coisa resultar das finalidades do contrato.



4. As regras sobre atribuição do direito ao programa aplicam-se sem prejuízo do direito a remuneração especial do criador intelectual quando se verificarem os pressupostos do n.º 2 do artigo 16.º da Lei n.º 4/90, de 10 de Março.

Artigo 144.º

Duração

1. O direito atribuído ao criador intelectual sobre a criação do programa extingue-se setenta anos após a sua morte.
2. Se o direito for atribuído originariamente a pessoa diferente do criador intelectual, o direito extingue-se setenta anos após a data em que o programa foi pela primeira vez licitamente publicado ou divulgado.
3. A caducidade do prazo de setenta anos só opera após o dia 1 de Janeiro do ano seguinte àquele em que o prazo se completar.

Artigo 145.º

Actos sujeitos a autorização

O titular do programa pode efectuar ou autorizar:

- a) A reprodução, permanente ou transitória, por qualquer processo ou forma, de todo ou de parte do programa. Se operações como o carregamento, visualização, execução, transmissão ou armazenamento de um programa de computador carecerem dessa reprodução, essas operações têm de ser submetidas a autorização do titular do direito;
- b) A tradução, adaptação, ajustamentos ou outras modificações do programa e a reprodução dos respectivos resultados, sem prejuízo dos direitos de autor da pessoa que altere o programa;



- c) Qualquer forma de distribuição ao público, incluindo a locação, do original ou de cópias de um programa de computador. A primeira comercialização na Comunidade de uma cópia de um programa efectuada pelo titular dos direitos ou realizadas com o seu consentimento extinguirá o direito de distribuição na Comunidade dessa mesma cópia, com excepção do direito de controlar a locação ulterior do programa ou de uma cópia.

Artigo 146.º

Direitos do titular

1. São ainda garantidos ao titular originário do programa o direito à menção do nome no programa e o direito à reivindicação da autoria deste.
2. Se o programa tiver um criador intelectual individualizável, cabe-lhe, em qualquer caso, o direito a ser reconhecido como tal e de ter o seu nome mencionado no programa.

Capítulo III

Direitos do Utente

Artigo 147.º

Direitos do utente

1. Não obstante o disposto no artigo anterior, todo o utente legítimo pode, sem autorização do titular do programa:
 - a) Providenciar uma cópia de apoio no âmbito dessa utilização;
 - b) Observar, estudar ou ensaiar o funcionamento do programa, para determinar as ideias e os princípios que estiverem na base de algum dos seus elementos, quando efectuar qualquer operação de carregamento, visualização, execução, transmissão ou armazenamento.
2. É nula qualquer estipulação em contrário ao disposto no número anterior.



3. O utente legítimo de um programa pode sempre, para utilizar o programa ou para corrigir erros, carregá-lo, visualizá-lo, executá-lo, transmiti-lo e armazená-lo, mesmo se esses actos implicarem operações previstas no n.º 1, salvo estipulação contratual referente a algum ponto específico.

Artigo 148.º

Descompilação

1. Não é necessária a autorização do titular dos direitos de autor quando a reprodução do Código e a tradução da sua forma, na acepção das alíneas a) e b) do artigo 145.º, forem indispensáveis para obter as informações necessárias à interoperabilidade de um programa de computador criado independentemente, com outros programas, uma vez preenchidas as seguintes condições:

- a) Esses actos serem realizados pelo licenciado ou por outra pessoa que tenha o direito de utilizar uma cópia do programa, ou em seu nome por uma pessoa devidamente autorizada para o efeito;
- b) Não se encontrarem já fácil e rapidamente à disposição das pessoas referidas na alínea a) as informações necessárias à interoperabilidade;
- c) Esses actos limitarem-se a certas partes do programa de origem necessárias à interoperabilidade.

2. O disposto no n.º 1 não permite que as informações obtidas através da sua aplicação:

- a) Sejam utilizadas para outros fins que não o de assegurar a interoperabilidade de um programa criado independentemente;
- b) Sejam transmitidas a outrem, excepto quando tal for necessário para a interoperabilidade do programa criado independentemente; ou
- c) Sejam utilizadas para o desenvolvimento, produção ou comercialização de um programa substancialmente semelhante na sua expressão, ou para qualquer outro acto que infrinja os direitos de autor.



3. As disposições do presente artigo não podem ser interpretadas no sentido de permitirem a sua aplicação de uma forma susceptível de lesar os legítimos interesses do titular de direitos ou que não se coadune com a exploração normal de um programa de computador.

Capítulo IV

Disposições Comuns

Artigo 149.º

Limites

1. Sempre que forem compatíveis, são aplicáveis aos programas de computador os limites estabelecidos para o direito de autor, nomeadamente os constantes do artigo 29.º da Lei n.º 4/90, de 10 de Março, mas o uso privado só será admitido nos termos do presente diploma.
2. É livre a análise de programas como objecto de pesquisa científica ou de ensino.

Artigo 150.º

Autonomia privada

1. Os negócios relativos a direitos sobre programas de computador são disciplinados pelas regras gerais dos contratos e pelas disposições dos contratos típicos em que se integram ou com que ofereçam maior analogia.
2. As estipulações contratuais são sempre entendidas de maneira conforme à boa fé e com o âmbito justificado pelas finalidades do contrato.



Capítulo V

Disposições Finais e Transitórias

Artigo 151.º

Apreensão

1. Aplicam-se à apreensão de cópias ilícitas de programas de computador as disposições relativas à apreensão de exemplares contrafeitos em matéria de direito de autor.
2. Podem igualmente ser apreendidos dispositivos em comercialização que tenham por finalidade exclusiva facilitar a supressão não autorizada ou a neutralização de qualquer salvaguarda técnica eventualmente colocada para proteger um programa de computador.
3. O destino dos objectos apreendidos será determinado na sentença final.

Artigo 152.º

Tutela penal

1. Um programa de computador é penalmente protegido contra a reprodução não autorizada.
2. É aplicável ao programa de computador o disposto no artigo 186.º do Título VII da presente lei.

Artigo 153.º

Tutela por outras disposições legais

A tutela instituída pelo presente título não prejudica a vigência de regras de diversa natureza donde possa resultar uma protecção do programa, como as emergentes da disciplina dos direitos de patente, marcas, concorrência desleal, segredos comerciais e das topografias dos semicondutores ou do direito dos contratos.



Artigo 154.º

Vigência

1. A protecção dos programas de computador inicia-se na data da entrada em vigor do presente diploma, mas os programas anteriormente criados são protegidos durante o tempo que gozariam ainda de protecção se esta lei fosse já vigente ao tempo da sua criação.
2. A aplicação do presente diploma não prejudica os contratos concluídos nem os direitos adquiridos antes da sua entrada em vigor, mas as regras sobre a invalidade das estipulações aplicam-se também a estes contratos.

Artigo 155.º

Tutela internacional

1. A tutela internacional é subordinada à reciprocidade material.
2. Na medida em que assim for estabelecido por convenção internacional, aplica-se o princípio do tratamento nacional.
3. Os programas que nos países de origem respectivos tiverem tombado no domínio público não voltam a ser protegidos.
4. É considerado autor quem assim for qualificado pela lei do país de origem respectivo; em caso de colisão de qualificações aplica-se a lei que se aproxime mais da lei angolana.



Título VI Protecção Jurídica de Bases de Dados

Capítulo I Objecto e âmbito de aplicação

Artigo 156.º

Objecto

1. O presente título é relativo à protecção jurídica das bases de dados.
2. Para efeitos do disposto no presente título, entende-se por «**base de dados**» a colectânea de obras, dados ou outros elementos independentes, dispostos de modo sistemático ou metódico e susceptíveis de acesso individual por meios electrónicos ou outros.
3. As bases de dados são protegidas pelo direito de autor.
4. A protecção atribuída às bases de dados não é extensiva aos programas de computador utilizados no fabrico ou no funcionamento de bases de dados acessíveis por meios electrónicos.

Artigo 157.º

Situações plurilocalizadas

1. Sem prejuízo do disposto em convenção internacional a que a República de Angola esteja vinculada, a protecção das bases de dados pelo direito de autor está sujeita ao país da sua origem, considerando-se como tal:
 - a) Quanto às bases de dados publicadas, o país da primeira publicação;
 - b) Quanto às bases de dados não publicadas, o país da nacionalidade do autor ou, tratando-se de pessoa colectiva, o da sede principal e efectiva da sua administração.



2. Não é, porém, reconhecida às bases de dados de origem estrangeira a protecção que, sendo atribuída pelo respectivo Estado às bases de dados de origem nacional, o não seja às bases de dados de origem angolana em igualdade de circunstâncias.
3. A referência a uma lei estrangeira, nos termos do n.º 1, entende-se com exclusão das suas normas de direito internacional privado.
4. É considerado autor quem como tal for qualificado pela lei do país de origem da base de dados, determinada nos termos do n.º 1, prevalecendo, em caso de conflito de qualificações, a lei do país cuja solução mais se aproxime da lei angolana.

Capítulo II

Direito de autor

Artigo 158.º

Protecção pelo direito de autor

1. As bases de dados que, pela selecção ou disposição dos respectivos conteúdos, constituam criações intelectuais são protegidas em sede de direito de autor.
2. O disposto no número anterior constitui o único critério determinante para a protecção pelo direito de autor.
3. A tutela das bases de dados pelo direito de autor não incide sobre o seu conteúdo e não prejudica eventuais direitos que subsistam sobre o mesmo.

Artigo 159.º

Autoria

1. São aplicáveis às bases de dados referidas no artigo anterior as regras gerais sobre autoria e titularidade vigentes para o direito de autor.



2. Presumem-se obras colectivas as bases de dados criadas no âmbito de uma empresa.
3. Os direitos patrimoniais sobre as bases de dados criadas por um empregado no exercício das suas funções, ou segundo instruções emanadas do dador de trabalho, ou criadas por encomenda, pertencem ao destinatário da base de dados, salvo se o contrário resultar de convenção das partes ou da finalidade do contrato.
4. O disposto no número anterior não prejudica o direito de remuneração especial do criador intelectual nos casos e nos termos previstos no n.º 2 do artigo 16.º da Lei n.º 4/90, de 10 de Março.

Artigo 160.º

Duração

1. O direito sobre a base de dados atribuído ao criador intelectual extingue-se setenta anos após a morte deste.
2. O prazo de protecção da base de dados atribuído originariamente a outras entidades extingue-se setenta anos após a primeira divulgação ao público da mesma.
3. A caducidade do prazo de setenta anos só opera após o dia 1 de Janeiro do ano seguinte àquele em que o prazo se completar.

Artigo 161.º

Conteúdo do direito de autor

1. O titular de uma base de dados criativa goza do direito exclusivo de efectuar ou autorizar:
 - a) A reprodução permanente ou transitória, por qualquer processo ou forma, de toda ou parte da base de dados;
 - b) A tradução, a adaptação, a transformação, ou qualquer outra modificação da base de dados;



- c) A distribuição do original ou de cópias da base de dados;
- d) Qualquer comunicação pública, exposição ou representação públicas da base de dados;
- e) Qualquer reprodução, distribuição, comunicação, exposição ou representação pública da base de dados derivada, sem prejuízo dos direitos de quem realiza a transformação.

Artigo 162.º

Direitos do titular

1. O titular originário da base de dados goza do direito à menção do nome na base e do direito de reivindicar a autoria desta.
2. Se a base de dados tiver um criador intelectual individualizável, cabe-lhe, em qualquer caso, o direito a ser reconhecido como tal e de ter o seu nome mencionado na base.

Artigo 163.º

Direitos do utente

1. O utente legítimo pode, sem autorização do titular da base de dados e do titular do programa, praticar os actos previstos no artigo 159.º com vista ao acesso à base de dados e à sua utilização, na medida do seu direito.
2. É nula a convenção em contrário ao disposto no número anterior.

Artigo 164.º

Excepções

1. Em derrogação dos direitos previstos no artigo 161.º, são ainda livres os seguintes actos:
 - a) A reprodução para fins privados de uma base de dados não electrónica;
 - b) As utilizações feitas com fins didácticos ou científicos, desde que se indique a fonte, na medida em que isso se justifique pelo objectivo não comercial a prosseguir;



- c) As utilizações para fins de segurança pública ou para efeitos de processo administrativo ou judicial;
- d) As restantes utilizações livres previstas no direito de autor nacional, nomeadamente as constantes do artigo 29.º da Lei n.º 4/90, de 1 de Março.

2. As reproduções permitidas no número anterior e as previstas no artigo 163.º devem ser efectuadas de forma a não prejudicar a exploração normal da base de dados nem causar um prejuízo injustificável aos legítimos interesses do autor.

Artigo 165.º

Reprodução, divulgação ou comunicação ilegítima de base de dados protegida

Quem, não estando para tanto autorizado, reproduzir, divulgar ou comunicar, ao público com fins comerciais, uma base de dados criativa nos termos n.º 1 do artigo 158.º, é punido com pena de prisão até 3 anos ou com pena de multa.

Capítulo III

Protecção especial do fabricante da base de dados

Artigo 166.º

Direito especial do fabricante

1. Quando a obtenção, verificação ou apresentação do conteúdo de uma base de dados represente um investimento substancial do ponto de vista qualitativo ou quantitativo, o seu fabricante goza do direito de autorizar ou proibir a extracção e ou a reutilização da totalidade ou de uma parte substancial, avaliada qualitativa ou quantitativamente, do seu conteúdo.

2. Para os efeitos do disposto no presente diploma, entende-se por:

- a) Extracção: a transferência, permanente ou temporária, da totalidade ou de uma parte substancial do conteúdo de uma base de dados para outro suporte, seja por que meio ou sob que forma for;



- b) Reutilização: qualquer forma de distribuição ao público da totalidade ou de uma parte substancial do conteúdo da base de dados, nomeadamente através da distribuição de cópias, aluguer, transmissão em linha ou outra modalidade.

3. O comodato público não constitui um acto de extracção ou de reutilização.

4. O direito previsto no n.º 1 é aplicável independentemente de a base de dados ou o seu conteúdo poderem ser protegidos pelo direito de autor ou por outros direitos.

5. Não são permitidas a extracção e ou a reutilização sistemáticas de partes não substanciais do conteúdo da base de dados que pressuponham actos contrários à exploração normal dessa base ou que possam causar um prejuízo injustificado aos legítimos interesses do fabricante da base.

Artigo 167.º

Transmissão do direito do fabricante

O direito do fabricante, previsto no n.º 1 do artigo anterior, pode ser transmitido ou objecto de licenças contratuais.

Artigo 168.º

Direitos e obrigações do utilizador legítimo

1. O utilizador legítimo de uma base de dados colocada à disposição do público pode praticar todos os actos inerentes à utilização obtida, nomeadamente os de extrair e de reutilizar as partes não substanciais do respectivo conteúdo, na medida do seu direito.

2. O utilizador legítimo de uma base de dados colocada à disposição do público não pode praticar quaisquer actos anómalos que colidam com a exploração normal desta e lesem injustificadamente os legítimos interesses do fabricante ou prejudiquem os titulares de direitos de autor ou de direitos conexos sobre obras e prestações nela incorporadas.

3. É nula qualquer convenção em contrário ao disposto nos números anteriores.



Artigo 169.º

Outros actos livres

O utilizador legítimo de uma base de dados colocada à disposição do público pode ainda, sem autorização do fabricante, extrair e ou reutilizar uma parte substancial do seu conteúdo nos seguintes casos:

- a) Sempre que se trate de uma extracção para uso privado do conteúdo de uma base de dados não electrónica;
- b) Sempre que se trate de uma extracção para fins didácticos ou científicos, desde que indique a fonte e na medida em que a finalidade não comercial o justifique;
- c) Sempre que se trate de uma extracção e ou de uma reutilização para fins de segurança pública ou para efeitos de um processo administrativo ou judicial.

Artigo 170.º

Prazo de protecção

1. O direito previsto no artigo 166.º produz efeitos a partir da conclusão do fabrico da base de dados e caduca ao fim de 15 anos, a contar de 1 de Janeiro do ano seguinte ao da data do seu fabrico.

2. No caso de uma base de dados que tenha sido colocada à disposição do público antes do decurso do prazo previsto no número anterior, o prazo de protecção daquele direito caduca ao fim de 15 anos a contar de 1 de Janeiro do ano seguinte àquele em que a base de dados tiver sido colocada pela primeira vez à disposição do público.



Artigo 171.º

Protecção de modificações substanciais

Qualquer modificação substancial, avaliada quantitativa ou qualitativamente, do conteúdo de uma base de dados, incluindo as modificações substanciais resultantes da acumulação de aditamentos, supressões ou alterações sucessivas que levem a considerar que se trata de um novo investimento substancial, atribui à base de dados resultante desse investimento um período de protecção própria.

Capítulo IV

Disposições comuns

Artigo 172.º

Autonomia privada

1. Os negócios relativos a direitos sobre bases de dados são disciplinados pelas regras gerais dos contratos e pelas disposições dos contratos típicos em que se integram ou com que ofereçam maior analogia.
2. São aplicáveis a estes negócios as disposições do artigo 19.º da Lei n.º 4/90, de 10 de Março.

Artigo 173.º

Apreensão

1. Podem ser apreendidas, nos termos dos procedimentos cautelares, as cópias ilícitas de bases de dados.
2. Podem igualmente ser objecto de apreensão os dispositivos em comercialização que tenham por finalidade exclusiva facilitar a supressão não autorizada ou a neutralização de qualquer salvaguarda técnica eventualmente colocada para proteger uma base de dados.
3. O destino dos objectos apreendidos será determinado na sentença final.



Capítulo V

Disposições finais e transitórias

Artigo 174.º

Tutela por outras disposições legais

1. A tutela instituída pelo presente título não prejudica a conferida por regras de diversa natureza relativas, nomeadamente, ao direito de autor ou a quaisquer outros direitos ou obrigações que subsistam sobre os dados, obras, prestações ou outros elementos incorporados numa base de dados, às patentes, às marcas, aos desenhos e modelos, à protecção dos tesouros nacionais, à legislação sobre acordos, às decisões ou práticas concertadas entre empresas e à concorrência desleal, ao segredo comercial, à segurança, à confidencialidade, à protecção dos dados pessoais e da vida privada, ao acesso aos documentos públicos ou ao direito dos contratos.
2. A protecção conferida pelo presente diploma às bases de dados realiza-se sem prejuízo da aplicação das disposições do título anterior da Lei n.º 8/01, de 11 de Maio.

Artigo 175.º

Aplicação no tempo

1. O prazo previsto no artigo 160.º aplica-se às bases criadas antes da data de entrada em vigor do presente diploma, desde que o mesmo não tenha ainda decorrido.
2. As bases de dados que na data de entrada em vigor do presente diploma sejam protegidas pelo direito de autor não verão diminuir o seu prazo de protecção ainda que não preencham os requisitos do n.º 1 do artigo 158.º
3. A protecção prevista no artigo 166.º para os fabricantes aplica-se igualmente às bases de dados cujo fabrico foi concluído durante os 15 anos anteriores à entrada em vigor deste diploma, contando-se o seu prazo de protecção a partir do dia 1 de Janeiro do ano seguinte ao da conclusão da base de dados.



Artigo 176.º

Contratos

As disposições do n.º 2 do artigo 163.º e do n.º 3 do artigo 168.º aplicam-se aos contratos já concluídos, sem prejuízo da manutenção dos mesmos bem como dos direitos adquiridos antes da entrada em vigor do presente diploma.

Título VII

Criminalidade Informática

Capítulo I

Disposições Gerais

Artigo 177.º

Direito Subsidiário

Aos crimes previstos no presente título são subsidiariamente aplicáveis as disposições do Código Penal.

Artigo 178.º

Definições

Para os fins do presente título, a expressão:

- a) **«Rede Informática»** designa um conjunto de dois ou mais computadores interconectados;
- b) **«Sistema Informático»** designa qualquer dispositivo isolado, ou conjunto de dispositivos interligados ou relacionados, que assegure ou do qual um ou mais elementos assegurem, em conformidade com um programa, o tratamento automatizado dos dados;
- c) **«Dados Informáticos»** designa qualquer representação de factos, informações ou conceitos sob uma forma que se preste ao tratamento num computador, incluindo um programa adequado para fazer um sistema informático executar determinada função;



- d) «**Programa Informático**» designa um conjunto de instruções capazes, quando inseridas num suporte explorável em máquina, de permitir à máquina que tem por funções o tratamento de informações, indicar, executar ou produzir determinada função, tarefa ou resultado;
- e) «**Topografia**» designa uma série de imagens entre si ligadas, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho ou parte dele de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico;
- f) «**Produto Semicondutor**» designa a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutores, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica;
- g) «**Intercepção**» designa o acto destinado a captar informações contidas num sistema automatizado de dados, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros;
- h) «**Pornografia Infantil**» inclui qualquer material pornográfico que represente de forma visual: 1) Um menor envolvido num comportamento sexual explícito; 2) Uma pessoa que aparece com um menor envolvido num comportamento sexual explícito. As gravações auditivas de carácter pornográfico que envolvam menores são igualmente consideradas como pornografia infantil;
- i) «**Material pornográfico simulado**» designa imagens realistas representando um menor envolvido num comportamento sexual explícito;
- j) «**Menor**» designa qualquer pessoa com idade inferior a 18 (dezoito) anos;
- k) «**Racismo ou Material Xenófobo**» designa qualquer documento escrito, qualquer imagem ou qualquer outra representação de ideias ou teorias, que defenda, promova ou incite ao ódio, à discriminação ou à violência, contra quaisquer indivíduos ou grupos de indivíduos, baseado na raça, cor, descendência, nacionalidade ou origem étnica ou religiosa;



- l) «**Dispositivo Ilícito**» designa um equipamento ou programa informático concebido ou adaptado com vista a permitir o acesso a um sistema ou rede informática, sob forma inteligível, sem autorização do proprietário do sistema ou rede informática;
- m) «**Valor elevado**» é aquele que exceder 10.000 Unidades de Correção Fiscal avaliados no momento da prática do facto;
- n) «**Valor consideravelmente elevado**» é aquele que excede 40.000 Unidades de Correção Fiscal avaliados no momento da prática do facto.

Artigo 179.º

Responsabilidade Penal das Pessoas Colectivas e Equiparadas

1. As pessoas colectivas, sociedades e meras associações de facto são penalmente responsáveis pelos crimes previstos na lei, quando cometidos em seu nome e ou no interesse colectivo pelos seus órgãos ou representantes.
2. A responsabilidade é excluída quando o agente tiver actuado contra a ordens ou instruções expressas de quem de direito.
3. A responsabilidade das entidades referidas no n.º 1 não exclui a responsabilidade individual dos respectivos agentes.
4. As entidades referidas no antigo anterior n.º 1 respondem solidariamente, nos termos da lei civil, pelo pagamento das multas, indemnizações e outras prestações a que forem condenados ao abrigo da presente lei.



Capítulo II

Dos Crimes ligados à Informática

Secção I

Crimes relativos à Confidencialidade, Integridade e Disponibilidade de Dados e Sistemas Informáticos

Artigo 180.º

Acesso Ilegítimo

1. Quem, não estando para tanto autorizado, e qualquer modo aceder a todo ou parte de um sistema ou rede informáticos será punido com pena de prisão até dois anos ou com pena de multa correspondente.
2. A pena será a de prisão até três anos ou multa se o acesso for conseguido através de violação de regras de segurança.
3. A pena será a de prisão de dois a cinco anos quando:
 - a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados classificados, protegidos por lei;
 - b) Se existir um benefício ou vantagem patrimonial.
4. A tentativa é punível.
5. Nos casos previstos nos n.º 1, 2 e 3 o procedimento penal depende de queixa.



Artigo 181.º

Intercepção Ilegítima

1. Aquele que, sem para tanto estar autorizado, e através de meios técnicos, interceptar comunicações não públicas de dados informáticos que se processam no interior de um sistema ou rede informáticos, a eles destinadas ou deles provenientes, será punido com pena de prisão até dois anos ou com pena de multa correspondente.
2. A tentativa é punível.
3. Nos casos previstos no nºs 1 e 2 o procedimento penal depende de queixa.

Artigo 182.º

Sabotagem Informática

1. Aquele que introduzir, alterar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir em sistema informático, actuando com intenção de entravar ou perturbar o funcionamento de um sistema informático ou de comunicação de dados à distância, será punido com pena de prisão até cinco anos ou com pena de multa até seiscentos dias.
2. A pena será a de prisão de um a cinco anos se o dano emergente da perturbação for de valor elevado.
3. A pena será a de prisão de um a dez anos se o dano emergente da perturbação for de valor consideravelmente elevado.



Artigo 183.º

Dano relativo a dados ou programas informáticos

1. Aquele que, de forma indevida ou sem para tanto estar autorizado, e actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo para si ou para terceiros, apagar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis dados ou programas informáticos alheios ou, por qualquer forma, lhes afectar a capacidade de uso será punido com pena de prisão até três anos ou pena de multa.
2. A tentativa é punível.
3. Se o dano causado for de valor elevado, a pena será a de prisão até cinco anos ou de multa até seiscentos dias.
4. Se o dano causado for de valor consideravelmente elevado, a pena será a de prisão de um a dez anos.
5. Nos casos previstos nos n.º 1, 2 e 3 o procedimento penal depende da queixa.

Artigo 184.º

Dispositivos Ilícitos

1. Quem, não estando para tanto autorizado, e com intenção de cometer os crimes previstos no presente título, produzir, vender, obter para utilização, importação, difusão ou por qualquer outra forma disponibilizar:
 - a) Um dispositivo, incluindo um programa informático, concebido ou adaptado de forma a através da sua utilização cometer um dos crimes previstos no presente título;



- b) Uma palavra passe, um código de acesso ou dados informáticos similares que permitem aceder a todo, ou a uma parte, de um sistema ou rede informática com a intenção de o usar a fim de cometer um dos crimes previstos no presente título;

Será punido com pena de prisão até três anos ou com pena de multa.

2. A tentativa é punível.

3. O procedimento criminal depende de queixa.

Secção II

Crimes Informáticos

Artigo 185.º

Falsificação Informática

1. Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados ou programas informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados, quando esses dados ou programas sejam susceptíveis de servirem como meio de prova, de tal modo que a sua visualização produza os mesmos efeitos de um documento falsificado, ou, bem assim, os utilize para os fins descritos, será punido com pena de prisão até cinco anos ou multa de cento e vinte a seiscientos dias.

2. Nas mesmas penas incorre quem use documento produzido a partir de dados ou programas informatizados que foram objecto dos actos referidos no número anterior, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiros.

3. Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de um a cinco anos.



Artigo 186.º

Reprodução ilegítima de programa protegido

1. Quem, não estando para tanto autorizado, proceder à reprodução, fixação, divulgação ou comunicação ao público um programa informático protegido por lei será punido com pena de prisão até três anos ou com pena de multa.
2. Na mesma pena incorre quem ilegítimamente reproduzir topografia de um produto semiconductor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semiconductor fabricado a partir dessa topografia.
3. A tentativa é punível.

Secção III

Crimes Relacionados com o Conteúdo

Artigo 187.º

Difusão de pornografia infantil através de sistema ou rede informática

1 – Quem:

- a) Produzir pornografia infantil para difusão através de um sistema ou rede informática;
- b) Oferecer ou disponibilizar pornografia infantil através de um sistema ou rede informática;
- c) Difundir ou transmitir pornografia infantil através de um sistema ou rede informática;

É punido com pena de prisão até 5 anos.

2. Quem praticar os actos descritos no número anterior relativamente a menor entre 14 e 18 anos é punido com pena de prisão até três anos.



3. Quem praticar os actos descritos no n.º 1 utilizando material pornográfico simulado ou manipulado de menor não existente é punido com pena de prisão até dois anos.
4. Quem praticar os actos descritos no n.º 1 com intenção lucrativa é punido com pena de prisão de um a oito anos.
5. Quem praticar os actos descritos no n.º 2 com intenção lucrativa é punido com pena de prisão de seis meses a cinco anos.
6. Quem adquirir ou detiver os materiais previstos no n.º 1 é punido com pena de prisão até um ano ou com pena de multa.
7. A tentativa é punível.

Artigo 188.º

Difusão de conteúdos racistas ou xenófobos através de sistema ou rede informática

1. Quem, com intenção de incitar ao ódio, à discriminação ou à violência:
 - a) Produzir conteúdos racistas ou xenófobos para difusão através de um sistema ou rede informática;
 - b) Oferecer ou disponibilizar conteúdos racistas ou xenófobos através de um sistema ou rede informática;
 - c) Difundir ou transmitir conteúdos racistas ou xenófobos através de um sistema ou rede informática;

É punido com pena de prisão até 3 anos ou com pena de multa correspondente.

2. Quem adquirir ou detiver os materiais previstos no n.º 1 é punido com pena de prisão até um ano ou com pena de multa correspondente.



3. A tentativa é punível.

Capítulo III

Penas

Artigo 189.º

Penas aplicáveis às pessoas colectivas e equiparadas

1. Pelos crimes previstos na presente lei são aplicáveis às pessoas colectivas e equiparadas as seguintes penas principais:

- a) Admoestação;
- b) Multa;
- c) Dissolução.

2. Aplica-se a pena de admoestação sempre que, nos termos gerais, tal pena possa ser aplicada à pessoa singular que, em representação e no interesse da pessoa colectiva ou equiparada, tiver praticado o facto.

3. Quando aplicar a pena de admoestação, o tribunal poderá aplicar cumulativamente a pena acessória de caução de boa conduta.

4. Cada dia de multa corresponde a uma quantia entre Kz 5.600,00 e Kz 112.000,00 que o tribunal fixará em função da situação económica e financeira da pessoa colectiva ou equiparada e dos seus encargos.

5. Se a multa for aplicada a uma entidade sem personalidade jurídica, responderá por ela o património comum e, na sua falta ou insuficiência, o património de cada um dos associados.



6. A pena de dissolução só será aplicada quando os titulares dos órgãos ou representantes da pessoa colectiva ou sociedade tenham agido com a intenção, exclusiva ou predominantemente, de, por meio dela, praticar os factos que integram os crimes previstos na presente lei ou quando a prática reiterada desses factos mostre que a pessoa colectiva ou sociedade está a ser utilizada para esse efeito, quer pelos seus membros, quer por quem exerça a respectiva administração.

Artigo 190.º

Penas acessórias

Relativamente aos crimes previstos no presente diploma, podem ser aplicadas as seguintes penas acessórias:

- a) Perda de bens;
- b) Caução de boa conduta;
- c) Interdição temporária do exercício de certas actividades ou profissões;
- d) Encerramento temporário do estabelecimento;
- e) Encerramento definitivo do estabelecimento;
- f) Publicidade da decisão condenatória.

Artigo 191.º

Perda de bens

1. O tribunal pode decretar a perda dos materiais, equipamentos ou dispositivos pertencentes à pessoa condenada que tiverem servido para a prática dos crimes previstos no presente diploma.
2. A perda de bens abrange o lucro ilícito obtido com a prática da infracção.
3. Se o tribunal apurar que o agente adquiriu determinados bens, empregando na sua aquisição dinheiro ou valores obtidos com a prática do crime, serão os mesmos também abrangidos pela decisão que decretar a perda.



Artigo 192.º

Caução de boa conduta

1. A caução de boa conduta implica a obrigação de o agente depositar uma quantia em dinheiro, a fixar entre Kz 5.600,00 e Kz 560.000,00, à ordem do tribunal, pelo prazo fixado na decisão condenatória, por um período entre seis meses e dois anos.
2. A caução de boa conduta deve, em regra, ser aplicada sempre que o tribunal condene em pena cuja execução declare suspensa.
3. A caução será declarada perdida a favor do Estado se o agente praticar, por meio de informática, nova infracção no período fixado na sentença, pela qual venha a ser condenado, sendo-lhe restituída no caso contrário.

Artigo 193.º

Interdição temporária do exercício de certas actividades ou profissões

1. A interdição temporária do exercício de certas actividades ou profissões pode ser decretada quando a infracção tiver sido cometida com flagrante e manifesto abuso da profissão ou no exercício de actividade que dependa de um título público ou de uma autorização ou homologação da autoridade pública.
2. A duração da interdição tem um mínimo de dois meses e um máximo de dois anos.
3. Incorre na pena do crime de desobediência qualificada quem, por si ou por interposta pessoa, exercer a profissão ou actividade durante o período da interdição.



Artigo 194.º

Encerramento temporário do estabelecimento

1. O encerramento temporário do estabelecimento pode ser decretado por um período mínimo de um mês e máximo de um ano, quando o agente tiver sido condenado em pena de prisão superior a seis meses ou em pena de multa superior a cem dias.
2. Não obstam à aplicação desta pena a transmissão do estabelecimento ou a cedência de direitos de qualquer natureza, relacionados com o exercício da profissão ou actividade, efectuados após a instauração do processo ou depois de cometida a infracção, salvo se, neste último caso, o adquirente se encontrar de boa fé.
3. O encerramento do estabelecimento nos termos do n.º 1 não constitui justa causa para o despedimento de trabalhadores nem fundamento para a suspensão ou redução do pagamento das respectivas remunerações.

Artigo 195.º

Encerramento definitivo do estabelecimento

1. O encerramento definitivo do estabelecimento pode ser decretado quando o agente:
 - a) Tiver sido anteriormente condenado por infracção prevista neste diploma em pena de prisão ou multa, se as circunstâncias mostrarem que a condenação ou condenações anteriores não constituíram suficiente prevenção contra o crime;
 - b) Tiver anteriormente sido condenado em pena de encerramento temporário;
 - c) For condenado em pena de prisão por infracção prevista neste diploma, que tenha determinado dano de valor consideravelmente elevado ou para um número avultado de pessoas.
2. Aplicam-se ao encerramento definitivo as disposições dos n.º 2 e 3 do artigo anterior.



Artigo 196.º

Publicidade da decisão

1. Quando o tribunal aplicar a pena de publicidade, será esta efectivada, a expensas do condenado, em publicação periódica editada na área de jurisdição da prática da infracção ou, na sua falta, em publicação da área de jurisdição mais próxima, bem como através da afixação de edital, por período não inferior a 30 dias, no próprio estabelecimento ou no local do exercício da actividade, por forma bem visível pelo público.
2. Em casos particularmente graves, nomeadamente quando a infracção importe lesão de interesses não circunscritos a determinada área do território, o tribunal poderá ordenar, também a expensas do condenado, que a publicidade da decisão seja feita no Diário da República ou através de qualquer meio de comunicação social.
3. A publicidade da decisão condenatória é feita por extracto, do qual constem os elementos da infracção e as sanções aplicáveis, bem como a identificação dos agentes.

Capítulo IV

Disposições Finais

Artigo 197.º

Processo de liquidação

1. Transitada em julgado a decisão que aplicar a pena de dissolução, o Ministério Público requer a liquidação do património, observando-se, com as necessárias adaptações, o processo previsto na lei para a liquidação de patrimónios.
2. O processo de liquidação corre no tribunal da condenação e por apenso ao processo principal.
3. Os liquidatários são sempre nomeados pelo juiz.



4. O Ministério Público requer as providências cautelares que se mostrem necessárias para garantir a liquidação.

Artigo 198.º
Entrada em Vigor

A presente lei entra em vigor no dia seguinte ao da sua publicação.