RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano V, v.1, n.1, jan/julho 2025. | submissão: 09/05/2025 | aceito: 11/05/2025 | publicação:13/05/2025

Responsabilidade civil de provedores e segurança da informação em moçambique

Civil liability of providers and information security in mozambique

Responsabilidad civil de los proveedores y seguridad de la información en mozambique

Raúl de Miguel Benjamim Jofrisse Nhamitambo[1]

RESUMO
A sociedade enfrenta grandes dasafios em equilibrar - se entre a garantia ao direito à informação, que ultrapassa o próprio direito à liberdade de expressão, e à proteção à intimidade e à vida privada diante aos novos desafios tecnológicos. O que leva a doutrina a revisitar os pressupostos da responsabilidade civil dos provedores e a seguranca da informacao. A teoria da responsabilidade subjetiva por culpa in omittendo, os provedores têm o dever de: retirar o conteúdo ilícito logo após a notificação da vítima e adotar as medidas necessárias, respeitados os limites de sua capacidade técnica, para fins de identificação do usuário responsável pela divulgação do material ofensivo. No mesmo julgado, constatou-se que os provedores respondem solidariamente com o autor direto do dano na hipótese de não tornarem o conteúdo infringente inacessível logo após a cientificação de sua existência pela parte interessada.
Palavras-chave: Sociedade, direito à informação, responsabilidade.

ABSTRACT
Society faces major challenges in balancing the guarantee of the right to information, which goes beyond the right to freedom of expression, and the protection of privacy and private life in the face of new technological challenges. This leads the doctrine to revisit the assumptions of civil liability of providers and information security. The theory of subjective liability due to culpa in omittendo, providers have the duty to: a) remove the illicit content immediately after notifying the victim; b) adopt the necessary measures, respecting the limits of its technical capacity, for the purpose of identifying the user responsible for disseminating the offensive material. In the same judgment, it was found that providers are jointly liable with the direct perpetrator of the damage if they do not make the infringing content inaccessible immediately after the interested party becomes aware of its existence.
Keywords: Access, visually impaired people, job market.

[1] Doutor em Ciências Jurídicas, pela Universidade Para La Cooperación Internacional México (UCIMEXICO) – México (2020); Mestre em Assessoria Jurídica de Empresas, pela Universidad a Distancia de Madrid (UDIMA) - Madrid (2016); Licenciado Ciências Jurídicas e Investigação Criminal, pelo extinto Instituto Superior de Ciências e Tecnologia Alberto Chipande (ISCTAC) – Beira (2011); Advogado e Membro da Ordem dos Advogados de Moçambique (desde Abril de 2018); Professor Auxiliar de Direito das Tecnologias de Informação e Comunicações (Direito das TIC's) – na Universidade Joaquim Chissano (UJC) – Maputo (desde Fevereiro de 2020), no Curso de Licenciatura em Engenharia de Tecnologias e Sistemas de Informação; Professor Auxiliar de Direito Administrativo e Noções de Direito Administraticvo – na Universidade Pedagógica de Maputo (UP - Maputo), nos Cursos de Licenciaturas em Gestão de Recursos Humanos e Gestão Pública e Educacional; Técnico Superior de Assistência Jurídica – Gabinete Jurídico (UP - Maputo); Docente Universitário de Introdução ao Direito, Direito Administrativo I e II e, Direito de Trabalho, nos Cursos de Licenciatura em Direito, Contabilidade e Auditoria e, Administração Pública e Autárquica – no Instituto Superior Maria Mãe de África (ISMMA); Professor Auxiliar no Instituto Superior de Contabilidade e Auditoria de Moçambique (ISCAM), leccionando a disciplina Complementos de Fiscalidade no Curso de Mestrado em Auditoria; Autor, Revisor, Avaliador Externo e Parecista na Revista Científica Multidisciplinar O Saber (desde II Semestre de 2024); Autor, Avaliador e Parecista na Revista Multidisciplinar RECIMA21 (desde I Semestre de 2025) e na Revista Internacional Consinter de Direito (**Conselho Internacional de Estudos Contemporâneos em Pós-Graduação – CONSINTER), desde II Semestre de 2025** e Organizador da Editora Científica Digital (Desde I Semestre de 2025). Matola – Maputo. ORCID: 0009-0006-4118-1970. rnhamitambo@gmail.com.(+258) 872058783/847417800.

RESUMEN
La sociedad se enfrenta a importantes retos para conciliar la garantía del derecho a la información, que trasciende el derecho a la libertad de expresión, con la protección de la privacidad y la vida privada ante los nuevos desafíos tecnológicos. Esto lleva a la doctrina a revisar los supuestos de responsabilidad civil de los proveedores y la seguridad de la información. Según la teoría de la responsabilidad subjetiva por culpa in omittendo, los proveedores tienen el deber de retirar el contenido ilícito inmediatamente después de notificar a la víctima y adoptar las medidas necesarias, respetando los límites de su capacidad técnica, para identificar al usuario responsable de la difusión del material ofensivo. En la misma sentencia, se determinó que los proveedores son solidariamente responsables con el autor directo del daño si no hacen inaccesible el contenido infractor inmediatamente después de notificar al interesado su existencia.
Palabras - clave: Sociedad, derecho a la información, responsabilidad.

INTRODUÇÃO

A tecnologia da informação revolucionou a maneira como vivemos e fazemos negócios. A convergência de tecnologias para ambientes inteligentes e ecossistemas integrados nos deixou vulneráveis. Isto tem sido acompanhado por uma ameaça crescente que não conhece limites, a título de exemplo : As ameaças cibernéticas. Actualmente, existe uma multiplicidade de ameaças e riscos que podem prejudicar o bom funcionamento do ciberespaço, incluindo os sistemas e serviços de TIC em Moçambique que podem provocar um impacto negativo nos esforços para o aproveitamento das TICs para o desenvolvimento socioeconómico. Dada a característica transfronteiriça das TIC's, nenhuma nação soberana ou corporação multinacional pode assegurar a segurança cibernética sozinho, exigindo uma abordagem conjunta, tanto dentro do país como a nível internacional. É neste âmbito que, Moçambique vem estando a dar passos largos para criar um ambiente em que o cidadão tenha um acesso crescente as Tecnologias de Informação e Comunicação (TIC) e aos serviços associados com um alto sentido de segurança. Por esta razão, várias acções e a diferentes níveis tem vindo a ser criadas e implementadas pelo Governo, por exemplo: Lei de transações eletrónicas, aprovada pela Lei n° 3/2017 de 9 de Janeiro, Estratégia nacional de segurança cibernética de Moçambique, Projecto de Governo Electrónico e de Infra-estruturas de Comunicação de Moçambique (Mozambique Electronic Government and Communications Infrastructure -MEGCIP), Rede Electrónica do Governo (GovNet), Sistema de Informação do Pessoal do Estado (SIP), e-SISTAF (Sistema de Informação de Administração Financeira do Estado), entre outros.

A presente pesquisa tem como objectivo abordar sobre a legislação moçambicana no diz respeito aos provedores e suas responsabilidades e a segurança da informação. O preveedor será responsabilizado civilmente do caso de danos no exercicio das suas actividades quotidianas.

A pesquisa se caracteriza como:

Quanto à finalidade: Bibliográfica, com base em material já elaborado e publicado, como livros, artigos científicos e legislação. Segundo CRESWELL, a pesquisa bibliográfica é baseada em material já elaborado e publicado, como livros, artigos científicos e legislação. Essa abordagem permite a análise crítica e aprofundada das teorias e perspectivas existentes sobre o tema, fornecendo uma base sólida para a construção do conhecimento.

Portanto, ao adoptar uma abordagem bibliográfica, este estudo se fortalece ao integrar conhecimento teórico consolidado com a realidade prática, fundamentando suas conclusões e recomendações em bases científicas e normativas. Dessa forma, a pesquisa propõe reflexões e soluções fundamentadas em literatura especializada e documentos oficiais.

Quanto à natureza: Básica ou pura, buscando a produção de novos conhecimentos sobre o tema em questão. Quanto à natureza, este estudo é classificado como básico ou pura, buscando a produção de novos conhecimentos. Como ressaltam Lakatos e MARCONI (2017), a pesquisa básica é voltada para a geração de teorias e conceitos, contribuindo para o avanço do entendimento sobre determinado tema.

Quanto à forma de abordagem: Qualitativa, buscando a compreensão dos significados e interpretações dos fenómenos relacionados ao tema. A abordagem qualitativa adoptada neste estudo.

Tecnicas e Instrumentos de Análise de dados

Para a análise dos dados recolhidos, utilizou-se a análise de conteúdo, que, segundo BARDIN (2011), é uma metodologia que possibilita a categorização, interpretação e inferência de informações contidas em materiais textuais, permitindo a identificação de padrões e significados subjacentes nos discursos e documentos analisados.

RESPONSABILIDADE DE PROVEDORES

Provedor

Segundo o dicionário "Aurélio", provedor é uma palavra pertecente tanto a classe de substantivo assim como de adjectivo, que significa "algo ou alguém que provê ou que fornece o necessário: o Governo é o provedor dos seus benefícios". Também, provedor pode ser qualquer "indivíduo responsável por certos estabelecimentos, instituições beneficentes ou assistencialistas". Portanto, qualquer entidade, empresa, indivíduo singular ou até mesmo um grupo de pessoas que forneça algo de qualquer tipo (alimentação, produtos, serviços, etc..) pode entender-se como um provedor, razão pela qual este termo seja utilizado em diversas áreas. Porém, importa referir que no nosso contexto, quando falamos deste termo, referimo-nos ao contexto de Tecnologias de Informação e Comunicação (TIC's).

Classificação de provedores

Segundo a Lei de transações electrónicas[2], nos artigos 10 e 13, os provedores podem ser classificados de duas formas : primário e intermediário, tendo cada um as suas responsabilidades bem delineadas conforme a mesma lei.

Provedor primário de serviços

"São provedores primários de serviços, as instituições públicas governamentais ou delegadas pela Entidade Reguladora das Tecnologias de Informação e Comunicação que enviam, recebem ou armazenam dados institucionais, colectivos ou individuais". Ibdi (artigo 10, número 1) [O]s provedores primários de serviços podem delegar as suas competências a terceiros, concessionar as suas atribuições e competências a provedores intermediários de serviços desde que:

a) a actividade da entidade delegada obedeça a lei e as regras fixadas pela entidade delegante;

b) a entidade delegada preste os seus serviços em nome próprio e responde, nos termos da Lei.

[2] Lei de transações eletrónicas, aprovada pela Lei n° 3/2017, de 9 de Janeiro.

Entidade Reguladora

"A Entidade Reguladora é uma instituição pública dotada de personalidade jurídica, autonomia administrativa e desempenha as suas funções em conformidade com a presente Lei, respectivo estatuto orgânico e demais legislação aplicável". Ibdi (artigo 11, número 1).

Segundo Ibdi (artigo 11, número 2 e 3), o Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC) é a Entidade Reguladora no âmbito da presente Lei, tendo a sua organização e funcionamento regulados pelo Estatuto Orgânico aprovado pelo Conselho de Ministros.

Proveedor intermediário de serviços

Segundo Ibdi (artigo 13), o provedor intermediário de serviços é aquele cuja responsabilidade é a materialização das competências atribuidas pelo provedor primário, isto mediante a atribuição de uma licença por parte deste. "O licenciamento para o exercício das actividades de provedor intermediário de serviços é da competência da entidade reguladora". Ibdi (artigo 13, número 2)

Responsabilidades dos orgãos

Entidade reguladora

Compete a Entidade Reguladora as seguintes responsabilidades, Ibdi (artigo 12, número 1) :

a) garantir o respeito e cumprimento da lei e os respectivos regulamentos;

b) apresentar proposta de regulamentos e outros diplomas de implementação da presente Lei, dentro dos limites da lei;

c) desempenhar as funções de regulação, supervisão e fiscalização;

d) assegurar a implementação do quadro de interoperabilidade do Governo Electrónico;

e) aplicar sanções decorrentes do incumprimento da presente Lei e demais legislação aplicável;

f) divulgar e promover a aplicação das transacções electrónicas, do comércio electrónico e do Governo Electrónico; g) licenciar os provedores intermediários de serviço;

h) emitir, modificar, renovar, suspender ou cancelar as licenças e registos estabelecidos na presente Lei;

i) assegurar a gestão do domínio ".mz";

j) assegurar a implementação e funcionamento do sistema de certificação electrónica do Estado;

k) proteger o consumidor no âmbito das transacções electrónicas, do comércio electrónico e do Governo Electrónico;

l) criar mecanismos de protecção da indústria e serviços nacionais de tecnologias de informação e comunicação;

m) emitir parecer sobre o licenciamento comercial das organizações comerciais na área das tecnologias de informaçãoe comunicação;

n) proceder à cobrança das taxas e multas;

o) propor ao Conselho de Ministros a actualização das taxas.

A Entidade reguladora ainda pode "exercer outras atribuições definidas no Estatuto Orgânico". Ibdi (artigo 12, número 2).

Provedor intermediário de serviços

Segundo a presente Lei, o Provedor intermediário de serviços tem as suas responsabilidades divididas em seis áreas: como emissor de serviços, receptor de serviços, receptor e emissor de serviços, entidade que zela pelo armazenamento da informação, monitor da informação, entidade que zela pelo resgito de identidade dos utilizadores.

Provedor intermediário de serviços como emissor de serviços

1. O provedor intermediário de serviços é responsável por garantir o acesso e assegurar a comunicação de informação transmitida pelos utilizadores a ele vinculados, através de uma rede ou sistema de comunicação.

2. O fornecimento do acesso e de transmissão da informação emitida pelos utilizadores que, incluem o armazenamento automático, intermediário e passageiro de informação transmitida numa rede de comunicação de dados, até ao termo do período definido para a sua transmissão.

3. O provedor intermediário deve manter em sigilo e confidência todas as comunicações de informação transmitidas pelos utilizadores a si vinculados, não podendo divulgar, fornecer ou utilizar em prejuízo dos utilizadores.

4. O provedor intermédio pode, mediante decisão judicial ou decisão administrativa, devidamente fundamentada, fornecer comunicações de informações que tenham conteúdo criminoso ou que atentem contra a segurança do Estado. Ibdi (artigo 14).

Provedor intermediário de serviços como receptor de serviços

"O provedor intermediário de serviços é responsável por garantir o acesso e assegurar a comunicação de informação recebida, destinada aos utilizadores a ele vinculados, através de uma rede ou sistema de comunicação de dados". Ibdi (artigo 15).

Provedor intermediário de serviços como emissor e receptor de serviços

O provedor intermediário de serviços deve, Ibdi (artigo 16):

a) manter a integridade da informação que recebe e transmitir na sua qualidade de provedor intermediário;

b) abster-se de utilizar ou passar para terceiros dados ou informação enviada ou destinada aos utilizadores a ele vinculados, salvo por decisão judicial;

c) evitar a remoção ou desactivação do acesso à informação armazenada;

d) responder pelos danos e prejuízos causados aos utilizadores, no âmbito do dever de sigilo e protecção de dados e informações destes.

Provedor intermediário de serviços como entidade que zela pelo armazenamento da informação

1. O provedor intermediário de serviços é responsável pelo armazenamento de informação para os utilizadores ou destes para outros a ele vinculados, sem prejuízo do dever de protecção e sigilo a que está adstrito.

2. O disposto no número anterior não se aplica aos casos em que o receptor do serviço age sob ordem legal da autoridade competente do provedor.

3. O disposto no presente artigo não afecta as decisões judiciais ou de autoridade administrativa competente. Ibdi (artigo 17):

Provedor intermediário de serviços como monitor da informação

1. O provedor intermediário de serviços não está sujeito à obrigação geral de monitorar a informação que transmita ou armazene, nem de procurar factos ou circunstâncias indicativas de actividade ilegal.

2. Sem prejuízo do disposto no número 1, o provedor intermediário de serviços deve colaborar, no sentido de:

a) informar às autoridades públicas competentes das actividades ilegais detectadas;

b) apresentar às autoridades competentes, a pedido destas, informação que permita a identificação de receptores de serviços que tenham contratos de armazenagem;

c) obter e manter dados que permitam a identificação dos provedores de serviço que contribuíram para a criação de conteúdos integrados em serviços por si prestados a terceiros;

d) identificar os utilizadores que transmitem ou armazenem dados com conteúdo ofensivo, usando o serviço de comunicação com remetente não identificado;

e) agir de imediato, sem quaisquer outras formalidades, perante denúncia, queixa ou informação de furto, roubo, perda ou desaparecimento de meios eletrónicos feitos pelo utilizador com o objectivo de recuperar ou impedir ou seu uso ilícito.

3. Para efeitos do disposto na alínea e) do número anterior, o utilizador é obrigado a informar o provedor intermediário de serviço sobre furto, o roubo, a perda ou desaparecimento de meios electrónicos na sua posse e uso. Ibdi (artigo 18).

Provedor intermediário de serviços como entidade que zela pelo resgito de identidade dos utilizadores

Em relação a este ponto, “os provedores intermediários devem registar e identificar os seus utilizadores, nos termos a regulamentar”. Ibdi (artigo 19) Os provedores de serviços, caso o pretendam, ainda podem fornecer serviços de certificação, desde o momento que eles sejam devidamente acredidados e cumpram com as suas responsabilidades como agentes de certificação.

Acreditação de provedores de serviços de certificação

Para a acreditação de provedores de serviços de certificação, deve-se comprir com os seguintes presupostos, Ibdi (artigo 59):

1. Todo o provedor de serviços de certificação que pretenda emitir certificados qualificados está sujeito a uma acreditação emitida pelos serviços competentes.

2. A acreditação pode ser conferida a um provedor de serviços de certificação, que, cumulativamente, cumprir os seguintes requisitos:

a) demonstrar segurança necessária para a prestação de serviços de certificação;

b) garantir a operação de um directório rápido, seguro e de serviços de revogação imediatos;

c) garantir que a data e hora em que um certificado é emitido ou revogado pode ser determinada com precisão;

d) verificar através de meios adequados de acordo com a legislação pertinente, a identidade, e, caso seja aplicável, quaisquer atributos especiais da pessoa a favor de quem é emitido o certificado qualificado;

e) contratar pessoal que tenha conhecimento, experiência e qualificações necessárias para os serviços prestados;

f) utilizar sistemas e produtos fiáveis que são protegidos contra modificações e que garantam segurança técnica de codificação do processo;

g) tomar medidas contra a falsificação de certificados nos casos em que o provedor de serviços de certificação gere dados de criação de assinatura, garantir a confidencialidade durante o processo de geração dos referidos dados;

h) tiver recursos financeiros suficientes para operar em conformidade com os requisitos estabelecidos na presente Lei, em particular no que concerne à assunção de responsabilidade por danos;

i) registar electronicamente toda a informação relevante relativa a um certificado qualificado para um período de tempo apropriado, com o objectivo de fornecer provas da certificação para efeitos de procedimentos legais;

j) não armazenar ou copiar dados de criação de assinaturas da pessoa a quem o provedor de serviços de certificação presta serviços chave de gestão;

k) antes de entrar numa relação contratual informar a pessoa sobre os termos e condições acerca da utilização do certificado incluindo limitações da sua utilização;

l) utilizar sistemas fiáveis para armazenar os certificados de uma forma verificável, por forma a que:

i) só pessoas autorizadas podem aceder para fazer introduções e alterações;

ii) a informação poder ser verificada no que concerne a autenticidade;

iii) os certificados estarem publicamente disponíveis para acesso só nos casos em que o consentimento do portador do certificado tenha sido obtido;

iv) quaisquer alterações técnicas que comprometam os requisitos de segurança sejam aparentes para o operador.

SEGURANÇA DA INFORMAÇÃO

Informação

"Dados que foram transformados, manipulados e organizados e que tem valor para apoio na tomada de decisão", por exemplo: O aluno está dispensado por ter atingido 14 valores de média. Fedeli, et.al. (2010), citado por SABBEN[3]. Na gestão empresarial moderna, a informação é tratada como um importante activo[4] da empresa. Essa informação pode ser impressa, manuscrita, gravada em meios magnéticos, ou simplesmente ser do conhecimento dos funcionários (falada). A informação pode ser classicada quanto aos seguintes critérios : confidencialidade, integridade, disponibilidade, ou ainda, ela pode ter uma classificação padrão.

Características da informação

Uma informação de qualidade deve ter basicamente as seguintes características, conecidas pela sigla (ACID): Atempada: deve ser fornecida no tempo certo e oportuno; Confidencial: não deve ser acedida por pessoas não devidamente autorizadas; Íntegra: não deve ser alterada, apagada sem autorização, etc.; E disponível: deve ser acessível sempre que for necessitada. Portanto,

[3]SEBBEN, A., et al. Introdução a informática: uma abordagem com libreoffice. Universidade Federal da Fronteira Sul. Chapaco-UEFS, 2012.

[4] Activo é qualquer elemento que tenha valor para uma determinada organização, exemplo: a sua imagem, as suas intalações, o seu pessoal, o seu capital, os seus dados, etc.

para uma informação de qualidade, as organizações e as demais entidades devem criar as condições necessárias para o comprimento das características acima descritas, facto que torna o processo de gestão de informação bastante útil.

Segurança da informação Seguranca da informação, ou Segurança de sistemas de informação "é a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidade de negócios" [ISO 27002].
"É a área do conhecimento dedicada á protecção dos activos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade" Idem.

Princípios básicos da segurança da informação

Confidencialidade: Certeza de que o que foi dito, escrito ou falado será acedido somente por pessoas autorizadas;
Integridade: Garantia de que a informação não foi alterada (de forma indevida ou não autorizada); Disponibilidade: Garantia de que a informação será acedida quando necessário; As organizações, para que tenham garantia de prestação de serviços de qualidade, sua manunteção, etc., devem definir políticas sólidas de segurança de informação. Esta prática vai permitir minizar o número de vulnerabilidades[5] sujeitas aos seus activos, e sobretudo minimizar o impacto no caso de haver certas ameaças[6] que explorem devidamente essas vulnerabilidades.

Cibersegurança

Cibersegurança (também chamada Segurança Cibernética), refere-se às práticas empregadas para garantir a integridade, confidencialidade e disponibilidade da informação. Ela é composta por um conjunto de ferramentas, abordagens de gestão de risco, tecnologias, treinamento e métodos para proteger redes, dispositivos, programas e dados contra ataques ou acesso não autorizado. Cibersegurança é o conjunto de tecnologias , processos e práticas desenhado para proteger as redes, os computadores e outros dispositivos electrónicos, programas e dados, de potencias ataques ou ameaças. Na prática, garantir segurança cibernética em uma

[5] É uma fraqueza sujeita aos activos da organização que pode ser explorada por uma ameaça.
[6] É um evento, ou uma força externa que pode explorer uma vulnerabilidade podendo quebrar os princípios básicos da Segurança de informação, facto que pode colocar em risco a saúde da organização.

empresa/organização, por exemplo, requer a coordenação de esforços em todo o sistema de informação, que inclui: Segurança de aplicativos; Segurança da informação; Segurança de rede; Recuperação de desastres/planeamento de continuidade de negócios; Segurança operacional; Educação do utilizador final.

Ameaças mais comuns no ciberespaço

As ameaças mais comuns no ciberespaço são: virus, phishing, keylogger, spyware, ransomware, botnet, clickjacking, negação de serviços, SQL Injection, etc.

Como evitar ataques de segurança cibernética

Com tantas ameaças por aí, é essencial aprender como se proteger de violações de segurança cibernética. Para se proteger de tais riscos, é importante ter uma base sólida de segurança cibernética que atenue o risco de um ataque. Além disso, existem algumas dicas que devem ser úteis para todos que usam a rede e todos os tipos de dispositivos da Internet: Instale e actualize regularmente o software antivírus para todos os computadores usados nos negócios, em casa ou em outros locais. Faça uma pequena pesquisa e encontre o melhor provedor de protecção na internet e não compre o software mais barato: Proteja sua conexão à Internet usando um firewall; Faça cópias de segurança para dados importantes e mantenha-os em segurança; Treine funcionários ou familiares em segurança cibernética e seus princípios; Altere regularmente senhas e use senhas robustas. Uma senha robusta contém letras minúsculas, maiúsculas, caractéres especiais e números. É recomendável não torná-lo uma palavra, apenas uma combinação aleatória. Actualize regularmente o software e os sistemas operacionais e; Proteja a rede.

Portanto, para além destas responsabilidades por parte das empresas para a garantia de um espaço cibernético seguro, também os países ao nível mundial vem emplementando várias estratégias para tornar esse bem precioso e ideal uma realidade, como é o caso de Moçambique. É por estas razões, que o nosso país acabou avaçando com uma proposta conhecida como "Estratégia nacional de segurança cibernética de moçambique", que preconiza várias estratégias para proporcionar ao nosso país, as organizações e ao público em geral, um espaço cibernético saudável e seguro.

Estratégia nacional de segurança cibernética de Moçambique

Princípios de orientação Segundo esta proposta os princípios que sustentam esta estratégia são, (ENSC:12): i. Legalidade: A ENSC de Moçambique tem em conta as diversas leis em vigor em Moçambique e promoverá a protecção dos direitos, liberdades e garantias fundamentais dos moçambicanos. ii. Abordagem baseada em risco: A ENSC adopta uma abordagem baseada em risco na avaliação de respostas as ameaças e riscos cibernéticos, assegurando a Segurança Cibernética em Moçambique. iii. Cooperação e Coordenação: Esta Estratégia promove a coordenação e a cooperação entre as várias partes interessadas, tanto a nível nacional como internacional. iv. Responsabilidade partilhada e crime cibernético: A ENSC reconhece a responsabilidade individual e partilhada de todos os utilizadores das TIC (indivíduos, sector privado e Governo). v. Acesso universal ao espaço cibernético: A ENSC procurará assegurar que todos os cidadãos moçambicanos devem ter acesso e poder utilizar o espaço cibernético de forma segura, independentemente da localização, género, raça, situação económica, entre outros.

Objectivos Estratégicos

Segunto a proposta acima referênciada, para o alcance da visão[7] e missão[8] da ENSC, foram definidos 5 (cinco) objectivos estratégicos: I. Melhorar a protecção da infra-estrutura crítica de informação (ICI). II. Reforçar o quadro legal, técnico e operacional de segurança cibernética. III. Estabelecer um quadro nacional para promover a partilha de informação, Cooperação e Coordenação em matéria de segurança cibernética. IV. Desenvolver capacidade técnica de pesquisa e inovação em matéria de segurança cibernética. V. Criar uma cultura nacional de segurança cibernética. Para a materialização destes objectivos um série de acções deve ser levada a cabo. É importante realçar que essas acções são categorizadas em função de cada um dos objectivos estratégicos acima apresentados.

Mecanismos de implementação

Segundo a presente proposta, em Moçambique não existe uma estrutura organizacional adequada para a coordenação das políticas e intervenções de segurança cibernética a nível

[7]Uma nação com um espaço cibernético seguro, resiliente e uma sociedade consciencializada.
[8] Desenvolver a capacidade necessária e o ambiente de segurança cibernética que garanta um espaço cibernético seguro.

operacional e estratégico. Considerando que a garantia da segurança cibernética é material transversal e que abrange diferentes sectores da sociedade, há assim a necessidade de elaboração de uma abordagem integrada e coordenada em matérias relacionadas a segurança cibernética. Em resposta a tal necessidade, esta estratégia obriga o estabelecimento de um Conselho Nacional de Segurança Cibernética (CNSC) a nível estratégico.

Conselho Nacional Segurança Cibernética (CNSC)

Seus membros

Este conselho, dada a sensibilidade da área em que actua, acaba justificando-se o facto de ser composto por elementos bem complexos, que passamos a apresentar, (ENSC: 21): Ministro que superintende aárea da Defesa; Ministro que superintende aárea de ordem,segurança e tranquilidades públicas; Ministro que superintende a área da Justiça; Ministro que superintende a área das comunicações; Ministro que superintende aárea das tecnologias de informação e comunicação.

Seu papel

Analisar e orientar o Estado sobre assuntos e/ou outras matérias pertinentes que contribuam para a segurança cibernética; Elaborar estratégias para a criação de estruturas e políticas organizacionais nacionais e regionais adequadas em matéria de crime cibernético. Assegurar a criação de capacidade institucional com vista a garantir a Defesa Nacional contra ataques e crimes cibernéticos; Idem.

Para além CNSC, para a garantia de uma melhor implementação da ENSC, outras elementos são necessários, como é o caso dos seguintes: uma unidade de coordenação e implementação do ENSC, um finaciamento e recursos, e uma monitoria e avaliação. Portanto, todos estes elementos, quando bem associados, podem trazer bons resultados na implementaçao da ENSC.

Responsabilidade civil de provedores e segurança da informação

Todos provedores de serviços, no exercício das suas actividades devem procurar sempre garantir a sua própria segurança, bem como a segurança dos seus utentes visto que o tipo des serviços que eles fornecem é muito sensível na medida em que são sujeitos a vários ataques,

facto que pode compremeter a segurança da informação, influênciando negativamente a vida e saúde da organização assim como dos seus utentes. Portanto, ao abrigo Lei de transações eletrónicas, aprovada pela Lei n° 3/2017, de 9 de Janeiro.

Os provedores de serviço tem como umas das responsabilidades as seguintes: a garantia da confidencialidade, integridade e disponibilidade da informacao; que constituem os pilares básicos da segurança da informação.

exis tem várias espécies de provedores de internet, existindo, igual mente, distinções no que toca à responsabilidade civil dos diver sos provedores de internet: provedor de backbone, provedor de acesso, provedor de hospedagem, provedor de conteúdo, prove dor de busca ou pesquisa e provedor de correio eletrónico.

A responsabilidade civil dos provedores no tratamento de dados sensíveis emerge como uma área de pesquisa vital. Esta pes quisa é justificada pela necessidade imperativa de proteger as informações pessoais dos usuários, garantindo que os provedores operem dentro de um quadro legal que promova a segurança dos dados e a privacidade individual.

O legislador moçambicano trata, no Código Civil, as duas modalidades de responsabilidade civil em lugares distintos: ao passo que a responsabilidade contratual aparece nos arts. 798.º e segs., ou seja, encontra-se no capítulo que regula, ao lado do cumprimento, as formas e efeitos do não cumprimento das obrigações; a responsabilidade extracontratual está regulada nos arts. 483.º e segs, no capítulo das fontes de obrigações, secção "responsabilidade civil". Note-se que quanto ao regime da obrigação de indemnizar, o legislador tratou as referidas modalidades conjuntamente – arts. 562.º e segs –, estabelecendo um regime próprio da mencionada obrigação, que de ambas as modalidades é suscetível de emergir. Este é um lugar de confluência das consequências decorrentes das duas modalidades de responsabilidade, como que unificando o seu regime10. Neste sentido, temos regimes diferentes com a mesma consequência – a obrigação de indemnizar. Portanto, a responsabilidade civil contratual e a responsabilidade civil extracontratual não são compartimentos estanques, funcionando, por vezes até, como verdadeiros vasos comunicantes[9]. E, neste seguimento, casos haverá em que o mesmo facto jurídico irá despoletar ambas as modalidades de responsabilidade civil[10].

[9] Cfr. VARELA, João Antunes, Das Obrigações em Geral, Volume I, pp. 521 e 522.

[10] Imagine-se, a título de exemplo, que um farmacêutico, distraído, entrega um medicamento errado ao cliente: temos um caso de responsabilidade extracontratual, por violação do direito à integridade física; e, simultaneamente, um caso de responsabilidade contratual, por violação do contrato de compra e venda. Outros casos em que isto poderá acontecer é na responsabilidade médica em hospitais privados.

CONCLUSÃO

Concluir que, com o crescimento das TIC's bem como da Internet, o Governo moçambicano teve a necessidade de analizar e aprovar a criação de vários órgãos, para proporcionar aos cidadãos moçambicanos, mais serviços baseados nas TIC's bem como na Internet. É caso dos provedores de serviços de comunicação, e armazenamento de dados nas redes de computadores. Este órgão tem a sua origem na luz da aprovação da Lei de transações eletrónicas, aprovada pela Lei n° 3/2017, de 9 de Janeiro, que para alem de apresentar os provedores e as suas responsabilidades, descreve vários outros aspectos referentes à vários tipos de transações electrónicas.

Com vista a garatia de segurança nesse tipo de transações, bem como a segurança da informação e do domínio das TIC's no geral, uma proposta de estratégia nacional de segurança cibernética de moçambique foi avançada. Esta proposta apresenta as estratégias necessárias para a implementação da mesma, bem como os mecanismos de implementação, tudo com a finalidade de garantir a segurança da informação e um espaço cibernético seguro.

Portanto, a Segurança da informação é um processo que envolve todas as áreas de negócio de uma organização e deve ser entendida como mais uma disciplina orientada a atingir a missão estabelecida. A Segurança da Informação é obtida a partir da implementação de um conjunto de controlos adequados as necessidades da organização. Controlos precisam ser estabelecidos, implementados, monitorados, analisados e melhorados para garantir que os objectivos do negócio e de segurança sejam atendidos.

Na Responsabilidade civil do provedor, o provedor é responsabilizado civilmente por danos causados por terceiros e, é subsidiária. A qual, deve tomar providências para tornar indisponível o conteúdo infringente, após ordem judicial. O mesmo não é responsável pelo conteúdo gerado pelos usuários, a não ser que negligencie a remoção de conteúdos ilegais ou ofensivos.

REFERÊNCIAS

GAGLIANO, Pablo Stolze. Manual de direito civil. volume único. São Paulo: Saraiva, 2017.

JORGE, Fernando Pessoa. Ensaio sobre os pressupostos da responsabilidade civil. Lisboa: ALMEDINA, 1968.

LEONARDI, Marcel. Responsabilidade civil de provedores de serviços de internet. São Paulo: Juarez de Oliveira, 2005.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de direito constitucional. 6. ed. São Paulo: Saraiva, 2011.

PADRÃO, Vinicius Jóras. A Constitucionalidade do artigo 19 do Marco Civil da Internet: síntese do debate e um olhar para o futuro.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (org). Relações Patrimoniais: Contratos, Titularidades e Responsabilidade Civil. Fórum: Rio de Janeiro, 2021. PENSANDO O DIREITO. Liberdade de Modelos de Negócios. Disponível em: http://pensando.mj.gov.br/marcocivil/pauta/liberdade-de-modelos-de-negocios/. Acesso em: 16/01/2022. 63

PINHEIRO, Patricia Peck. Direito digital. 5. ed. rev., atual. e ampl. de acordo com as Leis n. 12.735 e 12.737, de 2012. São Paulo: Saraiva, 2013.

ROBERTO, Don Karl. Recent Developments in Canada's "Notice and Notice" Regime. Disponível em: https://ojs.lib.uwo.ca/index.php/uwojls/announcement/view/123. Acesso em: 04/02/2022.

RODOTÁ, Stefano. A vida na sociedade da vigilância. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang. Curso de Direito Constitucional. 6. ed. São Paulo: Saraiva, 2017.

SOPRANA, Paula. Supremo adia para 2020 julgamento sobre retirada de conteúdo da internet. Disponível em: https://www1.folha.uol.com.br/tec/2019/12/supremo-adia-para-2020-julgamento-sobre-retirada-de-conteudo-dainternet.shtml?fbclid=IwAR3m6R9VC4LLMX9Rix9GX-3Vlun4uP_-PYlINCW6gwgywPamt7mJy7I1xaA. Acesso em: 09/02/2022.

SOUZA, Carlos Affonso Pereira de. As cinco fases da proteção à liberdade de expressão no Marco Civil da Internet. Disponível em: http://site.fdv.br/wp-content/uploads/2019/08/Artigo-Cinco-Faces-da-Liberdade-de-Express%C3%A3o-no-Marco-Civil-da-Internet-Carlos-Affonso.pdf. Acesso em: 05/02/2022.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. Marco Civil da Internet: construção e aplicação. Juiz de Fora: Editar Editora Associada, 2016.

TEFFÉ, Chiara Spadaccini de; SOUZA, Carlos Affonso. Responsabilidade civil de provedores na rede: análise da aplicação do Marco Civil da Internet pelo Superior Tribunal de Justiça. Revista IBERC, Minas Gerais, v. 1, n. 1, p. 01-28, nov./fev. 2019.

Legislação Nacional

BOLETIM DA REPÚBLICA, Lei de transações eletrónicas, aprovada pela Lei n° 3/2017, de 9 de Janeiro. Publicação Oficial da República de Moçambique: Maputo.

Proposta da Estratégia nacional de segurança cibernética de moçambique.