Registo biométrico de cartões SIM: que riscos para protecção de dados dos cidadãos e vigilância indevida?

Este artigo surge com o intuito de contribuir para um debate sobre o uso responsável das tecnologias de comunicação e informação que, fora da esperança que muitos haviam depositado nos seus primórdios de ampliarem o espaço público, a participação e o acesso à informação; estão a transformar-se em instrumentos de manipulação, desinformação e de vigilância massiva indevida.

Ernesto C. Nhanale[1]

Em muitos países, sobretudo nos contextos mais autoritários, com limitada cultura de liberdades de expressão e de direitos humanos, o avanço de digitalização e conectividade tem sido acompanhado por um processo regulatório frágil e permeável para a vigilância indevida sobre a vida privada dos cidadãos e, por vezes, por baixos mecanismos de prestação de contas e de transparência das entidades que gerem dados dos cidadãos. Tais violações têm, em muitas ocasiões, sido feitas num ambiente de uma regulação frágil em matérias de respeito dos direitos humanos em benefício da vigilância indevida e de comercialização de informação pessoal para fins económicos, antidemocráticos ou políticos, facilitando a manipulação da opinião pública ou mesmo para que actores políticos de governos autoritários vigiem os seus opositores ou mesmo activistas da Sociedade Civil que se lhes opõem às suas más práticas de governação.

O nosso interesse em introduzirmos e participarmos neste debate preza-se com as recentes medidas regulatórias introduzidas em Moçambique, através do Decreto 13/2023, de 11 de Abril, que regula o Registo dos Serviços de Telecomunicações, estabelecendo normas ao processo de registo dos subscritores dos serviços de telecomunicações a serem observadas pelos operadores destes serviços, seus agentes distribuidores e/ou revendedores, entidades públicas, privadas, pessoas singulares detentoras e utilizadoras de dispositivos de comunicações, com base nos serviços de telecomunicações.

Conforme a publicação da Agência de Informação de Moçambique (AIM), a 16 de Janeiro de 2024, o Instituto Nacional de Comunicações de Moçambique (INCM) iniciou, em regime piloto, a implementação de novas regras de registo de cartões SIM para os subscritores dos serviços de telecomunicações, devendo durar até 16 de Junho do presente ano de 2024.

Como iremos mostrar, não constitui somente nossa preocupação os riscos que esta medida representa para facilitar a vigilância digital indevida e ou o baixo nível de transparência em que ela foi tomada, mas também o facto de o INCM, no Workshop de apresentação das normas técnicas de registo de "central de risco", realizado em Abril de 2023, ter mostrado a pretensão de comercializar os dados dos cidadãos. Nesta ocasião, o representante do INCM, Reinaldo Zezela, disse que "poderão ser acedidas as bases de dados pelos operadores de telecomunicações no país, até pelos bancos, mediante o pagamento de taxas que variam de 0,10 a 20 meticais por cada registo. Esclareceu ainda que o valor cobrado servirá para suportar as despesas para a implementação, operacionalização e funcionamento das mesmas bases", conforme foi citado no jornal "A Carta" do dia 21 de Abril.

Como referiu o representante do INCM, citado pelo Jornal O País Online, do dia 22 de Maio, de 2023, "nós queremos assegurar que todo o indivíduo que estiver a usar um serviço na rede de telecomunicações do país seja identificável, sejamos capazes de rastreá-lo e tenhamos a certeza de que a operação está a ser feita pela pessoa certa. No antigo regulamento, registávamos apenas os cartões SIM, mas agora passamos a registar o próprio subscritor, o cartão, o dispositivo que o subscritor vai usar e o próprio agente", disse Reinaldo Zezela, cientista de dados do INCM.

Num contexto em que as leis não estabelecem nenhum mecanismo de protecção de dados e supervisão sobre os detentores de dados, como iremos garantir que os dados biométricos recolhidos pelas operadoras e centralizados pelo INCM sejam imunes à utilização para fins de "vigilância indevida", num contexto em que a configuração institucional do INCM lhe oferece baixo nível de independência do Governo e de uma cultura política autoritária, que tem vindo a caracterizar a governação em Moçambique?

> *No que diz respeito ao registo de dados biométricos, se pode, inclusivamente, verificar este risco sob ponto de vista do ambiente político, se considerarmos que a competição eleitoral, em Moçambique, tem sido dominada pelos mesmos actores no poder desde 1994, e com maior capacidade de controlo e influência sobre as instituições detentoras de dados, incluindo o INCM*

Mediante este contexto, a nossa discussão centra sobre os riscos que a recolha de dados biométricos dos cidadãos no registo dos cartões SIM representa para a protecção de dados dos cidadãos, assim como da "vigilância indevida". Vamos, por isso, tecer breves explicações sobre cinco argumentos entre si relacionados que, no nosso entender, constituem elementos fulcrais de riscos sobre os registos biométricos. i) o contexto político autoritário e permeabilidade para a vigilância; ii) os limites regulatórios; iii) o contexto de introdução do registo dos cartões "SIM" em Moçambique; iv) os riscos e o problema de comercialização de dados; e, finalmente, v) o registo SIM, nem sempre ser uma prática global e não ter produzido provas suficientes sobre a sua eficiência no combate ao crime.

O contexto político autoritário e permeabilidade para a vigilância

Primeiro, sobre o contexto político autoritário e permeabilidade para a vigilância, devemos assinalar o facto de Moçambique, desde a sua independência, ter sido fundado num Estado com tendência autoritária, sob o qual foram adoptadas medidas de restrições das liberdades políticas, o que implicava a aplicação de medidas fortes de vigilância, não somente para questões criminais, mas inclusivamente para o controlo dos que se representavam opositores do Partido-Estado. No percurso de Moçambique, mesmo no contexto democrático, foram assinaladas diversas situações que colocam em risco a segurança, desde as instabilidades políticas pós-eleitorais que levaram a Renamo a procurar transmitir as suas reivindicações por via do conflito, e, actualmente, o extremismo islâmico, em Cabo Delgado. Estes episódios, mesmo que exigissem o uso legítimo da vigilância, no contexto do autoritarismo político que o País vive, têm vindo a reforçar a cultura de vigilância indevida, num contexto em que o opositor, não somente se definia sob ponto de vista dos riscos de conflitos militares, mas também políticos.

No que diz respeito ao registo de dados biométricos, se pode, inclusivamente, verificar este risco sob ponto de vista do ambiente político, se considerarmos que a competição eleitoral, em Moçambique, tem sido dominada pelos mesmos actores no poder desde 1994, e com maior capacidade de controlo e influência sobre as instituições detentoras de dados, incluindo o INCM. Esta facilidade de acesso aos dados de cidadãos por certos actores e não outros pode contribuir para o fortalecimento e sofisticação dos mecanismos de manipulação da opinião pública, sobretudo com o advento da inteligência artificial e das chamadas deepfakes. Nos últimos pleitos eleitorais tem vindo a ser prática, em Moçambique, que cidadãos recebam mensagens de campanha dos partidos, sem nunca terem partilhado os seus contactos com os respectivos partidos políticos.

Existe uma relação entre os riscos de natureza política acima apresentados e as questões regulatórias que constituem o nosso segundo grupo de riscos de a recolha de dados biométricos ser usada para a vigilância indevida. Seja, em primeiro, o facto de que, embora tenhamos uma Constituição aberta à privacidade e Moçambique ter ratificado a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais, em 2019, através da Resolução nº 5/2019, não existe, no país, uma lei específica de protecção de dados. Do que actualmente existe são conjuntos de instrumentos que estabelecem contrariedades aos princípios de protecção de dados, o caso das 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.

> *Contudo, o contexto em que iniciou o debate sobre a necessidade de registo dos cartões SIM foi com protestos violentos contra a subida do custo de vida, na cidade de Maputo e Matola, tendo sido replicados em outras cidades do País, em Fevereiro de 2008 e Setembro de 2010, seguidos de um outro em Novembro de 2012, na cidade de Maputo.*

No terceiro nível, argumentamos o facto de que o contexto de introdução do registo dos cartões "SIM", em Moçambique, ter sido vinculado a uma clara necessidade de exercer a vigilância indevida. Se recuarmos, notaremos que a medida de registo de SIM não foi introduzida em 1997, quando a telefonia móvel iniciou os serviços em Moçambique, mas sim em 2015, tendo como fundo o mesmo argumento, a necessidade de combater o crime, as fraudes e proteger os próprios cidadãos (mais à frente iremos explicar as limitações deste argumento). Contudo, o contexto em que iniciou o debate sobre a necessidade de registo dos cartões SIM foi com protestos violentos contra a subida do custo de vida, na cidade de Maputo e Matola, tendo sido replicados em outras cidades do País, em Fevereiro de 2008 e Setembro de 2010, seguidos de um outro em Novembro de 2012, na cidade de Maputo.

Em 2010, o Centro de Integridade Pública – CIP fez o seu alerta sobre os riscos que esta medida representava e o seu carácter inconstitucional, pelo facto de se mostrar condicionadora das liberdades de expressão, manifestação e intercepção de comunicações dos cidadãos e, na sua opinião, competindo à Assembleia da República a introdução de medidas restritivas das liberdades fundamentais (Observatório de Direito nº 1, CIP, 2010). Considerando esse contexto, é nossa percepção que uma análise jurídica rigorosa deve ser feita sobre o Decreto 13/2023 de 11 de Abril, uma vez introduzir elementos nevrálgicos sobre a privacidade e os dados dos cidadãos que, possivelmente, podem preencher de diversos vícios de inconstitucionalidade. Por isso, o nosso convite aos estudiosos de direitos humanos e/ou direitos digitais para uma análise e discussão sobre o instrumento. E mais, tal Decreto entra em vigor num país que não dispõe de uma lei de protecção de dados, propriamente dita.

Os riscos de comercialização dos dados

A questão da privacidade como um direito humano fundamental deve ser considerada um elemento-chave para se compreender por que razão o INCM não pode, conforme o pronunciamento feito em Abril de 2023, comercializar os dados dos cidadãos. Nesse campo, entramos para o quarto elemento sobre os riscos de comercialização dos dados. A ideia fundamental que se deve reter é que os dados a serem recolhidos pertencem aos próprios cidadãos, sendo o INCM simples depositário, enquanto mandatário público de regulação, não lhe sendo, por isso, atribuído qualquer direito de comercialização de dados que não são seus. Pelo facto de centralizar e guardar dados recolhidos pelas operadoras, o INCM não passa a ter o monopólio e direitos exclusivos sobre esses dados.

> *Um dos problemas levantado, em todo o mundo e no âmbito da economia digital, é que a posse de dados de pessoas reforça, de forma inequívoca, o poder de quem os guarda, uma vez lhe oferecer a capacidade de fazer análise de comportamentos, prever e influenciar.*

Um dos problemas levantado, em todo o mundo e no âmbito da economia digital, é que a posse de dados de pessoas reforça, de forma inequívoca, o poder de quem os guarda, uma vez lhe oferecer a capacidade de fazer análise de comportamentos, prever e influenciar.

Como argumenta Carissa Véliz (2022), no seu livro "Privacidade é Poder", um dos problemas da economia dos dados reside na publicidade personalizada, uma vez que tem vindo a se provar que os anúncios micro-direccionados, baseados na identidade e comportamento, resultam em consequências negativas. Os casos do Cambridge Analytic nos Estados Unidos, e não só, são exemplo perfeito para compreender o quão a publicidade personalizada, baseada na inteligência artificial, corrói e distorce processos políticos. Esses anúncios, conforme refere, normalizam o uso hostil das tecnologias, transformando o marketing numa arma difusora de informação falsa, de fragmentação, manipulação e polarização na sociedade.

Por isso, no nosso entendimento, o INCM, enquanto Regulador, deve, a princípio, ser um fiel depositário dos dados dos cidadãos, sem que os use indevidamente para quaisquer fins. É, por isso, que deve-se realçar a importância de regulação independente, que ofereça plenas garantias de que o INCM possa assegurar a correcta guarda, manuseamento dos dados biométricos recolhidos e disponibilização somente em situações estritamente úteis para fins da justiça, segurança e baseadas em boas práticas, como, por exemplo, um mandado judicial para o seu acesso para fins de investigação criminal.

> *É, por isso, que deve-se realçar a importância de regulação independente, que ofereça plenas garantias de que o INCM possa assegurar a correcta guarda, manuseamento dos dados biométricos recolhidos e disponibilização somente em situações estritamente úteis para fins da justiça, segurança e baseadas em boas práticas*

O registo SIM, nem sempre ser uma prática global

Finalmente, o nosso último ponto crítico tem a ver com o facto de o registo de cartões SIM e de recolha de dados biométricos não ser directamente proporcional com o sucesso no combate ao crime.

Iniciemos por mostrar que, embora a tendência seja crescente nos últimos anos, o registo de cartões SIM não é uma prática mandatária, especificamente em países desenvolvidos com padrões elevados de segurança, democracia e economia de mercado, como Estados Unidos, Canadá, Inglaterra ou Finlândia.

Segundo um estudo publicado em 2023 pela Comparitech, uma entidade vocacionada a promover a segurança cibernética e a privacidade, em 2023 somente 24 países do mundo tinham obrigatoriedade de registo de cartões com dados biométricos. Nesses países, a China, o único com elevados padrões de segurança e de renda alta, e somente 8 países se encontravam em preparação para em 2024 adoptarem o registo SIM, incluindo a Rússia e Moçambique.

Para o caso de Moçambique, nota-se nos últimos 10 anos o crescimento exponencial de instalação de sistemas de câmaras de vigilância de alta-definição, seja a nível de residências, instituições de natureza privada, pública e mesmo em vias públicas – aqui a destacar o projecto de instalação de 450 câmaras de alta definição e de transmissão de dados, a tempo real, para fins de vigilância pública nas principais vias públicas das cidades de Maputo e Matola -, num ambiente de inexistência de uma regulação específica.

Contudo, o país, sobretudo a cidade de Maputo, tem vindo a assistir crimes violentos, incluindo raptos não esclarecidos, que levam diversos sectores da sociedade a questionar a utilidade e aplicabilidade destas tecnologias.

Em conclusão, mesmo sendo verdade e como mostramos, não pode ser líquido o argumento de que o registo biométrico visa garantir o combate ao crime, pois as experiências mostram fracassos e a existência de países com padrões de segurança aceitáveis e com capacidade de esclarecimento de crimes sem o registo mandatário de SIM Card, nem de recolha de dados biométricos. Pelo contrário, em contextos autoritários e de baixo nível de independência institucional das entidades reguladores, o registo biométrico dos cartões SIM pode representar elevados riscos de promover a "vigilância indevida" protagonizada pelos governos autoritários, sobretudo num contexto em que as leis são fracas e/ou inexistentes para reduzir estas práticas. A consequência é que isto pode alimentar o autoritarismo, através do reforço das capacidades de controlo, manipulação e propaganda, assim como reduzir a acção dos defensores dos direitos humanos e das organizações cívicas.

[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 os auspícios da British Academy Global Pressorrship, sedeado pela University of Glasgow, sob o qual tem vindo a desenvolver estas análises.