Quinta-feira, 16 de Fevereiro de 2017 I Série – N.º 27

DIÁRIO DA REPÚBLICA

ÓRGÃO OFICIAL DA REPÚBLICA DE ANGOLA

Preço deste número - Kz: 220,00

Toda a correspondência, quer oficial, quer relativa a anúncio e assinaturas do «Diário da República», deve ser dirigida à Imprensa Nacional - E.P., em Luanda, Rua Henrique de Carvalho n.º 2, Cidade Alta, Caixa Postal 1306, www.imprensanacional.gov.ao - End. teleg.: «Imprensa».

ASSINATURA

	Ano
As três séries	Kz: 611 799.50
A 1.ª série	Kz: 361 270.00
A 2.ª série	Kz: 189 150.00
A 3.ª série	Kz: 150 111.00

O preço de cada linha publicada nos Diários da República 1.ª e 2.ª série é de Kz: 75.00 e para a 3.ª série Kz: 95.00, acrescido do respectivo imposto do selo, dependendo a publicação da 3.ª série de depósito prévio a efectuar na tesouraria da Imprensa Nacional - E. P.

SUMÁRIO

ASSEMBLEIA NACIONAL

Lei n.º 7/17

de 16 de Fevereiro

A presente Lei visa responder, de forma eficaz e eficiente, aos novos desafios da sociedade da informação, à protecção da utilização do espaço cibernético angolano contra os riscos a eles associados e promover a inclusão digital;

Pretende-se, ainda, com a presente Lei, melhorar a oferta da prestação de serviços digitais, o acesso dos cidadãos à informação e ao conhecimento.

A Assembleia Nacional aprova, por mandato do povo, nos termos das disposições combinadas da alínea b) do artigo 161.º, do n.º 2 do artigo 165.º e da alínea d) do n.º 2 do artigo 166.º, todos da Constituição da República de Angola, a seguinte:

LEI DE PROTECÇÃO DAS REDES E SISTEMAS INFORMÁTICOS

CAPÍTULO I

Disposições Gerais

ARTIGO 1.º

(Objecto)

A presente Lei tem como objecto estabelecer o regime jurídico sobre as medidas de protecção das redes e sistemas informáticos.

ARTIGO 2.º

(Âmbito de aplicação)

1. A presente Lei aplica-se ao ciberespaço da República de Angola, contra qualquer acto de ataque, roubo informático, ciber-ataque e incidentes informáticos.

2. Sem prejuízo do disposto do número anterior e do disposto no Código Penal, a presente Lei é aplicável aos factos:

a) Cometidos em território nacional por cidadãos angolanos, estrangeiros ou por pessoa colectiva com domicílio em território angolano, que visem o ciberespaço ou dados informáticos;

b) Praticados fisicamente, total ou parcialmente, em território angolano, ainda que visem sistemas de informação ou dados localizados fora desse território;

c) Praticados no ciberespaço ou dados localizados em território angolano, independentemente do local onde esses factos forem fisicamente praticados;

d) Cometidos por cidadãos estrangeiros não residentes em território angolano, que visem o ciberespaço ou dados informáticos.

3. O disposto na Secção II e III do Capítulo III aplica-se aos operadores de comunicações electrónicas acessíveis ao público e aos prestadores de armazenagem principal, estabelecidos em território nacional.

ARTIGO 3.º
(Regime jurídico subsidiário)

O regime jurídico constante da presente Lei não prejudica:

a) O disposto nas normas constantes dos Tratados e das Convenções Internacionais, continentais e regionais vigentes na ordem jurídica nacional;

b) O disposto em legislação vigente que seja compatível com a presente Lei, nomeadamente:

i) O regime jurídico de protecção de dados pessoais;

ii) O regime jurídico das tecnologias e dos serviços da sociedade da informação;

iii) O regime jurídico das comunicações electrónicas e dos serviços da sociedade da informação.

ARTIGO 4.º
(Definições)

Para efeitos da presente Lei, considera-se:

a) «*Acesso condicional*» — A sujeição do acesso de um serviço a uma assinatura ou qualquer outra forma de autorização prévia individual;

b) «*Assinante*» — A pessoa singular ou colectiva que é parte num contrato com um operador de comunicações electrónicas acessíveis ao público;

c) «*Base de dados*» — As colectâneas de obras, dados ou outros elementos independentes, dispostos de modo sistemático ou metódico e susceptíveis de acesso individual por meios electrónicos ou outros;

d) «*CERT*» — Centro de Estudos, Respostas e Tratamento de incidentes informáticos;

e) «*Ciber-Ataque*» — O ataque efectuado geralmente através da *Internet*, no qual são violados sistemas informáticos, com o objectivo de espiar, provocar danos, roubar dados;

f) «*Ciberespaço*» — O conjunto dos sistemas tecnológicos e infra-estruturas de redes telemáticas, bem como do conjunto de informações e serviços da *Internet*;

g) «*Cibercrime*» — O crime cometido com o recurso aos sistemas electrónicos e as novas tecnologias de informação e comunicação;

h) «*Cibersegurança*» — A segurança relacionada com o ciberespaço;

i) «*Código de acesso*» — Dado ou senha que permite aceder, no todo ou em parte e sob forma inteligível, à um sistema de informação;

j) «*Código de identificação do utilizador (User ID)*» — O código único atribuído às pessoas, quando estas se tornam assinantes ou se registam num serviço de acesso à *Internet*, ou num serviço de comunicação pela *Internet*;

k) «*Conteúdos discriminatórios*» — Qualquer palavra, imagem ou outro que defenda, promova ou incite ao ódio ou a actos de violência contra uma pessoa ou grupo de pessoas por causa da sua raça, origem étnica, cor, nacionalidade, religião ou orientação sexual, com o propósito de os discriminar;

l) «*Dados*» — Qualquer representação de factos, vídeos ou imagens, informações ou conceitos, incluindo de programas de computador, que são armazenados, transmitidos ou processados num sistema de informação;

m) «*Dados de base pessoais*» — Os dados que permitem identificar uma pessoa, como seja o nome, idade, morada, telefone e endereço de correio electrónico;

n) «*Dados de localização*» — Quaisquer dados tratados num sistema de informação que indiquem a posição geográfica do equipamento terminal ou de um utilizador de um serviço prestado através de um sistema de informação;

o) «*Dados de tráfego*» — Qualquer dado tratado para efeitos do envio de uma comunicação, através de um sistema de informação ou para efeitos de facturação daquela, incluindo os dados que indicam a origem, destino, trajecto, hora, data, tamanho e duração da comunicação, ou o tipo de serviço subjacente;

p) «*Dados informáticos*» — Quaisquer dados susceptíveis de processamento por um sistema informático;

q) «*Dispositivo*» — Qualquer equipamento, material electromagnético, acústico, mecânico, técnico ou outros ou programa de computador;

r) «*DSL (Digital Subscriber Line)*» — A tecnologia que permite aproveitar o conjunto de pares de cabo de cobre para fins de serviços de *Internet* de banda larga;

s) «*Endereço do Protocolo IP*» — O conjunto de números que permitem a identificação e a comunicação consistente entre equipamentos (normalmente computadores) de uma rede privada ou pública, mediante uma plataforma de *Internet*;

t) «*Identificador de Célula (Cell ID)*» — A identificação da célula de origem e de destino de uma chamada telefónica numa rede móvel;

u) «*IMEI (International Mobile Equipmentidentity)*» — O código pré-gravado nos telefones móveis da tecnologia GSM, que permite a identificação do equipamento ou do terminal a nível internacional, ao ser transmitido ou ao interligar-se a uma rede de comunicações electrónicas acessíveis ao público. Caso a tecnologia usada não seja GSM

considera-se o código equivalente para a tecnologia em questão;

v) «*IMSI (International Mobile Subcriberidentity)*» — O código único de identificação para cada aparelho terminal de telefonia móvel cuja integração no cartão SIM do telemóvel, permite a sua identificação através das redes da tecnologia GSM e UMTS. Caso a tecnologia usada não seja GSM e UMTS considera-se o código equivalente para a tecnologia em questão;

w) «*Incidentes informáticos*» — Qualquer evento real ou suspeito relacionado com a segurança de sistema informático ou rede;

x) «*Intercepção de Comunicação*» — O acto destinado a captar dados contidos ou transmitidos através de um sistema de informação mediante o recurso a dispositivos;

y) «*Operadores de comunicações electrónicas*» — Os organismos, as pessoas colectivas de direito público, as pessoas singulares ou colectivas de direito privado ou misto, que oferecem redes ou serviços de comunicações electrónicas;

z) «*Operadores de comunicações electrónicas acessíveis ao público*» — São os operadores de redes de comunicações electrónicas públicas e os operadores de serviços de comunicações electrónicas públicos, conforme estes sejam definidos na legislação relevante;

aa) «*Prestador de serviço*» — Qualquer pessoa, singular ou colectiva, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema de informação, bem como qualquer outra entidade que trate ou armazene dados em nome e por conta daquela ou dos respectivos utilizadores, incluindo, mas não se limitando, a operadores de comunicações electrónicas e prestadores de serviços da sociedade da informação;

bb) «*Programa de computador*» — O conjunto de instruções (*software*) usado directa ou indirectamente num computador, tendo em vista a obtenção de determinado resultado, incluindo o material de concepção;

cc) «*Rede*» — O grupo de sistemas de informação interligados entre si que permite o envio e a recepção de dados;

dd) «*Rede do ciberespaço*» — Os sistemas de transmissão e, se for o caso, os equipamentos de comutação ou encaminhamento e os demais recursos que permitem o envio de sinais por cabo, meios radioeléctricos, meios ópticos, ou por outros meios electromagnéticos, incluindo as redes de satélites, as redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo a *Internet*) e móveis, os sistemas de cabos de electricidade, na medida em que sejam utilizados para a transmissão de sinais, as redes utilizadas para a radiodifusão sonora e televisiva e as redes de televisão por cabo, independentemente do tipo de informação transmitida;

ee) «*Roubo informático*» — Qualquer apropriação indevida de uma rede, sistema informático, bases de dados, equipamento informático, programa informático, usando a violência, ameaça, acesso ilegítimo com vista a estruturação incorrecta de programa ou sistema informático;

ff) «*Serviço da sociedade da informação*» — O Serviço prestado à distância por via electrónica, no âmbito de uma actividade económica na sequência de pedido individual do destinatário, considerando-se, para efeitos da presente definição:

i. «*Serviço*» — A disponibilização de conteúdos, bens (materiais e imateriais) e serviços, independentemente de a sua entrega ou prestação ser efectuada por via electrónica;

ii. «*À distância*» — Sem que as partes estejam simultaneamente presentes;

iii. «*Por via electrónica*» — Enviado da origem e recebido no destino através de meios electrónicos de processamento e de armazenamento de dados, incluindo a via informática, o cabo, rádio, meios ópticos e meios electromagnéticos, excluindo o telefone, telecópia, telex e teletexto televisivo;

iv. «*Pedido individual do destinatário*» — A solicitação do destinatário para que lhe seja prestado um serviço da sociedade da informação, incluindo o mero acesso ao sítio/página do prestador do serviço da sociedade da informação;

v. Não são serviços da sociedade da informação:

i) Serviços de radiodifusão televisiva e sonora;

ii) Distribuição automática de notas e bilhetes;

iii) Acesso às redes rodoviárias, parques de estacionamento, etc., mediante pagamento, mesmo que existam dispositivos electrónicos à entrada e ou à saída para controlar o acesso ou garantir o correcto pagamento.

gg) «*Serviço protegido*» — Qualquer serviço da sociedade da informação, com acesso condicional;

hh) «*Sistema de informação*» — Qualquer dispositivo ou conjunto de dispositivos, bem como a rede que suporta a comunicação entre eles, que, de forma separada ou conjunta, armazenam, tratam, transmitem, recebem ou recuperam dados;

ii) «*Sistema informático*» — Qualquer dispositivo ou conjunto de dispositivos que procedem ao armazenamento, tratamento, recuperação ou transmissão de dados informáticos em execução de um programa de computador;

jj) «*Sistema de comunicações electrónicas*» — A rede de comunicações electrónicas e qualquer dispositivo ou conjunto de dispositivos que permitem a transmissão de sinais por meio óptico, celular, radioeléctrico, electromagnético ou através de qualquer outra plataforma;

kk) «*Sociedade da Informação*» — Sociedade em que as principais actividades estão integradas pelas novas tecnologias da informação e comunicação onde a informação circula em redes electrónicas;

ARTIGO 5.°
(Cooperação internacional)

O Estado Angolano deve cooperar com os outros Estados e organizações internacionais em matéria de segurança do ciberespaço nacional para efeitos de prevenção, investigação ou procedimentos respeitantes aos crimes relacionados com os sistemas ou dados informáticos, recolha de prova em suporte electrónico, num restrito respeito, as normas sobre a transferência internacional de dados pessoais, e nos termos e limites do regime jurídico da cooperação internacional em matéria penal, e da protecção de dados pessoais.

CAPÍTULO II
Medidas de Protecção do Ciberespaço Acessíveis ao Público

SECÇÃO I
Redes do Ciberespaço

ARTIGO 6.°
(Segurança nas redes do ciberespaço)

As redes do ciberespaço devem assegurar a integridade, a confidencialidade e privacidade das comunicações mediante implementação de serviços de segurança lógica e física, estabelecidos no regime jurídico das comunicações electrónicas.

ARTIGO 7.°
(Infra-estruturas críticas)

Cabe aos operadores e prestadores de serviços de infra-estruturas críticas do Ciberespaço, aplicar um conjunto de medidas e técnicas que proporcionam a segurança e protecção dos activos essenciais para o bom funcionamento das funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico ou o funcionamento regular dos serviços públicos, como sejam os serviços de água, energia eléctrica e as comunicações electrónicas.

ARTIGO 8.°
(Encriptação de redes de comunicações electrónicas)

Incumbe ao operador da rede de comunicações electrónicas garantir as condições técnicas e de segurança em que se processa a comunicação electrónica para efeitos da transmissão de dados de tráfego e de localização relativos às pessoas singulares e colectivas.

ARTIGO 9.°
(Resposta a incidentes nas redes do ciberespaço)

As redes de comunicações electrónicas estão sujeitas as medidas técnicas e operacionais de respostas aos erros, ataques, roubos, acidentes, ciber-ataques e quaisquer outros incidentes provocados contra si, por via de mecanismos de gestão de respostas de incidentes adequados e eficientes.

ARTIGO 10.°
(Emergência de segurança das redes de comunicações electrónicas)

Cabe aos operadores e prestadores de serviços de redes de comunicações electrónicas implementar os serviços preventivos de avisos, alertas, recomendações e informações sobre segurança, de modo a garantir a contínua promoção da integridade e fiabilidade das redes.

ARTIGO 11.°
(Gestão de segurança nas redes de comunicações electrónicas)

Cabe aos operadores e prestadores de serviços de redes de comunicações electrónicas promover a execução de medidas e instrumentos necessários à antecipação, detecção, reacção e recuperação de situações de riscos de segurança nas redes.

SECÇÃO II
Sistemas Informáticos

ARTIGO 12.°
(Segurança nos sistemas da sociedade da informação)

O órgão responsável pela promoção da sociedade de informação, os provedores, operadores e prestadores de serviços dos sistemas da sociedade da informação, devem garantir a segurança de qualquer dispositivo ou conjunto de dispositivos que procedem ao armazenamento, tratamento, recuperação ou transmissão de dados informáticos em execução de um programa de computador.

ARTIGO 13.°
(Infra-estrutura informática)

Cabe à entidade responsável pela gestão ou aos operadores e prestadores de serviços garantir a aplicação de um conjunto de medidas e técnicas que proporcionam a segurança e protecção dos activos considerados essenciais para o bom funcionamento das infra-estruturas.

ARTIGO 14.°
(Segurança na *internet*)

Sem prejuízo dos termos e condições aplicáveis para utilização específica do ciberespaço, os operadores e prestadores de serviços de *internet* devem promover o registo dos utilizadores e a execução de medidas e instrumentos necessários à antecipação, à detecção, a reacção e a recuperação em situações de riscos de segurança, nas redes.

ARTIGO 15.°
(Emergência informática)

1. Os provedores, operadores e prestadores de serviços do Ciberespaço, antes do início do exercício das actividades, devem apresentar à entidade reguladora no domínio da

protecção de dados e ao órgão responsável pela promoção da sociedade de informação, um plano de gestão de acidentes e incidentes, em caso de emergência informática.

2. Em caso de ataques, roubo informático ou qualquer incidente informático, devem ser difundidos os alertas e avisos.

3. Os requisitos do plano de gestão de acidentes e incidentes, devem ser objecto de regulamentação.

ARTIGO 16.°
(Emergência de segurança)

1. Os serviços devem estar activados com dispositivos capazes de emitir alertas em caso de um evento ou uma solicitação, assim como enviar o relatório técnico sobre um servidor comprometido, código malicioso amplamente difundido, vulnerabilidades de *software* ou algo que for identificado por um sistema de detecção de intromissões ou um registo de eventos.

2. Os serviços reactivos, incluindo os de alertas e avisos, constituem a componente central do trabalho do Centro de Estudos, Respostas, e Tratamento de Incidentes Informáticos (CERT).

ARTIGO 17.°
(Gestão de acidente e incidente informático)

1. Os provedores, operadores e prestadores de serviços do ciberespaço devem garantir a assistência e a informação para preparar, auxiliar e acautelar a segurança dos sistemas protegidos, em antecipação de ataques, problemas ou eventos.

2. Sem prejuízo do disposto no número anterior, os provedores, operadores e prestadores de serviços do ciberespaço estão essencialmente orientados para reduzir o número de futuros incidentes, devendo para o efeito incluírem nos serviços os seguintes elementos:

a) Comunicações e anúncios;
b) Observatório de tecnologia;
c) Avaliações ou auditorias de segurança;
d) Configuração e manutenção de ferramentas, aplicações e infra-estruturas de segurança;
e) Desenvolvimento de ferramentas de segurança;
f) Serviços de detecção de intromissões;
g) Difusão de informações relacionadas com a segurança.

SECÇÃO III
Programas de Computador e das Bases de Dados

ARTIGO 18.°
(Programas de computador)

Sem prejuízo do regime jurídico das tecnologias de informação e dos serviços da sociedade da informação previsto na legislação em vigor, aos programas de computador, são aplicáveis às medidas e técnicas da presente Lei.

ARTIGO 19.°
(Bases de dados)

Sem prejuízo do disposto no regime jurídico das tecnologias de informação e dos serviços da sociedade da informação, a utilização das bases de dados deve obedecer as regras técnicas e procedimentos especializados de protecção adequada de acesso, armazenamento, duplicação de arquivos, tratamento e recuperação de informação automatizada.

CAPÍTULO III
Medidas de Protecção aos Dados de Tráfego e de Localização

SECÇÃO I
Preservação de Dados

ARTIGO 20.°
(Conservação expedita de dados)

1. Os responsáveis pelo tratamento dos dados específicos armazenados numa rede de comunicações electrónicas e sistemas da sociedade da informação, incluindo os dados de tráfego, ficam obrigados a assegurar a confidencialidade e devem ordenar a conservação expedita de dados, sob pena de nulidade.

2. Os dados referidos no número anterior devem ser preservados até 6 (seis) meses.

3. O responsável pelo tratamento dos dados deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados informáticos 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.

ARTIGO 21.°
(Conservação expedita de dados de tráfego e de localização)

Ao operador de comunicações electrónicas do ciberespaço acessível ao público ou prestador de serviços da sociedade da informação, a quem a preservação dos dados de tráfego e de localização, relativos à uma determinada comunicação que tenha sido ordenada à conservação, nos termos da legislação processual penal, deve indicar as outras entidades que nela participem, permitindo a identificação das mesmas.

ARTIGO 22.°
(Preservação de provas)

O operador de comunicações electrónicas acessíveis ao público ou o prestador de serviços da sociedade da informação que tenha armazenado num determinado sistema de informação, dados de tráfego e de localização necessários à produção de provas, tendo em vista a descoberta da verdade, deve disponibilizar o controlo desses dados ou permitir o acesso ao sistema de informação onde os mesmos estão armazenados, aos Magistrados Judiciais ou do Ministério Público, nos termos da legislação Penal aplicável e da presente Lei.

SECÇÃO II
Regras Específicas Aplicáveis a Operadores de Comunicações Electrónicas Acessíveis ao Público

ARTIGO 23.°
(Preservação de dados)

1. Os operadores de comunicações electrónicas acessíveis ao público e os prestadores de armazenagem principal devem conservar os dados de tráfego e de localização, bem como os dados conexos, para identificar o assinante ou o utilizador

de um serviço de comunicações electrónicas acessíveis ao público ou de um serviço de armazenagem principal, quando tais dados sejam por si gerados ou tratados no território nacional e no âmbito da sua actividade, exclusivamente para fins de investigação, detecção e repressão de crimes.

2. Os dados referidos no número anterior devem ser conservados por um período de 12 (doze) meses, contados a partir da data da conclusão da comunicação.

ARTIGO 24.º
(Categoria de dados a preservar)

Para efeitos do disposto no artigo anterior, devem ser conservados os seguintes dados:

a) Dados necessários para encontrar e identificar a fonte de uma comunicação;

b) Dados necessários para encontrar e identificar o destino de uma comunicação;

c) Dados necessários para identificar a data, a hora e a duração de uma comunicação;

d) Dados necessários para identificar o tipo de comunicação;

e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores ou o que se considera ser o seu equipamento;

f) Dados necessários para identificar a localização do equipamento de comunicação móvel;

g) Dados necessários para identificar a localização de um endereço do protocolo IP.

ARTIGO 25.º
(Dados para encontrar e identificar a fonte de uma comunicação)

1. Nas comunicações telefónicas, pela rede fixa e móvel, para encontrar e identificar a fonte de uma comunicação, os operadores de comunicações electrónicas acessíveis ao público devem conservar os seguintes dados:

a) O número de telefone de origem;

b) O nome e endereço do assinante ou do utilizador registado.

2. No acesso ao correio electrónico e nas comunicações telefónicas através da *Internet* para encontrar e identificar a fonte de uma comunicação, os operadores de comunicações electrónicas acessíveis ao público devem conservar os seguintes dados:

a) O código de identificação atribuído ao utilizador;

b) O código de identificação do utilizador e o número de telefone atribuído a qualquer comunicação que entre na rede telefónica pública;

c) O nome e o endereço do assinante ou do utilizador registado, à quem o endereço do protocolo IP, o código de identificação de utilizador ou o número de telefone, estavam atribuídos no momento da comunicação.

ARTIGO 26.º
(Dados para encontrar e identificar o destino de uma comunicação)

1. Nas comunicações telefónicas através da rede fixa e móvel, para encontrar e identificar o destino de uma comunicação, os operadores de comunicações electrónicas acessíveis ao público devem conservar os seguintes dados:

a) Os números marcados e, em casos que envolvam serviços suplementares como o reencaminhamento ou a transferência de chamadas, o número ou números para onde a chamada foi reencaminhada;

b) O nome e o endereço do assinante ou do utilizador registado.

2. No acesso ao correio electrónico e comunicações telefónicas através da *Internet* para encontrar e identificar o destino de uma comunicação, os operadores de comunicações electrónicas acessíveis ao público devem conservar os seguintes dados:

a) O código de identificação do utilizador ou o número de telefone do destinatário pretendido ou de uma comunicação telefónica através da *Internet*;

b) Os nomes e os endereços dos subscritores ou dos utilizadores registados e o código de identificação de utilizador do destinatário da comunicação pretendida.

ARTIGO 27.º
(Dados necessários para identificar a data, a hora e a duração de uma comunicação)

1. Nas comunicações telefónicas pela rede fixa e móvel, para identificar uma comunicação, os operadores de comunicações electrónicas acessíveis ao público devem conservar a data, a hora e a duração da comunicação.

2. No acesso ao correio electrónico e às comunicações telefónicas através da *Internet* para identificar a data, a hora e a duração de uma comunicação, os operadores de comunicações electrónicas acessíveis ao público devem conservar os seguintes dados:

a) A data e a hora do início e do fim da ligação ao serviço de acesso à *Internet*, com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à *Internet*, bem como o código de identificação de utilizador do subscritor ou do utilizador registado;

b) A data e a hora do início e do fim da ligação ao serviço de correio electrónico através da *Internet* ou de comunicações através da *Internet*, com base em determinado fuso horário.

ARTIGO 28.º
(Dados necessários para identificar o tipo de comunicação)

Para identificar o tipo de comunicação, os operadores de comunicações electrónicas acessíveis ao público devem conservar os seguintes dados:

a) O serviço telefónico utilizado nas comunicações telefónicas na rede fixa e móvel;

b) O serviço de *Internet* utilizado através do correio electrónico nas comunicações telefónicas pela *Internet*.

ARTIGO 29.º
(Dados necessários para identificar o equipamento de comunicações electrónicas)

1. Para identificar o equipamento de telecomunicações dos utilizadores, os operadores de comunicações electrónicas acessíveis ao público devem conservar os seguintes dados:

a) Os números de telefone de origem e de destino, nas comunicações telefónicas pela rede fixa;

b) Os números de telefone de origem e de destino, nas comunicações telefónicas pela rede móvel:

c) A Identidade Internacional de Assinante Móvel (IMSI) de quem telefona através da rede móvel;

d) A Identidade Internacional do Equipamento Móvel (IMEI) de quem telefona através da rede móvel;

e) A Identidade Internacional de Assinante Móvel (IMSI) do destinatário do telefonema, através da rede móvel;

f) A Identidade Internacional do Equipamento Móvel (IMEI) do destinatário do telefonema, através da rede móvel;

g) No caso dos serviços pré-pagos de carácter anónimo, a data e a hora da activação inicial do serviço e o identificador da célula a partir da qual o serviço foi activado através da rede móvel.

2. No acesso ao correio electrónico e às comunicações telefónicas pela *Internet*, para identificar o equipamento de comunicações electrónicas dos utilizadores, os operadores de comunicações electrónicas acessíveis ao público devem conservar os seguintes dados:

a) O número de telefone que solicita o acesso por linha telefónica;

b) A linha de assinante digital (DSL) ou qualquer outro identificador terminal do autor da comunicação.

ARTIGO 30.º
(Dados necessários para identificar a localização do equipamento de comunicação móvel)

Para identificar a localização do equipamento de comunicação móvel, os operadores de comunicações electrónicas acessíveis ao público devem conservar os seguintes dados:

a) O identificador da célula no início da comunicação;

b) Os dados que identifiquem a situação geográfica das células, tomando como referência os respectivos identificadores de célula, durante o período em que se procede a conservação de dados.

ARTIGO 31.º
(Dados necessários para identificar a localização do endereço do Protocolo IP)

Para identificar a localização de endereço do protocolo IP, os operadores de comunicações electrónicas acessíveis ao público devem conservar os seguintes dados:

a) A identificação, na rede, dos equipamentos acessíveis por endereço IP;

b) Os mapas de endereçamento das redes;

c) Os dados que identifiquem a situação geográfica do endereço IP, tomando como referência os registos das Entidades Regionais de Registos da *Internet*, responsáveis pela distribuição e gestão dos recursos de números da *Internet*, tais como endereços IP e sistema autónomo de números.

ARTIGO 32.º
(Comunicação não iniciada ou concluída no território nacional)

1. Os operadores de comunicações electrónicas acessíveis ao público devem conservar também aqueles dados em que a comunicação não seja iniciada ou concluída no território nacional.

2. Os dados telefónicos e da *Internet* relativos à chamadas telefónicas falhadas devem ser conservados quando sejam gerados ou tratados e armazenados pelos operadores de comunicações electrónicas acessíveis ao público, no contexto da oferta de serviços de comunicação.

3. Os dados relativos às chamadas não estabelecidas, não são conservados.

SECÇÃO III
Regras Específicas Aplicáveis aos Prestadores de Armazenagem Principal

ARTIGO 33.º
(Categoria de dados a conservar)

1. Os prestadores de armazenagem principal devem conservar, por um período de 6 (seis) meses, a contar da data da conclusão do alojamento, as seguintes categorias de dados:

a) O país de origem dos dados armazenados;

b) O nome e o endereço do fornecedor dos dados;

c) O endereço do protocolo IP do fornecedor dos dados;

d) A data do início e do fim do alojamento dos dados.

2. A conservação de dados que revelem o conteúdo das comunicações é proibida, sem prejuízo das regras aplicáveis à intercepção e gravação legais de dados.

3. Os operadores de comunicações electrónicas acessíveis ao público, bem como os prestadores de armazenagem principal, na qualidade de responsáveis pelo tratamento dos dados pessoais que conservem ao abrigo deste artigo, devem assegurar o cumprimento das obrigações impostas ao responsável pelo tratamento constantes da legislação aplicável, nomeadamente o direito de acesso e de informação aos titulares dos dados.

ARTIGO 34.º
(Formalidades)

1. Não carece de autorização da Agência de Protecção de Dados Pessoais o tratamento dos dados nos termos e para os fins previstos nas Secções II e III do presente capítulo III o qual está sujeito a mera notificação.

2. O titular dos dados não pode opor-se ao respectivo tratamento, nem à sua transmissão, nos termos da Lei da Protecção de Dados Pessoais.

SECÇÃO IV
Medidas de Protecção dos Dados

ARTIGO 35.º
(Condições de conservação dos dados)

1. Os operadores de comunicações electrónicas acessíveis ao público e os prestadores de armazenagem principal devem:

a) Garantir que os dados conservados sejam da mesma qualidade e estejam sujeitos, pelo menos, à mesma protecção e segurança que os dados na rede;

b) Tomar as medidas técnicas e organizativas adequadas à protecção dos dados previstos no presente Capítulo, contra a destruição acidental ou ilícita, a perda ou a alteração acidental e o armazenamento, tratamento, acesso ou divulgação não autorizada ou ilícita;

c) Tomar as medidas técnicas e organizativas adequadas para garantir que, apenas os trabalhadores ou colaboradores, incluindo subcontratados especialmente autorizados por si, tenham acesso aos dados referentes às categorias previstas no número 1 do artigo 33.º da presente Lei.

2. Verificando-se que mais do que um operador de comunicações electrónicas acessíveis ao público conserva os mesmos dados relativos à mesma comunicação, como sucede nos casos de selecção e de pré-selecção, os referidos operadores podem definir, contratualmente, a quem incumbe a obrigação de conservação dos dados, devendo dar conhecimento por escrito, do mesmo, à Autoridade das Comunicações Electrónicas, ficando o outro operador isento da obrigação referida.

3. Os dados referentes às categorias previstas no n.º 1 do artigo 33.º da presente Lei, com excepção dos dados de base, devem permanecer bloqueados desde o início da sua conservação, sendo alvo de desbloqueio, somente para efeitos de transmissão, nos termos do processo de investigação criminal, mediante despacho fundamentado do magistrado competente.

4. O disposto nos números anteriores não prejudica a observação dos princípios, nem o cumprimento das regras relativas à qualidade e à salvaguarda da confidencialidade e da segurança dos dados pessoais.

5. A autoridade pública competente para o controlo da aplicação do previsto nos números anteriores é a Agência de Protecção de Dados Pessoais.

ARTIGO 36.º
(Transmissão de dados)

1. A transmissão de dados conservados, nos termos das secções II e III do presente Capítulo, só pode ser autorizada por despacho fundamentado pelo Magistrado Judicial competente.

2. A transmissão dos dados deve ser efectuada por via electrónica e observar um grau de codificação e protecção o mais elevado possível, de acordo com o estado da técnica, ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados.

3. As condições de transmissão dos dados por via electrónica são fixadas em diploma próprio, podendo incluir a criação de plataformas web, através das quais as autoridades judiciárias competentes possam aceder directamente aos dados de tráfego e de localização, bem como aos dados conexos relacionados.

4. A Autoridade Pública competente para o controlo da aplicação do disposto no n.º 2 do presente artigo, é a Agência de Protecção de Dados Pessoais.

ARTIGO 37.º
(Obrigação de intercepção)

1. Os operadores de comunicações electrónicas acessíveis ao público são obrigados a instalar, à expensas próprias e a disponibilizar à autoridade judiciária competente, sistemas de intercepção legal, mediante despacho fundamentado do Magistrado competente.

2. Os operadores de comunicações electrónicas acessíveis ao público devem proceder à intercepção e registo de dados, quando solicitados, por despacho fundamentado do Magistrado competente e apenas nos casos em que a intercepção e registo sejam admissíveis.

ARTIGO 38.º
(Destruição dos dados)

1. Sem prejuízo do previsto no artigo anterior, os operadores de comunicações electrónicas acessíveis ao público devem:

a) Destruir os dados indicados no presente capítulo, no final do período de conservação, excepto os dados que devam ser preservados por ordem do Juiz competente;

b) Destruir os dados ou cópias dos dados que tenham sido preservados após o decurso do período de conservação, quando tal lhe seja determinado por ordem das autoridades competentes e desde que os dados em causa não tenham sido também preservados ao abrigo do órgão de investigação criminal sob direcção do Ministério Público.

2. A autoridade pública competente para o controlo da aplicação do previsto no número anterior é a Agência de Protecção de Dados Pessoais.

3. A destruição dos dados previstos no n.º 1 do presente artigo, não prejudica a sua conservação para outros fins, desde que cumpridos os requisitos constantes da lei aplicável.

SECÇÃO V
Preservação da Soberania, Segurança do Estado e Ordem Pública

ARTIGO 39.º
(Sistema de Intercepção de dados)

Os operadores de comunicações electrónicas acessíveis ao público devem assegurar o acesso aos órgãos de inteligência e de segurança do Estado mediante autorização prévia do Magistrado competente, para proceder a intercepção de comunicações, nos termos do artigo 212.º da Constituição da República de Angola.

CAPÍTULO IV
Equipa de Monitorização e Respostas aos Incidentes Informáticos

ARTIGO 40.º
(Organização e funcionamento)

A organização e funcionamento da Equipa de Monitorização e Respostas aos Incidentes Informáticos são estabelecidos por diploma próprio.

ARTIGO 41.º
(Cooperação institucional)

A Equipa de Monitorização e Respostas aos Incidentes Informáticos deve estabelecer relações de cooperação institucional com organismos públicos e privados e outras congéneres na promoção da protecção e segurança do ciberespaço nacional.

CAPÍTULO V
Regime Sancionatório

ARTIGO 42.º
(Contravenções e multas)

1. Sem prejuízo de outras sanções que se mostrem aplicáveis, constitui contravenção punível com multa, a prática dos seguintes actos:

a) O incumprimento dos requisitos previstos nos artigos 12.º, 13.º, 14.º, 15.º e 18.º da presente Lei é aplicável uma multa que varia de Kz: 7.000.000,00 (sete milhões de Kwanzas) a Kz: 150.000.000,00, (cento e cinquenta milhões de Kwanzas);

b) O incumprimento dos requisitos previstos nos artigos 16.º, 17.º, 19.º, 21.º e 23.º da presente Lei é aplicável uma multa que varia de Kz: 7.000.000,00 (sete milhões de Kwanzas) a Kz: 150.000.000,00 (cento e cinquenta milhões de kwanzas);

c) A não conservação das categorias dos dados previstos nos artigos 29.º, 30.º e 31.º da presente Lei é aplicável uma multa que varia de Kz: 7.000.000,00 (sete milhões de Kwanzas) a Kz : 150.000.000,00 (cento e cinquenta milhões de kwanzas);

d) A não conservação das categorias dos dados previstos nos artigos 32.º, 33.º e 34.º da presente Lei é aplicável uma multa que varia de Kz: 3.000.000,00 (três milhões de kwanzas) a Kz: 75.000.000,00 (setenta e cinco milhões de Kwanzas);

e) A não conservação das categorias dos dados previstos no n.º 1 do artigo 37.º é aplicável uma multa que varia de Kz: 1.000.000,00 (um milhão de Kwanzas) a Kz: 3.000.000,00 (três milhões de Kwanzas);

2. É aplicável uma Multa que varia de Kz: 5.000.000,00 (cinco milhões Kwanzas) a Kz: 200.000.000,00 (duzentos milhões de Kwanzas) nos seguintes casos:

a) O incumprimento do disposto no artigo 35.º da presente Lei;

b) Falta de transmissão dos dados às autoridades judiciais competentes, quando autorizada nos termos do n.º 1 do artigo 36.º da presente Lei;

c) O incumprimento das medidas de destruição dos dados, nos termos do artigo 38.º da presente Lei.

3. Tratando-se de pessoas colectivas, as contravenções previstas no número anterior são agravadas ao dobro dos respectivos limites.

4. A determinação da medida da multa é feita em função da ilicitude concreta do facto, da culpa do agente e dos benefícios obtidos com a prática da contravenção e das exigências de prevenção.

5. Na determinação da ilicitude concreta do facto e da culpa deve atender-se, entre outras, às seguintes circunstâncias:

a) Ao perigo ou ao dano causados;

b) Ao carácter ocasional ou reiterado da infracção;

c) A existência de actos de ocultação tendentes a dificultar a descoberta da infracção;

d) A existência de actos praticados pelo agente, destinados a reparar por sua livre iniciativa, os danos ou obviar os perigos causados pela infracção;

e) A intenção do agente de obter, para si ou para outrem, um benefício ilegítimo ou de causar danos.

6. Na determinação da multa aplicável são ainda ponderadas a situação económica do infractor e o volume de negócios consolidado no ano civil anterior.

7. Se o mesmo facto constituir, simultaneamente, crime e contravenção, o agente é punido sempre a título de crime, nos termos previstos da legislação Penal.

8. As sanções aplicadas às contravenções em concurso são sempre cumuladas materialmente.

ARTIGO 43.º
(Aplicação das multas)

1. Compete à Agência de Protecção de Dados Pessoais a instrução dos processos de contravenção.

2. A aplicação das multas previstas na presente Lei compete ao Presidente da Agência de Protecção de Dados Pessoais, sob prévia deliberação da Agência.

3. A deliberação da Agência de Protecção de Dados Pessoais, depois de homologada pelo Presidente, constitui título executivo, no caso de não ser impugnada no prazo legal.

CAPÍTULO VI
Disposições Finais

ARTIGO 44.°
(Direito subsidiário)

Aos crimes contra os sistemas e dados informáticos, aplica-se subsidiariamente o regime jurídico previsto na Legislação Penal e Processual Penal em vigor.

ARTIGO 45.°
(Dúvidas e omissões)

As dúvidas e as omissões que resultarem da interpretação e da aplicação da presente Lei são resolvidas pela Assembleia Nacional.

ARTIGO 46.°
(Revogação)

É revogada toda a legislação que contrarie o disposto na presente Lei.

ARTIGO 47.°
(Entrada em vigor)

A presente Lei entra em vigor à data da sua publicação.

Vista e aprovada pela Assembleia Nacional, em Luanda, aos de 18 de Novembro 2016.

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

Promulgada aos 31 de Dezembro de 2016.

Publique-se.

O Presidente da República, José Eduardo dos Santos.

MINISTÉRIO DAS FINANÇAS

Despacho n.º 66/17
de 16 de Fevereiro

Tendo sido presente ao Ministro das Finanças para efeitos de autorização, ouvido o Ministério da Administração Pública, Trabalho e Segurança Social, um processo de alteração do Contrato de Constituição do Fundo de Pensões da Sonils, Limitada, nos termos do artigo 21.° do Regulamento sobre os Fundos de Pensões, aprovado pelo Decreto n.° 25/98, de 7 de Agosto;

Em conformidade com os poderes delegados pelo Presidente da República, nos termos do artigo 137.° da Constituição da República de Angola, conjugado com as disposições combinadas do n.° 1 do artigo 2.° do Decreto Presidencial n.° 6/10, de 24 de Fevereiro, e da alínea d) do n.° 1 do artigo 4.° do Estatuto Orgânico do Ministério das Finanças, aprovado pelo Decreto Presidencial n.° 299/14, de 4 de Novembro, determino:

Ponto Único: — É autorizada a alteração do Contrato de Constituição de Fundo de Pensões da Sonils, Limitada, denominado Fundo de Pensões da Sonils, Limitada, anexo ao presente Despacho e que dele faz parte integrante.

Publique-se.

Luanda, aos 16 de Fevereiro de 2017.

O Ministro, *Augusto Archer de Sousa Mangueira.*

ALTERAÇÃO INTEGRAL AO CONTRATO DE CONSTITUIÇÃO DO FUNDO DE PENSÕES DA SONILS, LIMITADA

Entre:

SONILS — Sonangol Integrated Logistic Services, Limitada, com sede na Rua 6 — I.L., Boavista, em Luanda, República de Angola, Contribuinte Fiscal n.° 5410002733, adiante designada por «Associada Fundadora», neste acto representado por Hélder Jorge de Sousa, na qualidade de Director Geral, e com poderes para o acto;

E

FÉNIX — Sociedade Gestora de Fundos de Pensões, S.A.R.L., com sede na Rua Alfredo Troni, n.° 79, Edifício do BPC, 14.°, em Luanda, República de Angola, Contribuinte Fiscal n.° 5403088113, registado na Conservatória do Registo Comercial de Luanda, sob o n.° 671, adiante designada por «Entidade Gestora», Certificado de Licença n.° 03/ISS/MF/04, de 3 de Setembro, com o capital social de Kz: 438.410.000,00 (quatrocentos e trinta e oito milhões, quatrocentos e dez mil Kwanzas, equivalente a USD 5.000.000,00 (cinco milhões de dólares dos Estados Unidos da América), neste acto representado por João de Almeida Neto e Zinho Baptista Manuel, na qualidade de Presidente do Conselho de Administração e Administrador, respectivamente, e com poderes para o acto.

Considerando que:

I. Os Fundos de Pensões têm-se erigido, ao longo dos últimos anos, como importante instrumento no financiamento da previdência privada em complemento do Sistema de Segurança Social visando o bem-estar futuro da população reformada;

II. Os Fundos de Pensões são patrimónios autónomos exclusivamente afectos à realização de um ou mais Planos de Pensões;

III. A SONILS — Sonangol Integrated Logistic Services, Limitada, (adiante abreviadamente designada por Associada Fundadora) é a actual associada do presente fundo de pensões fechado, denominado Fundo de Pensões da Sonils, Limitada;

IV. Este Fundo de Pensões funcionou, até à presente data, como veículo de financiamento de um plano de pensões de benefício definido;