MOÇAMBIQUE

Policy Brief

Processo de legislação sobre Direitos Digitais, em Moçambique, deve garantir a protecção de dados, a privacidade e reduzir riscos de vigilância digital

Este policy brief fundamenta e mostra que, num momento em que o país avança para produzir as leis sobre Cibersegurança, Crimes Cibernéticos (Cibercrimes) e Protecção de Dados, o processo deve ser orientado e inspirado por padrões legislativos considerados modelos (os casos da Declaração de Malabo, leis das Maurícias e Directivas da EU sobre protecção de dados), como forma de garantir que elas respeitem os direitos às privacidades e reduzam os riscos de vigilância massiva. Por outro lado, a aprovação destas leis deve ser seguida por um conjunto de reformas institucionais, revisão e revogação de instrumentos contrários, como as Leis número 12/2012 e 13/2013; os artigos 18 e 9 da nova Lei das Telecomunicações (Lei número 4/2016), assim como o número 4 do artigo 14 da mesma lei; e artigo 15 da Lei (nº 4/2021) da Autoridade Reguladora de Comunicações.

Por Ernesto C. Nhanale[1]

Depois de muito tempo atrasado, Moçambique anda, nos últimos dois anos, num passo acelerado para o desenvolvimento de um quadro legal sobre a Cibersegurança, Crimes Cibernéticos (Cibercrimes) e Protecção de Dados. Trata-se de um conjunto de leis que buscam responder aos desafios regulatórios do incontornável e omnipresente processo de digitalização da sociedade, nos seus diversos níveis de domínio de vida, desde os processos produtivos, sociais, económicos, políticos, culturais, militares, judiciais, etc.

A urgência destas leis releva-se, não somente em resposta a um movimento global de produção legislativa, em matérias de direitos digitais, em que diversos organismos internacionais aprovam leis-modelos para orientarem os estados membros nos processos legislativos nacionais. A título de exemplo, a União Africana aprovou, em 2012, a Convenção de Malabo[2], desafiando os Estados membros a subscreverem um quando legal e de políticas Nacionais para Cibersegurança e Protecção de Dados, sendo que diversos países africanos, a exemplo de Maurícias, Botswana e Tanzânia e, a nível dos PALOP, Cabo Verde, desenvolveram, entre os anos 2010 a 2020, as suas leis sobre as questões em voga.

Para além do movimento político global, a urgência destas leis – o caso específico de Cibersegurança e Crimes Cibernéticos – são fundamentadas na aceleração dos crimes cibernéticos de que o país tem vindo a ser alvo, que chegam a atingir cerca de 1.5 milhões de casos mensais[3], em resultado das suas vulnerabilidades e do seu baixo nível de resposta aos desafios impostos pela transformação digital. O nível crítico sob o qual o nosso país ainda se encontra, tem sido revelado em diversos índices globais de avaliação das questões de Cibersegurança. A última edição do National Ciber Secutiry Index mostra que Moçambique ocupa a posição 157, no total de 176 países avaliados. Nos seus diversos indicadores, o National Ciber Secutiry Index faz uma avaliação negativa ao país no processo de desenvolvimento de estratégia e políticas sobre a Cibersegurança e a Protecção de Dados, embora mencione os artigos 65 – 65 da Lei de transacções electrónicas[4]. Uma outra avaliação importante tem sido feita pela União Internacional das Telecomunicações que, na sua última edição, através do Índice Global de Cibersegurança de 2020, mostra que Moçambique situava-se na posição

1 *Director Executivo do MISA-Moçambique, exercendo as funções de Professor de Media e Jornalismo. Nos últimos anos, enquanto pesquisador, tem vindo a investigar sobre o impacto da digitalização na vigilância e violação dos direitos à privacidade, estando ligado ao Projecto de Pesquisa "Public oversight of digital surveillance for intelligence purposes: a comparative case study analysis of oversight practices in Southern Africa" implementado sob as auspicias da British Academy Global Pressorrship sedeado pela* University of Glasgow, *sob o qual tem vindo a desenvolver estas análises.*

2 *Moçambique ratifica a Convenção da União Africana sobre Cibersegurança e a Protecção de Dados Pessoais, em 2019, através da resolução nº 5/2019.*

3 *Mais detalhes leia: "Moçambique sofre 1.5 milhões de ataques de cibersegurança mensais", https://cartamz.com/index.php/sociedade/item/14301-mocambique-sofre-1-5-milhao-de-ataques-de-ciberseguranca-mensais, acessado aos 05 de Novembro de 2023.*

4 *Para mais informação veja o NCSI – National Cyber Security Index em https://ncsi.ega.ee/country/mz/, consultado a 02 de Novembro de 2023.*

123 do total 194, com 24.18 pontos dos 100 disponíveis. O GCI também as questões do desenvolvimento do quadro legal, em Moçambique, como inclusivamente críticas sobre os indicadores de segurança cibernética[5].

Sob ponto de vista da protecção de dados pessoais, pode-se destacar que a sua imperatividade marca-se pelo facto de a digitalização ter vindo revelar e provado uma tendência tenebrosa da sua utilização para a vigilância massiva, assim como o uso abusivo dos dados dos cidadãos para fins comerciais e políticos. No contexto Nacional, a par da aceleração da digitalização dos sectores sociais, factores como a deterioração da democracia, das liberdades de expressão[6], a cultura de vigilância política, os investimentos em tecnologias de vigilância pública e privada, e a insurgência em Cabo-Delgado têm sido considerados elementos críticos sobre a urgência de um quadro legal específico, assim como a implementação de medidas e reformas institucionais para assegurar a protecção de dados pessoais[7].

Para além de responder ao contexto global e às questões críticas supracitadas, o desenvolvimento das leis sobre Cibersegurança, Crimes Cibernéticos (Cibercrimes) e Protecção de Dados surgem como resposta de regulamentação dos direitos Constitucionais à Segurança e à protecção dos dados pessoais, previstos nos artigos 41, 71 e outros. Foi por isso que o Governo, no seu Programa Quinquenal 2020-2024, num "despertar tardio", abriu-se à empreitada legislativa[8], como resposta ao previsto na Política da Sociedade de Informação (2018) para "criar políticas e legislação no âmbito da segurança cibernética"[9], bem assim na necessidade de se "promover a adesão de Moçambique a políticas, instrumentos legais e convenções regionais e internacionais sobre a sociedade da informação"[10].

O MISA Moçambique, desde 2020, tem vindo a participar e a contribuir directamente no processo de desenvolvimento das leis. Entre 2021 e 2022, o MISA tem vindo a participar activamente nos trabalhos desenvolvidos pela equipa do INTIC – Instituto Nacional de Tecnologias de Informação e Comunicação, entidade tutelada pelo Ministério de Ciência, Tecnologia e Ensino Superior, sendo que, ao longo deste período, foi finalizado, em Agosto de 2023, o *draft* da Lei de Cibersegurança, seguindo-se os comentários para a Lei de Cibercrimes e, conforme disse o PCA do INTIC, na sessão de encerramento da última reunião de auscultação para a Lei de Cibersegurança, já foram dados passos significativos para que se inicie o processo de desenvolvimento do *draft* da lei sobre protecção de dados pessoais.

As diversas análises produzidas pelas equipas de especialistas do MISA, sugerem que existem questões críticas que os actores envolvidos no processo de desenvolvimento destas propostas, assim como as diversas entidades governamentais e o Parlamento devem tomar em atenção, por forma a garantir que, ao serem aprovadas, não sejam viciadas de elementos que conduzem à formalização da vigilância digital, a exemplo do que aconteceu em Zimbabwe, onde as organizações cívicas engajaram-se activamente para a produção destas leis, todavia, os resultados finais foram para além do que se pretendia.

Estas questões críticas dividem-se em dois níveis: o primeiro tem a ver com a existência de instrumentos legais, actualmente vigentes que colidem com os propósitos de protecção de dados, sendo promotores da vigilância, devendo, por recomendação, ser revistos ou revogados para que as novas leis sejam efectivas. Por outro lado, algumas normativas e propostas feitas nas actuais leis em desenvolvimento, em especial o *draft* da Lei de Cibersegurança devem carecer de atenção particular, por forma a evitar que sejam usadas para a vigilância massiva.

O quadro legal e institucional a ser revisitado:

Sobre o primeiro aspecto ligado à existência, no ordenamento jurídico moçambicano, dalgumas leis ordinárias que, de certa forma, se mostram contrárias a alguns princípios fundamentais estabelecidos na Constituição, o MISA cita no policy brief publicado a 15 de Setembro de 2020 dois casos cruciais:

1. Do novo regime jurídico do Serviço de Informação e Segurança do Estado (SISE), introduzido pelas Leis números 12/2012 e 13/2013, que dá poderes ao director-geral do SISE de interceptar as comunicações dos cidadãos, sem sequer estar previsto um protocolo sobre como os dados do cidadão são depois geridos e/ou acondicionados;

2. Da Lei das Transacções Electrónicas (Lei número 3/2017) e da nova Lei das Telecomunicações (Lei número 4/2016), que permitem, respectivamente nos seus artigos 18 e 19, que autoridades administrativas possam ter acesso a dados confidenciais de particulares/cidadãos, qual quebra da privacidade e a protecção de dados pessoais.

Acresce-se dois elementos que publicámos, previamente, num relatório sobre os riscos de vigilância electrónica em Moçambique, que passamos a citar:

1. A existência de disparidades e conflitos sobre as situações em que informações devem ser disponibilizadas

5 *Mais detalhes obre o GCI siga o link: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E, acessado aos 05 de Novembro de 2023.*

6 *Vide os relatórios do MISA-Moçambique sobre as liberdades de Imprensa e de Expressão - https://www.misa.org.mz/index.php/publicacoes/relatorios/relatorio-2008/143-relatorio-sobre-a-liberdade-de-imprensa-e-dh-em-mocambique-2022, acessado aos 02 de Novembro de 2023.*

7 *Precisamos de assinalar que, para além da CRM, Moçambique tem um quadro solto de leis, artigos embutidos em algumas leis e instrumentos sobre a protecção de dados, o caso dos artigos 65 – 65 da Lei de transacções electrónicas (lei nº 3/2017) e o decreto nº 44/2019 de "Protecção do Consumidor do Serviço de Telecomunicações.*

8 *Para detalhes, ver Resolução número 15/2020. De 14 de Abril.*

9 *Página 32.*

10 *Página 33.*

pelos provedores intermédios, no âmbito dos actuais dispositivos sobre a protecção de dados dispersos. Por exemplo, mesmo que a Lei nº 03/2017 das transacções electrónicas obrigue ao sigilo dos provedores intermediários[11] dos serviços de transmissão de dados, ela abre espaço para que tais informações sejam oferecidas fora do mandado judicial, não somente para fins criminais, conforme refere o número 4 do artigo 14: "o provedor intermédio pode, mediante decisão judicial ou decisão administrativa, devidamente fundamentada, fornecer comunicações ou informações que tenham conteúdo criminoso ou que atentem contra a segurança do Estado". Esta abertura à concessão da informação para autoridades não judiciais, abre espaço para que a informação de índole pessoal seja fornecida com base em ordens administrativas sob argumento de segurança do Estado, num contexto em que a noção de segurança do Estado[12] encontra-se, ela própria, difusa[13].

2. Igual ao ponto anterior, a Autoridade Reguladora de Comunicações, no quadro das suas atribuições, pode aplicar medidas administrativas para obrigar aos operadores, por si tutelados, providenciarem informações, conforme a alínea d) do artigo 15 da Lei que a funda (nº 4/2021): "emitir instruções administrativas para os operadores, prestadores de serviços e demais utilizadores dos recursos de frequências radioeléctricas e numeração de telecomunicações, desde que não interfiram na gestão privada e nos direitos e liberdades, por lei definidos, salvo justo receio de crime ou perigo de segurança do Estado". Esta atribuição, para além de proibir, permite a ingestão na privacidade e institui a vigilância, por completo, pois, não sendo necessário que haja indícios, desde que a ARECOM entenda que haja receios, mesmo sem mandado do juiz/tribunal, pode aplicar uma medida administrativa para o acesso aos dados privados.

O aspecto crucial a ser retirado do draft da Lei de Cibersegurança:

Mesmo depois de terem sido feitos muitos alinhamentos na proposta, no texto final proposta a que tivemos acesso, chamou maior atenção a questão da previsão de regimes aplicáveis à conservação e acesso a metadados (isto é, aos dados sobre dados) relativos às comunicações electrónicas (Artigos 33 a 38 da respectiva proposta). Conforme a análise feita, as matérias propostas nos artigos 33 a 38 não têm que ver com Segurança Cibernética, salvo incidentalmente, revelando um aproveitamento político da ocasião para inserir regras que deveriam estar numa Lei sobre Protecção de Dados Pessoais, numa Lei sobre Cibercrime, desde que esta contenha também regras sobre investigação e acesso às provas, ou no Código de Processo Penal.

Em todos os casos, é indispensável estarem previstas garantias em termos de tipos e gravidade dos crimes, assim como um controlo judicial prévio para o acesso aos metadados, inclusive com um especial dever de fundamentação no *draft* da proposta de lei de Cibersegurança. De outro modo, as "autoridades", incluindo as Polícias e os Serviços de Informações, ficam habilitadas a monitorizar, em tempo real ou diferido, a vida de cada cidadão, nomeadamente se este tiver um telemóvel com acesso à *Internet*, incluindo redes sem fios: onde estava, com quem se comunicou e que conteúdos viu em-linha. Foi por uma situação similar que na União Europeia, por exemplo, mesmo com todas essas garantias e limitando a possibilidade de acesso ao combate ao terrorismo e à criminalidade grave, o Tribunal de Justiça da União Europeia (Acórdão proferido no Processo *Digital Rights Ireland*, de 8 de Abril de 2014) anulou a Directiva de 2006 que o permitia, por incompatibilidade com a *Carta dos Direitos Fundamentais da União Europeia.*

11 No âmbito da Lei 02/2017, o provedor intermediário de serviços define-se como "qualquer pessoa que, em representação de outra, envia, recebe ou armazena mensagens de dados. São aqueles que prestam serviço de acesso à rede ou que prestam serviços a partir dela (provedores de acesso, provedores de conteúdos, provedores de aplicativos e provedores de hospedagem).

12 Lei número 19/91, de 18 de agosto (Lei dos Crimes contra a Segurança do Estado). Maputo: Imprensa Nacional.

13 A noção da "segurança do Estado" em Moçambique tem sido muito contestada, sobretudo porque a Lei nº 19/91 que a define ser difusa, estabelecendo, no seu artigo 22, que a difamação ao PR, ministros, juízes do Tribunal Supremo e mesmo secretários-gerais de partidos políticos é considerada crime contra a segurança do Estado, a que cabe uma pena entre um a dois anos de prisão. Isto significa que, em nome da "segurança do Estado" pode-se solicitar comunicações normais dos cidadãos, sempre que elas se refiram a críticas às figuras que as protegem.