Crimes cibernéticos e segurança cibernética em Moçambique

Vanessa Pires
Associada
da MDR Advogados

Geth dos Santos Tangune
Advogada Estagiária
da MDR Advogados

As tecnologias de informação revolucionaram a maneira como vivemos e fazemos negócios. Com o surgimento da pandemia da COVID-19 e as necessidades de distanciamento físico entre as pessoas, a tendência tem sido de aumento do tráfego de internet e de aumento do número de assinantes de telefonia celular, bem como de provedores e utilizadores de plataformas digitais.

O crescente acesso aos serviços das tecnologias de informação e comunicação, incluindo a internet, traz muitas oportunidades de desenvolvimento. No entanto, este aumento é também acompanhado de crescentes vulnerabilidades a que o cidadão está sujeito, crescendo com isto os crimes cibernéticos.

O Relatório da União Internacional de Telecomunicações (UIT) sobre o Índice Global de Segurança Cibernética (GCI) de 2018 colocou Moçambique entre os países com o pior nível de segurança cibernética, tendo por base a análise das medidas legais, técnicas e organizacionais e o desenvolvimento de capacidades e de cooperação internacional. Por isso, num *ranking* de 194 países, Moçambique ocupou as posições 26 e 132, no índice continental e global respectivamente. No relatório do GCI de 2020, divulgado entretanto pela UIT, Moçambique subiu nove posições, tendo passado da posição 132 para a posição 123, numa lista com 193 países avaliados.

No âmbito legal, nota-se que a consciência da ameaça e dos efeitos negativos dos crimes cibernéticos sobre a nação e sobre os cidadãos moçambicanos tem crescido e têm sido feitos esforços para garantir que há instrumentos de protecção ao cidadão e que penalizam quem comete crimes com recurso a tecnologias de informação e comunicação.

Em relação à segurança cibernética, destaca-se que Moçambique ratificou, através da Resolução n.º 5/2019, de 20 de Junho, a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais (CUACPDP), adoptada pela 23.ª Sessão Ordinária da Cimeira dos Chefes de Estado e de Governo da União Africana, a 27 de Junho de 2014, em Malabo, na Guiné Equatorial.

Importa referir que, embora a CUACPDP tenha sido introduzida em Moçambique após a sua ratificação em 2019, a respectiva adesão ocorreu já em 2014, tendo alguns diplomas legais sobre o tema sido aprovados antes da sua ratificação.

A CUACPDP fixa as normas de segurança essenciais para a criação de um espaço digital credível para transacções electrónicas, para o reforço dos direitos fundamentais, nomeadamente a protecção de dados pessoais bem como a promoção da cibersegurança, e para a luta contra o cibercrime. O instrumento visa igualmente reforçar a legislação existente nos países membros em matéria de tecnologias de informação e comunicação. Os países membros devem também garantir a segurança nas transacções electrónicas. A este respeito, importa referir que foi aprovada a Lei n.º 3/2017, de 9 de Janeiro (a Lei das Transacções Electrónicas), que estabelece o regime jurídico das transacções electrónicas em geral, do comércio electrónico e do governo electrónico em particular, visando garantir a protecção e a utilização das tecnologias de informação e comunicação. Esta lei estabelece também o regime sancionatório das infracções cibernéticas, garantindo a protecção do consumidor.

"[...] Moçambique tem vindo a desenvolver uma série de instrumentos com vista a garantir a segurança cibernética, a protecção contra os crimes cibernéticos e a adequação destes instrumentos à evolução das tecnologias no país, bem como a sua penalização."

No âmbito da promoção da segurança cibernética e da luta contra o crime cibernético, determina a CUACPDP que cada Estado parte deve desenvolver uma política nacional de cibersegurança, de modo a identificar os riscos que o país enfrenta e a definir como se podem alcançar os objectivos dessa política. Os Estados parte devem também adoptar estratégias suficientes para a implementação da política nacional de cibersegurança. O Governo moçambicano aprovou a Política Nacional de Segurança Cibernética e a Estratégia Nacio-

nal de Segurança Cibernética através da Resolução n.º 69/2021, de 31 de Dezembro.

Relativamente às medidas legislativas, estabelece o artigo 25.º da CUACPDP que cada Estado parte deve adoptar as medidas legislativas e/ou regulamentares que julgar adequadas e eficazes, considerando como infracções criminais os actos que afectem a confidencialidade, a integridade, a disponibilidade e a sobrevivência dos sistemas das tecnologias de informação e comunicação. Neste contexto, é relevante mencionar que o Código Penal, aprovado pela Lei n.º 24/2019, de 24 de Dezembro, prevê crimes relativos a instrumentos de pagamento electrónico, sendo que o artigo 294.º versa sobre fraudes relativas aos instrumentos e canais de pagamento electrónico. Nos termos deste artigo, constitui crime o acesso ilegal a um sistema de pagamento electrónico mediante a violação indevida dos mecanismos de segurança. Este artigo penaliza também a criação de programas informáticos e outros meios preparados deliberadamente para a prática de infracções relacionadas com instrumentos de pagamentos electrónicos. A Secção IV do Título IV do Código Penal versa também sobre crimes de falsidade informática e crimes conexos, como a interferência em dados informáticos, a instalação de vulnerabilidades que interfiram no funcionamento de sistemas informáticos e o uso abusivo de dispositivos (artigos 336.º a 339.º do Código Penal).

O Decreto n.º 90/2020, de 9 de Outubro, aprova o Estatuto Orgânico do Instituto Nacional de Tecnologias de Informação e Comunicação, IP, incluindo a Divisão de Segurança Cibernética e Protecção de Dados que tem, entre outras, a função de criar capacidade nacional de prevenção, de monitorização e de combate a incidentes de segurança cibernética.

No plano legal, Moçambique tem vindo a desenvolver uma série de instrumentos com vista a garantir a segurança cibernética, a protecção contra os crimes cibernéticos e a adequação destes instrumentos à evolução das tecnologias no país, bem como a sua penalização. Porém, surgem várias dificuldades, principalmente no que concerne à criação de medidas para a protecção contra os ataques cibernéticos, como, por exemplo, a protecção contra *softwares* maliciosos e medidas para melhorar a atribuição de responsabilidades por esses ataques.

Embora Moçambique tenha ratificado a CUACPDP, a cooperação internacional em cibersegurança, especialmente no âmbito da Comunidade de Desenvolvimento da África Austral e da União Africana, constitui ainda um desafio.

De acordo com um relatório publicado pela Procuradoria-Geral da República, constitui igualmente um enorme desafio a capacitação dos técnicos das autoridades de justiça criminal em matérias de crimes informáticos e de recolha de provas digitais, de modo a que estes estejam à altura de lidar com estas matérias.

Em suma, a segurança cibernética é actualmente de extrema importância para o país, no sentido de garantir que o ciberespaço é utilizado com segurança tanto pelo Governo como pelo sector privado, pela sociedade civil e pelas demais instituições.