Em conformidade com a Resolução ACHPR/Res.620 (LXXXI) de 2024

ORIENTAÇÕES AFRICANAS SOBRE A PROMOÇÃO E A UTILIZAÇÃO DO ACESSO A DADOS COMO FERRAMENTA PARA A PROMOÇÃO DOS DIREITOS HUMANOS E DO DESENVOLVIMENTO SUSTENTÁVEL NA ERA DIGITAL

Índice

PREFÁCIO

As presentes Orientações são emitidas pela Comissão Africana dos Direitos Humanos e dos Povos (a Comissão Africana) nos termos da Resolução 620 sobre «Promover e Aproveitar o Acesso aos Dados como Ferramenta para o Avanço dos Direitos Humanos e do Desenvolvimento Sustentável na Era Digital», adotada pela Comissão Africana durante a sua 81.ª Sessão Ordinária.

A Resolução 620 reconhece que, na era digital, os dados não são meramente um recurso a ser gerido, mas uma condição prévia para a concretização dos direitos humanos e a consecução do desenvolvimento sustentável. A Resolução exorta os Estados Partes a adotarem medidas que garantam o acesso aos dados detidos tanto por atores públicos como por atores privados relevantes, com o objetivo de promover os direitos humanos e o desenvolvimento sustentável. A Resolução confere ao Relator Especial sobre a Liberdade de Expressão e o Acesso à Informação em África o mandato de realizar

consultas alargadas em todo o continente e de desenvolver normas adequadas para orientar a recolha, a utilização e o acesso aos dados. As presentes Orientações são emitidas em cumprimento desse mandato.

As Orientações são o resultado de consultas exaustivas com as partes interessadas, incluindo atores dos setores público e privado, organizações da sociedade civil, defensores dos direitos digitais e investigadores de todo o continente. As Orientações refletem a diversidade das experiências africanas e o compromisso comum de garantir que a transformação digital contribua para o gozo dos direitos humanos e o desenvolvimento.

O objetivo das Diretrizes é elaborar medidas políticas, legais e institucionais, respondendo a um contexto em que:

- Os quadros de acesso à informação existentes, embora essenciais, não abordam adequadamente os desafios de implementação específicos colocados pelo volume, complexidade e natureza proprietária dos dados, bem como pela predominância do setor privado no controlo e acesso aos dados;
- Sem transparência, supervisão ou vias de recurso adequadas, a inteligência artificial baseada em dados, os sistemas algorítmicos e a tomada de decisões automatizada podem prejudicar significativamente os direitos humanos;
- Os fluxos transfronteiriços de dados, incluindo o domínio das empresas tecnológicas transnacionais no processamento e armazenamento de dados, colocam desafios específicos à aplicação dos quadros jurídicos nacionais;
- O acesso desigual às infraestruturas digitais, à conectividade e à literacia digital — entre os Estados africanos e no interior destes — agrava as desigualdades existentes e exclui as comunidades marginalizadas dos benefícios da governação e do desenvolvimento baseados em dados;
- As mulheres e as raparigas, as pessoas com deficiência, os jovens, os povos indígenas, as comunidades rurais e outros grupos marginalizados enfrentam riscos acrescidos de danos relacionados com os dados e deparam-se com barreiras únicas ao acesso a dados essenciais para a concretização dos seus direitos;
- As leis de proteção de dados e privacidade, embora essenciais, têm sido por vezes utilizadas para bloquear o acesso legítimo a dados de interesse público, obstruindo assim a transparência, a responsabilização e o direito à informação;
- Muitos Estados africanos poderiam beneficiar da existência de instituições de supervisão eficazes e independentes, com autoridade para decidir sobre o acesso aos dados, ordenar medidas corretivas e garantir o cumprimento das obrigações de acesso.

Neste contexto, as Orientações prevêem medidas que, em conjunto, servirão para promover e aproveitar o acesso aos dados como uma ferramenta para o avanço dos direitos humanos e do desenvolvimento sustentável na era digital. Constituem um instrumento de *soft law* que oferece uma interpretação autorizada das obrigações dos Estados Partes ao abrigo da Carta Africana, em particular no que diz respeito aos artigos 9.º (direito de receber informação) e 22.º (direito ao desenvolvimento). Baseiam-se na jurisprudência existente da Comissão sobre acesso à informação, privacidade, democracia, desenvolvimento e direitos digitais. As Orientações destinam-se a apoiar:

- Os Estados Partes: como um modelo para a reforma legislativa, política e institucional, bem como um ponto de referência para o cumprimento das obrigações decorrentes da Carta Africana;
- O poder judicial e os órgãos quase judiciais: como um auxílio interpretativo na resolução de litígios que envolvam o acesso a dados;
- As instituições nacionais de direitos humanos e a sociedade civil: como um quadro para a monitorização, a defesa e a prestação de contas;
- Aos atores do setor privado: como orientação sobre as melhores práticas em matéria de transparência, responsabilização e governação responsável dos dados;

- Para as instituições regionais e sub-regionais: como referência para alinhar os instrumentos de governação digital com as normas de direitos humanos e desenvolver abordagens africanas transnacionais.

O direito de acesso aos dados não é um luxo que possa ser adiado; é fundamental para a dignidade humana, para governação democrática e para busca coletiva de uma África justa e próspera. Asseguremos que o acesso aos dados seja moldado de forma a garantir que a transformação digital não deixe ninguém para trás.

Exma. Comissária Geereesha Topsy-Sonoo,
Relatora Especial sobre a Liberdade de Expressão e o Acesso à Informação em África

PREÂMBULO

Afirmando o seu mandato nos termos do artigo 45.º da Carta Africana dos Direitos Humanos e dos Povos (a Carta Africana), incluindo a competência para formular e estabelecer princípios e regras nos quais os Estados africanos possam basear a sua legislação;

Recordando a Resolução 620, «Promover e Aproveitar o Acesso aos Dados como Ferramenta para o Avanço dos Direitos Humanos e do Desenvolvimento Sustentável na Era Digital», que reconhece a importância dos dados para o avanço dos direitos humanos e do desenvolvimento sustentável e que incumbe o Relator Especial sobre a Liberdade de Expressão e o Acesso à Informação em África de desenvolver normas adequadas em conformidade;

Recordando o artigo 9.º da Carta Africana, que garante a todos os indivíduos o direito de acesso à informação, e reconhecendo adicionalmente que, na era digital, este direito inclui o acesso aos dados;

Recordando o artigo 22.º da Carta Africana, que afirma o direito ao desenvolvimento, e reconhecendo adicionalmente que o acesso aos dados é essencial para a concretização deste direito, nomeadamente através da participação informada no planeamento do desenvolvimento, na tomada de decisões e nas oportunidades económicas;

Recordando ainda que os direitos consagrados na Carta Africana são indivisíveis, interdependentes e inter-relacionados, e que o acesso aos dados é necessário para o gozo efetivo dos direitos civis, políticos, económicos, sociais e culturais;

Reconhecendo os artigos 19.º e 21.º da Declaração Universal dos Direitos Humanos e os artigos 19.º e 25.º do Pacto Internacional sobre os Direitos Civis e Políticos, que garantem o direito de acesso à informação e o direito de participar em eleições periódicas genuínas, livres, justas e credíveis;

Recordando a Declaração de Princípios sobre a Liberdade de Expressão e o Acesso à Informação em África, a Lei-Modelo sobre o Acesso à Informação para África e as Orientações sobre o Acesso à Informação e as Eleições em África, bem como várias outras resoluções, que, em conjunto, estabelecem o quadro normativo que sustenta os direitos usufruídos através dos ecossistemas de informação no continente, incluindo os direitos de acesso à informação, privacidade e proteção de dados, participação política e liberdade de expressão;

Reconhecendo a Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais e o Quadro de Política de Dados da União Africana, que proporcionam importantes quadros regionais para a governação de dados;

Afirmando que o acesso aos dados e a proteção dos dados pessoais são obrigações complementares e que qualquer limitação ao acesso deve ser prevista por lei, prosseguir um objetivo legítimo e ser estritamente necessária e proporcionada numa sociedade democrática;

Recordando ainda a Resolução 473 sobre a necessidade de realizar um estudo sobre os direitos humanos e dos povos e a Inteligência Artificial (IA), a robótica e outras tecnologias novas e emergentes em África, que sublinha o empenho da Comissão nas tecnologias emergentes que afetam o acesso aos dados;

Tomando nota da Estratégia de Transformação Digital para África (2020–2030) da União Africana e da Agenda 2063, para as quais o acesso aos dados é fundamental para o desenvolvimento inclusivo, a inovação e a integração continental;

Reconhecendo que os direitos humanos consagrados na Carta Africana dependem cada vez mais do acesso aos dados na era digital;

Reafirmando que o acesso aos dados para o bem público pode promover os direitos humanos e a inovação social, bem como ajudar a apoiar o progresso no sentido de concretizar o direito ao desenvolvimento, os Objetivos de Desenvolvimento Sustentável e *a Agenda 2063: A África que Queremos*;

Preocupada com o facto de, apesar da proliferação de tecnologias baseadas em dados, não existirem orientações específicas para os governos africanos e os intervenientes privados sobre a promoção e a utilização do acesso aos dados, tal como estabelecido na Resolução 620

A Comissão Africana dos Direitos Humanos e dos Povos, reunida na sua [...] Sessão Ordinária, realizada [...]

Adota as Orientações Africanas sobre o Acesso aos Dados, um instrumento para promover e aproveitar o acesso aos dados como ferramenta para fazer avançar os direitos humanos e o desenvolvimento sustentável na era digital.

DEFINIÇÕES

A Carta Africana refere-se à Carta Africana dos Direitos Humanos e dos Povos.

Comissão Africana refere-se à Comissão Africana dos Direitos Humanos e dos Povos.

Anonimização significa um processo de alteração de registos de modo que estes não se relacionem com uma pessoa singular identificada ou identificável, ou um processo de tornar os dados pessoais anónimos de modo que o titular dos dados não seja ou deixe de ser identificável.

Inteligência Artificial (IA) designa software capaz de realizar tarefas que normalmente requerem inteligência humana, incluindo a capacidade de emular a aprendizagem, o raciocínio e a tomada de decisões humanos. A tomada de decisões automatizada sob IA refere-se a decisões tomadas sem intervenção humana significativa. Todos os sistemas de IA dependem de dados tanto para os seus modelos de treino como para aplicações subsequentes, tais como inferências em tempo real e resultados gerativos.

Os dados abrangem a representação em formato eletrónico de informação a um nível granular, com potencial para conversão em significado de nível superior. Normalmente, compreendem sinais e registos sob qualquer forma, recolhidos, armazenados, processados ou partilhados em formatos estruturados ou não estruturados, incluindo texto, imagens, som, vídeo e impulsos de sensores. Incorporam dados pessoais (relativos a um indivíduo identificado ou identificável) e dados não pessoais (tais como dados ambientais ou estatísticos). A informação em si pode ser tratada como dados para operações de conversão de conhecimento posteriores.

Conjunto de dados significa uma coleção de dados e é tipicamente organizado em tabelas, matrizes ou formatos específicos, como CSV ou JSON, para facilitar a recuperação e a análise. Os conjuntos de dados são essenciais para a análise de dados, a aprendizagem automática, a IA e outras aplicações que requerem dados fiáveis e acessíveis. Com a IA generativa, os conjuntos de dados também podem ser constituídos a partir de dados não estruturados, expandindo assim a forma como os dados podem ser organizados e utilizados como recurso.

O acesso aos dados refere-se ao direito legal ou à capacidade técnica de recuperar, visualizar, utilizar, mover ou manipular dados como parte do direito mais amplo à informação, incluindo de detentores de dados de organismos públicos e privados, e é possibilitado pela disponibilidade, integridade e usabilidade desses dados. O acesso pode ser obtido através do download de dados ou do processamento de dados noutro local, incluindo no próprio local, com a opção de guardar os resultados desse processamento.

Ecossistema de dados significa a integração e a interação entre diferentes partes interessadas relevantes, incluindo detentores de dados, produtores de dados, intermediários de dados e titulares de dados, que estão envolvidos ou são afetados por acordos de acesso e partilha de dados de acordo com as suas diferentes funções, responsabilidades e direitos, tecnologias e modelos de negócio. É necessária a capacidade e o envolvimento do Estado para promover o acesso a este ecossistema e garantir que os direitos humanos e a soberania nacional não sejam prejudicados.

Por **«detentores de dados»** entende-se as entidades ou indivíduos que têm autoridade legal para permitir a partilha e o acesso aos dados. Podem ser responsáveis pelo tratamento de dados ao abrigo das leis de proteção de dados, sendo responsáveis pelas operações de tratamento de dados.

Por **«intermediários de dados»** entende-se as entidades que operam no âmbito de acordos de acesso e partilha de dados, facilitando o acesso e/ou a partilha de dados ou a troca comercial de dados.

Literacia de dados significa a capacidade do público de reconhecer e exercer os seus direitos no que diz respeito às oportunidades e riscos relacionados com questões de dados, com base nos seus conhecimentos e competências, bem como na sua compreensão dos parâmetros legais, éticos e institucionais aplicáveis.

Partilha de dados significa o ato de conceder acesso a dados para utilização por terceiros, sujeito aos requisitos técnicos, financeiros, legais ou organizacionais aplicáveis. A partilha pode ser feita diretamente ou através de um intermediário de dados e pode ocorrer sob diversas condições de licença.

Por **«titular dos dados»** entende-se uma pessoa singular identificável ou um grupo identificável a quem os dados se referem, incluindo comunidades ao abrigo do direito consuetudinário ou nacional, e que tem o direito de consentir na recolha, tratamento e distribuição dos seus dados.

Por **«dados dinâmicos»** entende-se registos em formato digital, sujeitos a atualizações frequentes ou em tempo real, em particular devido à sua volatilidade ou rápida obsolescência; os impulsos elétricos gerados por sensores são tipicamente considerados dados dinâmicos.

Conjuntos de dados de elevado valor: registos cuja reutilização está associada a benefícios importantes para a sociedade, o ambiente e a economia, em particular devido à sua adequação para a criação de serviços e aplicações de valor acrescentado e de novos empregos de alta qualidade e dignos, e devido ao número de potenciais beneficiários dos serviços e aplicações de valor acrescentado baseados nesses conjuntos de dados.

A informação inclui qualquer original ou cópia de material documental, independentemente das suas características físicas, tais como registos, correspondência, factos, opiniões, conselhos, publicidade, memorandos, dados, estatísticas, livros, desenhos, planos, mapas, diagramas, fotografias, registos áudio ou visuais, e qualquer outro material tangível ou intangível, independentemente da forma ou do suporte em que se encontre.

A integridade da informação significa a exatidão, a coerência e a fiabilidade do conteúdo, dos processos e dos sistemas de informação para manter um ecossistema de informação fiável, sendo fundamentalmente possibilitada pela integridade subjacente dos dados.

Interoperabilidade significa a facilidade técnica de dois ou mais espaços de dados ou redes de comunicação, sistemas, produtos conectados, aplicações, serviços de processamento de dados ou componentes trocarem e utilizarem dados para desempenhar as suas funções.

Formato legível por máquina significa um formato de ficheiro estruturado de modo que as aplicações de software possam facilmente identificar, reconhecer e extrair dados específicos, incluindo declarações de facto individuais e a sua estrutura interna.

Metadados significam informações descritivas sobre os dados primários. Os metadados podem incluir dados pessoais.

Formato aberto significa um formato de ficheiro independente da plataforma e disponibilizado ao público sem qualquer restrição que impeça a reutilização.

Dados abertos referem-se a dados disponibilizados num formato legível por máquina, gratuitamente e ao abrigo de uma licença aberta que permite a utilização, reutilização e redistribuição sem restrições.

Por **«dados pessoais»** entende-se informações relativas a uma pessoa singular identificada ou identificável, através das quais essa pessoa pode ser identificada, direta ou indiretamente, nomeadamente através de identificadores como o nome, o número de identificação, os dados de localização ou um identificador online, ou de fatores específicos da identidade física, jurídica, fisiológica, mental, económica, cultural ou social de um indivíduo.

Pseudonimização significa o tratamento de dados pessoais de forma que esses dados já não possam ser atribuídos a um titular de dados específico sem o recurso a informações adicionais, desde que essas informações adicionais sejam mantidas separadamente e estejam sujeitas a medidas técnicas e organizacionais destinadas a garantir que os dados pessoais não sejam atribuídos a uma pessoa singular identificada ou identificável.

Por **«entidade privada»** entende-se: (a) uma pessoa singular que exerça ou tenha exercido qualquer atividade comercial, empresarial, profissional ou outra, mas apenas nessa qualidade; (b) uma sociedade que exerça ou tenha exercido qualquer atividade comercial, empresarial, profissional ou outra; ou (c) qualquer pessoa coletiva ou sucessor em direito; excluindo, no entanto, as entidades públicas e as entidades privadas relevantes.

A divulgação proativa refere-se a um fluxo regular de informação, através do fornecimento rotineiro de informação ao público sem que seja necessário que as pessoas apresentem um pedido.

Por **«autoridades públicas»** entende-se as pessoas coletivas, os órgãos legislativos e as autoridades judiciais, na medida em que exerçam funções administrativas, tal como definido pela legislação nacional.

Por **«organismo público»** entende-se quaisquer autoridades administrativas a nível nacional, regional e local (por exemplo, o governo central, o governo provincial e outros órgãos municipais, a polícia, as autoridades de saúde pública e de educação, os serviços de arquivos públicos, etc.) e as autoridades públicas.

O interesse público é um critério que designa benefícios partilhados pela sociedade no seu conjunto (por exemplo, serviços públicos e infraestruturas), em vez de promover apenas interesses individuais, de grupo ou privados. Tais benefícios são promovidos e protegidos por todos, especialmente pelos organismos públicos. Determinar o interesse público implica ponderar avaliações concorrentes do impacto potencial e considerar compromissos ao longo do tempo.

O valor público refere-se ao valor criado para o público em geral e para o benefício social, incluindo o setor público, como a utilização de dados para a participação em políticas públicas e outros fins de interesse público, visando garantir a sustentabilidade, a equidade ou a inclusão, e um impacto positivo na sociedade, na economia e no ambiente.

Publicar significa disponibilizar de uma forma e maneira facilmente acessível ao público e inclui o fornecimento de cópias ou a disponibilização de informações através de meios de comunicação de radiodifusão e eletrónicos.

Por **«organismo privado relevante»** entende-se qualquer organismo que, de outro modo, seria um organismo privado nos termos das presentes Orientações e que seja (a) detido total ou parcialmente, ou controlado ou financiado, direta ou indiretamente, por fundos públicos, mas apenas na medida desse financiamento; ou (b) que exerça uma função estatutária ou pública ou preste um serviço estatutário ou público, mas apenas na medida dessa função estatutária ou pública ou desse serviço estatutário ou público.

Por **«dados de investigação»** entende-se registos em formato digital, que não sejam publicações científicas, recolhidos ou produzidos no decurso de atividades de investigação científica e utilizados como prova no processo de investigação, ou que sejam comummente aceites na comunidade científica como necessários para validar as conclusões e os resultados da investigação.

Por **«direitos sui generis** em termos de propriedade intelectual» entende-se a aplicação, em jurisdições específicas, de direitos únicos para categorias específicas de propriedade intelectual, tais como a proteção de bases de dados, nos casos em que a base de dados não dá origem a direitos ao abrigo das leis tradicionais de propriedade intelectual, como a lei das patentes ou dos direitos de autor.

Dados sensíveis referem-se a dados pessoais que revelam origem racial ou étnica, opiniões políticas, crenças religiosas, informações de saúde, dados biométricos ou genéticos, ou outras informações que requerem proteção reforçada.

PRINCÍPIOS FUNDAMENTAIS

As presentes Orientações baseiam-se diretamente na Resolução 620, que reconhece que o acesso aos dados constitui uma parte essencial do direito à informação e é vital como ferramenta para os direitos humanos, a democracia e o desenvolvimento sustentável. As medidas a seguir expostas baseiam-se nos seguintes princípios, inspirados diretamente na resolução da Comissão:

Os dados como um ativo estratégico: Os dados são um ativo público estratégico com potencial transformador para serem utilizados no interesse público, em prol do valor público, para promover a democracia, a boa governação e a concretização dos objetivos de desenvolvimento acordados a nível internacional e africano. Os dados devem, por conseguinte, servir para apoiar políticas, serviços ou intervenções que melhorem o bem-estar social, a transparência e a responsabilização.

Acesso aos dados por definição: Os sistemas de recolha, armazenamento e divulgação de dados devem ser concebidos com funcionalidades de divulgação proativa, normas de acessibilidade e disposições de interoperabilidade e segurança por predefinição.

Divulgação proativa: O acesso sem a necessidade de pedidos ativos deve aplicar-se, no mínimo, a conjuntos de dados essenciais de interesse público, tais como orçamentos, contratos públicos, saúde, educação e dados ambientais, e ser disponibilizado em formatos abertos e reutilizáveis.

Divulgação máxima: O princípio da divulgação máxima deve ser a regra por defeito para todos os dados públicos e para os dados de organismos privados relevantes. A divulgação deve ser presumida, a menos que seja comprovadamente prejudicial. As restrições ao acesso devem constituir uma exceção restrita, estritamente justificada pelas normas internacionais de direitos humanos.

Justiça e equidade em matéria de dados: Os indivíduos têm direito a informações significativas sobre a proveniência, a lógica, o significado, as consequências e as categorias dos dados envolvidos na tomada de decisões automatizada que afeta os seus direitos, e têm o direito de contestar decisões baseadas exclusivamente no tratamento automatizado e de solicitar uma revisão humana. Além disso, as iniciativas em matéria de dados devem ser concebidas para combater as desigualdades estruturais e garantir que as comunidades marginalizadas e vulneráveis tenham acesso equitativo aos dados, à sua governação e aos benefícios decorrentes da sua utilização.

Integridade dos dados e integridade da informação: Para ser significativo, o direito de acesso aos dados exige que estes apresentem integridade no que diz respeito à exatidão, consistência e fiabilidade dos processos e sistemas, o que, por sua vez, reforça a integridade da informação e um ecossistema de informação fiável.

Complementaridade entre o acesso aos dados **e a proteção** dos dados**:** O acesso aos dados e a proteção dos dados pessoais são obrigações complementares. Nenhuma delas deve ser perseguida em detrimento da outra. Os quadros de proteção de dados devem incluir exceções para o acesso legítimo a dados de interesse público, e os quadros de acesso devem incorporar salvaguardas para proteger os dados pessoais contra o uso indevido, a discriminação e a vigilância ilegal.

Transparência, responsabilização e ética: A recolha, o tratamento e a utilização de dados devem ser transparentes e responsáveis. Os princípios éticos devem estar incorporados em todas as iniciativas relacionadas com dados, com mecanismos para abordar preconceitos nos dados e na tomada de decisões automatizada. Além disso, os dados são uma ferramenta indispensável para a responsabilização e devem, por isso, ser acessíveis a jornalistas e investigadores para questões de interesse público, responsabilização do poder e promoção de um discurso público bem informado.

Responsabilização do setor privado: Os Estados Partes têm o dever positivo de regulamentar os atores privados cujas práticas em matéria de dados tenham impacto no gozo dos direitos humanos. Estas Orientações estendem-se aos dados detidos por entidades privadas quando tais dados forem necessários para o exercício dos direitos humanos, forem de interesse público significativo, para além do caso das entidades privadas relevantes definidas acima. Os quadros jurídicos que impõem obrigações de transparência, responsabilização e acesso devem abranger os atores do setor privado quando os dados estiverem implicados em danos e benefícios para os direitos humanos.

Recursos eficazes: Qualquer pessoa a quem seja negado o direito de acesso aos dados deve ter direito a um recurso eficaz perante um órgão independente com poderes para ordenar a divulgação, impor sanções e conceder reparação adequada.

MEDIDAS

Medidas gerais

Para garantir um quadro robusto e coerente de governação de dados que preste a devida atenção às questões de acesso e esteja em conformidade com as normas regionais e internacionais, as orientações que se seguem estabelecem 12 medidas que deverão ser tomadas:

1. Incorporar a Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais e o Quadro de Política de Dados da União Africana na legislação nacional, a fim de garantir a coerência e facilitar a interoperabilidade regional.

2. Combinar uma abordagem governamental global às estruturas de dados para permitir uma coordenação eficaz das políticas e uma participação abrangente de múltiplas partes interessadas.
3. Criar ou reforçar um Quadro Nacional Integrado de Gestão de Dados (descrito abaixo) que promova a produção e o acesso a dados relevantes para os direitos humanos e o desenvolvimento, e que favoreça o fluxo equitativo e seguro de dados entre o governo, os indivíduos, a sociedade civil, o meio académico e o setor privado, salvaguardando simultaneamente contra violações da segurança dos dados, bem como formas de extração e tratamento que violem os direitos humanos.
4. Desenvolver e implementar uma Política Nacional de Dados Abertos que obrigue as instituições públicas e os organismos que recebem fundos públicos a disponibilizar proativamente os dados ao público.
5. Normalizar os processos de acesso para pedidos de dados públicos e privados, incluindo requisitos de justificação consistentes para casos de não divulgação.
6. Assegurar que os titulares e os responsáveis pelo tratamento de dados obtenham o consentimento informado sempre que necessário, limitem a utilização dos dados a finalidades definidas e respeitem os direitos dos titulares dos dados ao acesso, à retificação e à eliminação.
7. Estabelecer um quadro jurídico claro que defina de forma restrita as circunstâncias em que os organismos do setor público e outras partes interessadas podem ter acesso a dados detidos por organismos privados em situações de interesse público superior genuíno e demonstrável (tais como em emergências públicas, crises de saúde comprovadas ou para supervisão eleitoral exigida por lei). Esse acesso deve estar sujeito a rigorosos critérios de necessidade e proporcionalidade, supervisão independente ou revisão judicial e a protocolos robustos de segurança de dados e salvaguardas de responsabilização.
8. Criar ou designar formalmente uma instituição estatal, como uma Comissão de Informação ou Autoridade de Proteção de Dados (ou híbrida ou equivalente), e dotá-la de poderes legais, capacidade técnica e recursos financeiros suficientes para supervisionar a governança de dados. Esta instituição deve garantir que todas as atividades de recolha, tratamento e partilha de dados cumpram as leis nacionais e internacionais aplicáveis, promova um equilíbrio entre privacidade, acesso e outras questões, e ofereça reparação eficaz por violações dos direitos relacionados.
9. Dar prioridade ao armazenamento de dados governamentais abertos em centros de dados nacionais ou regionais para promover a soberania.
10. Promover o acesso a dados sobre a extensão de práticas ambientalmente sustentáveis, tais como fontes de energia para centros de dados e a gestão, reciclagem e eliminação de resíduos eletrónicos.
11. Tomar medidas para garantir o acesso aos dados com o objetivo de avaliar se os conjuntos de dados utilizados para IA e tomada de decisões algorítmicas são representativos, validados quanto à precisão e monitorizados quanto a enviesamentos, e avaliar a proveniência dos dados e as restrições de utilização.
12. Cooperar a nível regional e sub-regional africano para desenvolver abordagens comuns entre países para garantir o acesso aos dados recolhidos e detidos por atores transnacionais do setor privado.

Medidas legais, políticas e programáticas

Para se alinhar com um quadro jurídico em conformidade com os direitos humanos em matéria de acesso aos dados, as medidas correspondentes garantirão que:

13. **A legislação e a regulamentação existentes sejam interpretadas de forma a abranger os dados:**
    a. As isenções de acesso à informação sejam expressamente entendidas de forma a abranger «dados» e «conjuntos de dados» como formas de informação sujeitas ao direito de acesso, com disposições aplicáveis sobre divulgação proativa, formatos, recusa de acesso, supervisão e aplicação.

b. Quaisquer disposições contraditórias nas regras jurídicas existentes (por exemplo, Leis de Segredos de Estado, leis de cibersegurança) que possam afetar desnecessariamente o acesso aos dados possam ser identificadas e resolvidas.

14. O direito de acesso aos dados seja consagrado:

Como componente do direito de acesso à informação garantido por lei, o acesso aos dados deve ser abrangido pelos seguintes princípios em disposições legais atuais ou novas:

a. Todas as pessoas têm o direito de aceder aos dados detidos por organismos públicos e organismos privados relevantes de forma rápida e económica.
b. Todas as pessoas têm o direito de aceder aos dados de outras entidades privadas que possam ajudar no exercício ou na proteção de qualquer direito, de forma rápida e a baixo custo.
c. O direito de acesso aos dados deve ser orientado pelos princípios da divulgação proativa e da divulgação máxima, limitado por isenções estritamente definidas, que devem ser previstas na lei e cumprir rigorosamente o direito e as normas internacionais em matéria de direitos humanos.
d. As medidas legais que regulam o consentimento devem incluir direitos claros de adesão e de recusa que abranjam a recolha, o tratamento e o acesso, de modo que os indivíduos mantenham um controlo efetivo sobre os seus dados pessoais.
e. Os dados devem estar abertamente disponíveis, serem facilmente localizáveis, acessíveis, utilizados, partilhados e divulgados por qualquer pessoa para qualquer finalidade que não esteja limitada por isenções restritas.
f. As transferências transfronteiriças de dados devem cumprir as leis nacionais de proteção de dados e os acordos internacionais para garantir uma proteção equivalente.
g. Quando o acesso aos dados servir um interesse público superior (por exemplo, saúde, ambiente, eleições, resposta a catástrofes, combate à violência de género), as obrigações de divulgação devem ser absolutas.
h. São necessárias disposições legais que prevejam vias de recurso em caso de recusa de acesso aos dados, nomeadamente através da especificação de uma revisão administrativa por um órgão de supervisão ou provedor de justiça, bem como através da possibilidade de recurso judicial.

15. As divulgações de interesse público são protegidas:

a. Nenhuma pessoa será sujeita a sanções civis, penais, administrativas, laborais ou outras, nem a qualquer prejuízo, por divulgar dados sobre irregularidades ou que revelem uma ameaça grave à saúde, à segurança ou ao ambiente, ou cuja divulgação seja do interesse público.

16. Existe o dever de criar, conservar, organizar e manter dados:

a. São necessárias disposições legais para exigir que os organismos públicos e os organismos privados relevantes criem, conservem, organizem e mantenham dados de forma a facilitar a integridade dos dados e a apoiar o exercício do direito de acesso.
b. A conservação de dados deve estar em conformidade com os princípios da proporcionalidade, e os conjuntos de dados de longo prazo essenciais para os direitos e o desenvolvimento (por exemplo, população, ambiente, arquivos públicos) devem ser conservados para além dos prazos administrativos habituais.
c. Os organismos públicos e privados relevantes devem ser obrigados a manter e publicar catálogos dos conjuntos de dados que detêm, com metadados e condições de utilização claramente indicados.

17. O valor público está no cerne do acesso aos dados:

a. Para concretizar o valor público, é necessário o envolvimento inclusivo das partes interessadas relevantes no ecossistema de dados — incluindo grupos vulneráveis, sub-representados ou marginalizados — durante a conceção, implementação e monitorização dos quadros de governação de dados, incluindo no que diz respeito às disposições relativas ao acesso aos dados.

b. A transparência dos acordos de acesso e partilha de dados é necessária para incentivar a adoção de práticas responsáveis de governação de dados ao longo de todo o ciclo de valor dos dados, incluindo no que diz respeito ao cumprimento de códigos de conduta, princípios éticos e regulamentos de privacidade e proteção de dados.
c. Quando estão em causa dados pessoais, é necessário o cumprimento dos quadros de privacidade e proteção de dados no que diz respeito aos dados pessoais a que se acede e que são partilhados, incluindo com quem são partilhados, para que finalidade e em que condições o acesso pode ser concedido a terceiros.
d. É importante incentivar e facilitar modelos inovadores de partilha de dados, incluindo, entre outros, doações de dados e conjuntos de dados, envolvendo investigadores, cientistas de dados e jornalistas.

18. Os mercados de dados são competitivos e funcionam para todos:

a. Os mercados competitivos de dados exigem uma política de concorrência sólida e uma regulamentação que aborde a possível exploração da posição dominante no mercado e preveja mecanismos de aplicação e reparação que aumentem a autonomia e o controlo das partes interessadas, de modo a garantir a proteção adequada dos consumidores, dos direitos de propriedade intelectual, dos interesses legítimos em matéria de segurança, da privacidade e da proteção dos dados pessoais.
b. A governação deve incentivar parcerias de partilha de dados neutras em termos de concorrência, incluindo Parcerias Público-Privadas (PPP), em que a partilha de dados entre os setores público e privado possa criar valor adicional para a sociedade.
c. Ao facilitar a partilha de dados entre os setores público e privado, devem ser tomadas as medidas necessárias para evitar conflitos de interesses, incluindo garantir que:
    i. Os organismos públicos não concedam acesso exclusivo a dados que comprometa a concorrência leal, mas tratem todos os participantes no mercado em condições justas, razoáveis e não discriminatórias, equilibradas com a consideração de regimes de acesso e parceria por níveis, a fim de distribuir valor para além das entidades com mais recursos e gerar benefícios inclusivos;
    ii. As parcerias público-privadas e privado-privadas não resultem na captura de dados públicos para vantagem comercial privada em detrimento do acesso público generalizado.
d. Os Estados podem desenvolver orientações de concorrência específicas por setor para mercados de dados distintos, particularmente em áreas como plataformas digitais e intermediários online; publicidade; serviços de telecomunicações e conectividade; serviços financeiros e tecnologia financeira; dados de saúde e serviços de saúde digitais; e dados agrícolas e tecnologia agrícola.

19. A utilização de dados é facilitada:

a. É necessário promover a localizabilidade, acessibilidade, interoperabilidade e reutilização de dados entre organizações, incluindo dentro e entre os setores público e privado. Em particular, isto exige esforços para garantir que:
    i. Os dados sejam fornecidos juntamente com quaisquer metadados, documentação, modelos de dados e algoritmos necessários, disponibilizados de forma transparente e atempada, e apoiados por mecanismos adequados de controlo do acesso aos dados, incluindo interfaces de programação de aplicações (API);
    ii. O desenvolvimento e a adoção de especificações interoperáveis para o acesso, partilha e utilização eficazes dos dados, incluindo normas comuns para formatos e modelos de dados, bem como implementações de código aberto e formatos abertos.
b. Os quadros de governação de dados prevejam programas públicos para aumentar a sensibilização sobre os benefícios do acesso a dados abertos e interoperáveis.

20. Existem procedimentos em vigor para os pedidos de acesso aos dados:

a. Quando o acesso aos dados estiver sujeito a um pedido:

i. O acesso deve ser concedido o mais rapidamente possível e dentro dos prazos estabelecidos pela legislação nacional (não excedendo 30 dias para pedidos normais, sujeitos a prorrogação limitada em circunstâncias justificadas).
ii. O acesso deve ser concedido a um custo reduzido, com taxas limitadas aos custos marginais de reprodução e divulgação, quando aplicável. O acesso a dados gerados pelos utilizadores e a dados de interesse público significativo deve ser gratuito.
iii. Os dados devem ser fornecidos em formatos abertos, interoperáveis e legíveis por máquina, incluindo, quando apropriado, formatos acessíveis a pessoas com deficiência.
iv. Nenhum requerente deve ser obrigado a demonstrar um interesse jurídico ou pessoal específico nos dados solicitados nem a apresentar uma justificação para o pedido, salvo disposição em contrário da lei para categorias específicas de dados sensíveis.
v. Os requerentes têm direito a receber assistência para apresentar os seus pedidos oralmente ou por escrito, devendo ser prestado o apoio adequado a pessoas analfabetas e a pessoas com deficiência, para que possam apresentar os seus pedidos em condições de igualdade com os demais.
vi. Qualquer recusa em divulgar dados deve ser comunicada atempadamente e por escrito, deve ser devidamente fundamentada e deve basear-se no direito e nas normas internacionais. A recusa deve especificar a isenção aplicável, o dano que a divulgação causaria e as considerações de interesse público ponderadas.

b. No que diz respeito aos dados disponibilizados por meios automatizados, incluindo interfaces de programação de aplicações (API), portais ou *feeds* em tempo real, aplicam-se as seguintes orientações:
i. Os mecanismos de acesso devem ser claramente documentados, estar disponíveis ao público e ser apoiados por assistência técnica, quando apropriado.
ii. O acesso não deve estar sujeito a barreiras técnicas irrazoáveis, bloqueios de propriedade ou condições discriminatórias injustas.
iii. Os utilizadores devem ter o direito de aceder aos dados através de APIs sem serem obrigados a justificar a finalidade do acesso, exceto quando necessário para prevenir violações de direitos ou proteger a segurança.

c. Quando os dados forem dinâmicos ou sujeitos a atualizações frequentes (incluindo dados de sensores, dados de monitorização em tempo real ou dados de *streaming*), os mecanismos de acesso devem permitir a sua recuperação atempada. Os Estados e os organismos privados relevantes devem assegurar que os dados dinâmicos de interesse público significativo (por exemplo, monitorização ambiental, dados de saúde pública, dados de resposta a catástrofes) sejam acessíveis em tempo real ou quase em tempo real, sempre que tecnicamente viável.

d. Os procedimentos de acesso devem distinguir entre:
i. Conjuntos de dados completos: quando for solicitado o acesso a conjuntos de dados na íntegra, os procedimentos devem facilitar o download em massa ou o acesso via API.
ii. Dados granulares ou específicos: quando for solicitado ou concedido o acesso apenas a registos de dados específicos, os procedimentos devem permitir a recuperação precisa sem exigir o acesso ao conjunto de dados na íntegra.

e. Os Estados podem estabelecer procedimentos de pedido normalizados, incluindo portais online e formulários eletrónicos, para agilizar o acesso. Tais procedimentos não devem criar barreiras indevidas e devem proporcionar alternativas para indivíduos sem acesso à Internet ou sem literacia digital.

f. Qualquer recusa, atraso ou divulgação parcial de dados deve ser passível de recurso perante um órgão de supervisão independente designado ao abrigo das presentes Orientações (ver Apêndice C). O órgão de supervisão pode ordenar a divulgação, impor prazos ou conceder reparações.

Isenções e salvaguardas

21. Isenções

a. Os dados só podem ser legitimamente retidos quando o prejuízo para o interesse protegido ao abrigo da isenção relevante for comprovadamente superior ao interesse público na divulgação da informação. Esses dados só podem ser retidos durante o período em que o prejuízo possa ocorrer.
b. Quando uma parte de um conjunto de dados que contenha os dados solicitados estiver isenta de divulgação, a parte isenta deve ser separada ou suprimida e deve ser concedido acesso ao restante do conjunto de dados.
c. As leis que regem a classificação de dados devem estipular o período máximo de classificação e restringir a classificação apenas na medida do necessário, nunca por tempo indeterminado.
d. Em geral, os dados só podem ser legitimamente retidos como isenção se a sua divulgação:
    i. Resultar na divulgação injustificada de informações pessoais de terceiros;
    ii. Causar prejuízo substancial a um interesse comercial ou financeiro legítimo das partes interessadas relevantes ou de outros terceiros;
    iii. Pusesse em perigo a vida, a saúde ou a segurança de um indivíduo;
    iv. Causar prejuízo substancial à segurança nacional e à defesa do Estado;
    v. Causar prejuízo substancial às relações internacionais, quando os dados se relacionem com informações que devam ser mantidas em sigilo nos termos do direito internacional, a posição do Estado no que diz respeito a negociações internacionais e a correspondência diplomática ou oficial com Estados ou organizações internacionais e missões diplomáticas ou consulares;
    vi. Prejudicar a aplicação da lei, em particular a prevenção e deteção de crimes, a detenção ou acusação de infratores e a administração da justiça;
    vii. Que resulte na divulgação de comunicações confidenciais entre médico e paciente, advogado e cliente, jornalista e fontes, ou que, de outra forma, estejam protegidas contra a divulgação em processos judiciais; ou
    viii. Comprometa a integridade de um exame profissional ou de um processo de recrutamento.
e. Isenções específicas relativas aos dados: Para além das isenções acima referidas, os dados podem ser retidos quando:
    i. A divulgação de dados anonimizados criasse um risco significativo de reidentificação de indivíduos ou grupos, e tal risco não pudesse ser adequadamente mitigado através de medidas técnicas ou organizacionais.
    ii. A divulgação de algoritmos, código-fonte ou modelos proprietários comprometa substancialmente a integridade, a segurança ou o funcionamento de sistemas algorítmicos, desde que tal retenção não impeça uma responsabilização significativa pelas decisões que afetam os direitos individuais.
    iii. A divulgação de especificações técnicas, protocolos de acesso ou medidas de segurança criaria um risco substancial de acesso não autorizado, manipulação ou danos aos sistemas de tratamento de dados.
    iv. A divulgação violaria direitos de propriedade intelectual protegidos pela legislação nacional, desde que tais direitos não sejam utilizados para impedir o acesso legítimo a dados de interesse público ou para frustrar o direito de acesso a dados gerados pelos utilizadores.
f. As isenções estabelecidas nas secções acima devem ser interpretadas de forma restrita. Quando o interesse público na divulgação se sobreponha ao prejuízo para o interesse protegido, os dados devem ser divulgados.

22. Salvaguardas

Espera-se que os organismos públicos apliquem salvaguardas ao acesso ou reutilização de dados públicos, segundo as quais:

a. O acesso só é concedido quando o organismo do setor público ou o organismo competente, na sequência do pedido, tiver garantido que os dados foram anonimizados, no caso de dados pessoais.
b. No caso de informações comercialmente confidenciais, incluindo segredos comerciais ou conteúdos protegidos por direitos de propriedade intelectual, o acesso pode depender da modificação, agregação ou tratamento dos dados através de outros métodos de controlo da divulgação.
c. Os organismos públicos devem impor condições que preservem a integridade dos dados, reservando-se o direito de verificar o processo, os meios e os resultados do tratamento de dados realizado pelo reutilizador, bem como o direito de limitar a utilização dos resultados do tratamento que prejudiquem os direitos e interesses do organismo público ou de terceiros, sem sobrepor-se ao interesse público.
d. Em conformidade com a Convenção da União Africana sobre a Prevenção e o Combate à Corrupção, devem existir proteções contra retaliações, bem como garantias de anonimato e imunidade legal no que diz respeito a divulgações de boa-fé por parte de denunciantes que alertem para práticas de gestão de dados que restrinjam arbitrariamente os direitos de acesso aos dados.

Garantias para os intervenientes privados:

a. Os agentes privados sujeitos a obrigações de acesso ao abrigo das presentes Orientações devem, em conformidade com a legislação nacional, assegurar as seguintes salvaguardas:
    i. O acesso para reutilização de dados só será concedido quando o agente privado tiver assegurado que os dados pessoais foram anonimizados, a menos que o acesso se destine a um fim de interesse público que exija dados pessoais;
    ii. As informações comercialmente confidenciais, incluindo segredos comerciais ou propriedade intelectual, devem ser modificadas, agregadas ou tratadas por qualquer outro método de controlo da divulgação, a menos que a divulgação seja exigida por um interesse público superior;
    iii. Quando o acesso for concedido através de um ambiente de tratamento seguro, o agente privado deve manter a integridade e a segurança do ambiente e reservar-se o direito de verificar o processo, os meios e os resultados do tratamento efetuado pelo reutilizador;
    iv. Quaisquer condições impostas ao acesso ou à reutilização devem ser publicamente disponíveis, claramente enunciadas e aplicadas de forma não discriminatória.
b. Os agentes privados devem incluir condições contratuais ou outras condições juridicamente vinculativas que proíbam os reutilizadores de utilizar os dados acedidos para:
    i. Vigilância ilegal ou discriminação;
    ii. Violação dos direitos à privacidade ou à proteção de dados;
    iii. Assédio;
    iv. Qualquer finalidade que viole o direito internacional em matéria de direitos humanos.

Aplicação

23. Responsabilidade:

O órgão de supervisão designado, de preferência a Comissão de Informação ou equivalente (ver Apêndice C), será responsável pela aplicação destas Orientações, monitorando assim o cumprimento, investigando violações e emitindo diretivas.

24. Conformidade e auditorias

a. A supervisão deve promover, e pode exigir, que os organismos públicos e privados realizem auditorias regulares para reforçar práticas proativas de divulgação de dados. Como parte deste processo, as instituições podem ser encorajadas a publicar, pelo menos anualmente, uma lista dos conjuntos de dados sob a sua

custódia, incluindo informações sobre o seu estatuto de acessibilidade (aberto, restrito ou confidencial), juntamente com justificações para quaisquer restrições.

b. A autoridade de supervisão deve realizar auditorias e inspeções regulares para garantir o cumprimento das normas de gestão, divulgação e ética de dados.

25. Sanções e Recursos

26. Os Estados devem adotar medidas políticas, regulamentares ou administrativas para lidar com o incumprimento das obrigações de divulgação proativa ou dos pedidos de dados. Tais medidas devem responder a:

a. A destruição, danificação, alteração, ocultação ou falsificação deliberada ou negligente de dados e a obstrução ou interferência no desempenho das funções de um detentor de dados ou de um mecanismo de supervisão, reconhecendo estes atos como infrações sujeitas a medidas corretivas adequadas, devem ser estabelecidos como crimes puníveis por lei.

b. As instituições, os responsáveis e os executivos de instituições que apresentem um padrão de incumprimento das obrigações de divulgação proativa ou que tenham sistematicamente obstruído a divulgação podem ser sancionados de acordo com os quadros regulamentares. Um órgão de supervisão independente terá o direito de publicar relatórios sobre padrões de incumprimento das obrigações de divulgação proativa ou de obstrução sistemática da divulgação, bem como sobre as sanções aplicáveis.

27. As medidas devem ser proporcionadas e sujeitas ao seguinte quadro escalonado:

a. Nível 1: Transparência – O órgão de supervisão independente deve emitir um relatório público identificando a natureza e a extensão do incumprimento e recomendando medidas corretivas.

b. Nível 2: Ação corretiva – Deve ser concedido à entidade um prazo razoável, não inferior a 90 dias, para corrigir o incumprimento. O órgão de supervisão pode prestar assistência técnica para facilitar o cumprimento.

c. Nível 3: Recursos civis – Os indivíduos afetados, as organizações da sociedade civil e as instituições nacionais de direitos humanos terão legitimidade para requerer medidas cautelares, indemnizações ou decisões declaratórias perante um tribunal independente por danos decorrentes do incumprimento.

d. Nível 4: Sanções judiciais – Quando o incumprimento for persistente, grave e não corrigido após o esgotamento dos Níveis 1 a 3, poderão ser impostas sanções proporcionadas, mas apenas:
   i. Por decisão de um tribunal ou tribunal independente e imparcial;
   ii. Na sequência da constatação de incumprimento persistente, flagrante e não sanado;
   iii. Sendo a sanção proporcional à natureza e gravidade da violação.

e. Condições:
   i. As autoridades administrativas não terão o poder de impor sanções financeiras, revogações de licenças, restrições operacionais ou proibições de acesso à plataforma sem autorização judicial independente prévia.

f. As medidas de responsabilização previstas nesta secção não devem ser utilizadas para:
   i. Vitimização política;
   ii. Censura arbitrária da liberdade de expressão;
   iii. Coação económica;
   iv. Vigilância ou assédio de utilizadores, jornalistas ou defensores dos direitos humanos.

28. Recusas:

a. Os requerentes cujo pedido de divulgação de dados seja recusado devem receber uma justificação por escrito e poder iniciar uma revisão interna, sem custos, num prazo razoável, por exemplo, entre 30 e 45 dias.

b. A análise desses recursos deve ocorrer no prazo máximo de 90 dias e ser comunicada em formatos claros e acessíveis. Os requerentes mantêm o direito de recorrer a instâncias adicionais através de órgãos judiciais ou outros órgãos independentes, em conformidade com os procedimentos nacionais.
c. As decisões de recurso e revisão devem ser comunicadas em formatos acessíveis, sem taxas administrativas,
d. Os indivíduos afetados, as organizações da sociedade civil e as instituições nacionais de direitos humanos terão legitimidade para recorrer a órgãos judiciais ou outros órgãos independentes, tais como medidas cautelares, indemnizações ou decisões declaratórias perante um tribunal independente, relativamente a danos decorrentes do incumprimento.

ACESSO, ÉTICA E IA

Os conjuntos de dados utilizados para IA devem ser precisos, representativos e geridos de forma segura, com salvaguardas para impedir o acesso não autorizado, a manipulação ou as violações. O público deve ter acesso aos dados relativos ao cumprimento dessas normas éticas.

29. Medidas recomendadas:

a. Os sistemas de IA utilizados na prestação de serviços públicos ou na governação devem ser obrigados a apresentar avaliações de impacto sobre os direitos humanos que abranjam os dados envolvidos. Isto é essencial para identificar e mitigar preconceitos relacionados com os dados que possam exacerbar as desigualdades estruturais e a discriminação, e o público tem o direito de aceder aos dados sobre essas avaliações.
b. Pode ser exigido aos prestadores de serviços de IA que comuniquem como estão a identificar e a mitigar os riscos éticos e em matéria de direitos antes da implementação, incluindo a forma como as questões de qualidade e acesso aos dados podem estar implicadas no viés dos dados, no viés algorítmico, na explicabilidade e na responsabilização. O público tem o direito de aceder aos dados contidos nesses relatórios.
c. Os direitos de acesso aos dados podem ser alargados a atores privados, incluindo plataformas digitais, cuja utilização de inteligência artificial e de sistemas de tomada de decisão automatizada tem o potencial de afetar direitos fundamentais. No caso de plataformas digitais, as avaliações de impacto sobre os direitos humanos exigidas podem incluir avaliações dos dados e do acesso aos dados no que diz respeito à forma como a moderação de conteúdos, a classificação e os sistemas de recomendação afetam os direitos de acesso à informação, à privacidade, à liberdade de expressão e à não discriminação. O público tem o direito de aceder a tais avaliações.
d. As partes interessadas, incluindo as comunidades afetadas, devem ser envolvidas na conceção, implementação e avaliação dos sistemas de IA para garantir o alinhamento com os valores e expectativas da sociedade, nomeadamente no que diz respeito ao acesso aos dados, bem como à proveniência, qualidade, representatividade e segurança dos dados.
e. A cooperação regional e sub-regional em África apoiará a aplicação eficaz destas normas a nível nacional.

IMPLEMENTAÇÃO

30. A operacionalização destas Orientações abrangerá várias etapas:

a. É necessário adotar medidas legislativas, administrativas, judiciais, orçamentais e outras para dar efeito a estas Orientações e facilitar a sua divulgação.
b. Estas orientações foram concebidas para serem implementadas através de uma abordagem multilateral, garantindo a participação significativa do governo, do setor privado, da sociedade civil, dos meios de comunicação social, do meio académico, da comunidade técnica e das comunidades afetadas na conceção, implementação e supervisão de políticas e práticas.

c. Os Estados podem colaborar com a sociedade civil, os meios de comunicação social, o meio académico, o setor privado e as comunidades para conceber, implementar e monitorizar políticas e práticas relativas aos dados, incluindo no que diz respeito ao acesso aos dados. Além disso, os Estados podem colaborar ativamente com o Relator Especial sobre a Liberdade de Expressão e o Acesso à Informação em África à medida que avançam, fornecendo perspetivas nacionais para informar sobre a forma como os dados servem como uma força poderosa para os direitos humanos, a transparência, a inclusão e o desenvolvimento em toda a África.
d. É necessário que existam programas nacionais de literacia de dados e competências digitais para capacitar o público a compreender os seus direitos em matéria de dados, e que as entidades reguladoras avaliem os sistemas de recomendação online e de moderação de conteúdos baseados em dados, bem como os modelos de negócio das plataformas.
e. O desenvolvimento profissional contínuo é essencial para os funcionários públicos nas áreas da governação de dados, acesso, gestão da qualidade e utilização ética, de modo a informar a tomada de decisões baseadas em evidências.
f. São necessários recursos dedicados e contínuos para melhorar a qualidade, a integridade e a exaustividade dos dados públicos em todos os setores, uma vez que a má qualidade dos dados constitui um obstáculo significativo ao valor que é desbloqueado pelo acesso público aos dados.
g. Os Estados podem adotar e aplicar periodicamente indicadores de desempenho mensuráveis para a implementação do acesso aos dados no âmbito de quadros de governação de dados, desenvolvidos através de consulta pública.
h. Deve haver revisões periódicas dos quadros de acesso aos dados e da sua aplicação, pelo menos de três em três a cinco em cinco anos, para se adaptarem às mudanças tecnológicas e às experiências de implementação. As conclusões dessas revisões devem ser tornadas públicas e formalmente comunicadas ao parlamento ou a um órgão de supervisão equivalente, a fim de garantir a transparência e a responsabilização.
i. Em conformidade com o artigo 62.º da Carta Africana, cada Relatório Periódico apresentado à ACHPR pode fornecer informações detalhadas sobre as medidas tomadas para facilitar o cumprimento das disposições das presentes Orientações.
j. O Relator Especial incentivará revisões nacionais dos quadros de acesso aos dados e poderá envolver-se no desenvolvimento de orientações adicionais e na apresentação voluntária de relatórios por parte dos Estados ou instituições sobre os progressos na implementação da Resolução 620.

ANEXO A: MEDIDAS PARA DADOS ESPECÍFICOS

1. Categorias selecionadas de dados:

a. Os dados sensíveis devem ser encriptados, ter o acesso limitado e ser tratados apenas para fins explicitamente autorizados.
b. O acesso aos dados de crianças deve estar em conformidade com a Convenção das Nações Unidas sobre os Direitos da Criança e com a necessidade de uma governança de dados sensível às crianças, incluindo mecanismos de consentimento e proteção.
c. Devem existir salvaguardas contra a estigmatização ou a utilização indevida de dados relativos a grupos marginalizados, em conformidade com as Orientações da ONU sobre a Desagregação de Dados para os ODS, bem como com os princípios da CARE sobre a Soberania dos Dados Indígenas.
d. Os dados desagregados por sexo são essenciais para apoiar a igualdade de género, de acordo com o Conjunto Mínimo de Indicadores de Género da ONU Mulheres.

2. Dados Orçamentais e Fiscais:

a. Os requisitos podem prever a publicação de conjuntos de dados legíveis por máquina sobre contratos públicos, despesas fiscais e dívida, em conformidade com o Índice de Orçamento Aberto e as normas da *International Budget Partnership*.

3. Dados de Investigação Financiados com Fundos Públicos:

a. As políticas nacionais e as medidas institucionais podem especificar regimes de acesso aos dados de investigação financiados com fundos públicos, de acordo com os seguintes objetivos e princípios:
   i. Abertura: equilibrar os interesses do acesso aberto aos dados para aumentar a qualidade e a eficiência da investigação e da inovação com a necessidade de restrições justificáveis que reconheçam os direitos de propriedade intelectual, a proteção de dados pessoais e a confidencialidade, a segurança e os interesses comerciais legítimos
   ii. Transparência: disponibilizar e tornar acessíveis informações claras sobre as organizações produtoras de dados, documentação sobre os dados que produzem e especificações das condições associadas à utilização desses dados.
   iii. Responsabilidade formal: promover regras institucionais explícitas e formais sobre as responsabilidades das várias partes envolvidas em atividades relacionadas com dados no que diz respeito à autoria, créditos dos produtores, propriedade, restrições de utilização, acordos financeiros, regras éticas, condições de licenciamento e responsabilidade.
   iv. Conformidade legal: prestar a devida atenção, na conceção de regimes de acesso a dados de investigação digitais, aos requisitos legais nacionais relativos à segurança nacional e à privacidade.
   v. Proteção da propriedade intelectual: descrever formas de obter acesso aberto ao abrigo dos diferentes regimes jurídicos de direitos de autor ou de outras leis de propriedade intelectual aplicáveis a bases de dados, bem como a segredos comerciais.
   vi. Interoperabilidade: prestar a devida atenção aos requisitos das normas internacionais relevantes para a utilização de múltiplas formas, em cooperação com organizações internacionais.
   vii. Qualidade e segurança: promover boas práticas no que diz respeito aos métodos, técnicas e instrumentos utilizados na recolha, divulgação e arquivo acessível de dados, de modo a permitir o controlo de qualidade através da revisão por pares e de outros meios de salvaguarda da autenticidade, originalidade, integridade e segurança, bem como de determinação da responsabilidade.
   viii. Eficiência: promover uma maior rentabilidade no sistema científico africano e global, através da promoção de boas práticas na gestão de dados, no acesso e nos serviços de apoio especializados.
   ix. Responsabilização: avaliar o desempenho dos regimes de acesso aos dados para maximizar o apoio ao acesso aberto entre a comunidade científica e a sociedade em geral.

b. As instituições de investigação devem desenvolver Políticas de Gestão de Dados de Investigação. Estas políticas devem estabelecer regras e diretrizes sobre a forma como os dados de investigação devem ser recolhidos, armazenados e partilhados, em conformidade com as melhores práticas nacionais e internacionais para reutilização para fins comerciais ou não comerciais, na medida em que sejam financiados com fundos públicos, e disponibilizá-los publicamente através de um repositório institucional ou temático que permita o acesso e a partilha de dados.

c. Todas as instituições académicas e de investigação, bem como quaisquer entidades que tratem dados académicos, devem estabelecer, implementar e divulgar publicamente protocolos claros para a conservação, anonimização e destruição desses dados. Estes protocolos devem incluir salvaguardas específicas para impedir a reutilização ilegal de trabalhos apresentados por estudantes e outros resultados de investigação.

Dados de saúde:

a. Criar um ecossistema digital de saúde interoperável que facilite a troca segura de dados, salvaguardando simultaneamente a privacidade dos doentes. Uma abordagem baseada nas oportunidades e nos riscos pode servir de base a procedimentos claros de revisão e aprovação e a processos de aprovação simplificados que envolvam múltiplas organizações.
b. É necessário distinguir entre dados agregados de saúde pública (que devem ser abertos) e dados pessoais de saúde (que devem ser protegidos), orientando-se pelos Princípios de Governação de Dados de Saúde da OMS.
c. As seguintes medidas garantirão o acesso aos dados de saúde para reutilização:
    i. Introduzir melhorias concretas em matéria de privacidade e transparência, uma vez que a confiança do público é crucial para a obtenção de dados dos doentes.
    ii. Estabelecer um ambiente de dados centralizado e seguro para padronizar o tratamento dos dados dos doentes, impor o armazenamento padronizado e a curadoria de um catálogo de conjuntos de dados de uso comum, com diretrizes claras sobre quais as entidades elegíveis para acesso.
    iii. Criar uma biblioteca online para disponibilizar código de curadoria de dados, testes e documentação, a fim de garantir o acesso a dados bem curados.
    iv. Desenvolver um mapa único que detalhe todos os procedimentos de aprovação com todas as organizações relevantes, garantindo a transparência dos critérios de aprovação, as agências reguladoras responsáveis pela aprovação e prazos claros e transparentes para as decisões de acesso.
    v. Criação de uma aplicação comum para questões éticas, orientação sobre a informação e permissões de acesso.

Dados ambientais:

a. Devem existir obrigações claras para a divulgação proativa de dados ambientais, em conformidade com os quadros continentais e regionais, tais como o Princípio 10 da Declaração do Rio e a Convenção de Aarhus da UNECE, alinhadas com os instrumentos de governação nacionais relativos aos recursos naturais.
b. São necessários requisitos para que as autoridades públicas e as empresas privadas, particularmente aquelas que operam na indústria extrativa e de alto impacto, publiquem dados de impacto ambiental e social de forma aberta e abrangente. Esta divulgação deve incluir avaliações de referência, relatórios de monitorização e medidas de mitigação de riscos, garantindo que as comunidades e as partes interessadas tenham acesso atempado à informação que afeta os seus direitos, meios de subsistência e ambientes. De acordo com a Iniciativa de Transparência das Indústrias Extrativas (EITI), devem ser exigidos dados desagregados em termos de impacto nas empresas, nos projetos e nas comunidades.
c. É essencial prever disposições para o acesso em tempo real ou quase real a dados relativos a riscos ambientais (por exemplo, poluição, desflorestação).
d. É necessário o acesso a dados sobre o consumo de energia dos centros de dados para armazenamento e processamento, bem como sobre a gestão, reciclagem e exposição de resíduos eletrónicos.

Dados privados no interesse público:

a. Para libertar o valor dos dados em toda a economia, são necessárias medidas que garantam que os dados do setor privado estejam adequadamente disponíveis, acessíveis e utilizáveis para fins de interesse público e em toda a economia, protegendo simultaneamente os direitos sobre os dados e a propriedade intelectual do setor privado.
b. A governação deve garantir a disponibilidade de normas de dados abertas e interoperáveis para divulgações proativas por parte do setor privado, a fim de permitir a utilização de dados no interesse público.
c. É necessário promover a sensibilização entre as organizações do setor privado para os benefícios sociais da divulgação proativa e da partilha de dados, através de contactos regulares com o setor privado.
d. Os Estados podem explorar incentivos, tais como programas de reconhecimento público, para aumentar a divulgação proativa de dados do setor privado e a partilha de dados pelo setor privado numa base voluntária.

e. São necessárias medidas para promover a transparência em todas as colaborações de partilha de dados, incluindo os dados utilizados e o impacto da colaboração.

Orientação setorial:

É importante dispor de mecanismos de autorregulação ou de corregulação — incluindo orientações voluntárias, normas, códigos de conduta e modelos a nível setorial para acordos de acesso e partilha de dados.

8. Acesso aos dados detidos pelas plataformas digitais no interesse público:

a. As plataformas devem comprometer-se a uma maior transparência no que diz respeito às suas práticas de recolha de dados, tomada de decisões algorítmica e termos de serviço relacionados com o acesso aos dados.
b. Os Estados africanos podem superar as desvantagens em termos de poder face às plataformas digitais, garantindo uma abordagem pan-africana à governação das empresas multinacionais que são detentoras significativas de dados, incluindo a cooperação para desenvolver um Código de Conduta continental relativo ao acesso das partes interessadas aos dados no interesse público.
c. Este Código de Conduta, adaptado e atualizado regularmente a nível nacional pela Comissão de Informação (ou equivalente), pode incluir, entre outras, as seguintes disposições:
    i. Essas plataformas devem comprometer-se a abster-se de iniciar, prosseguir ou ameaçar com ações judiciais contra investigadores, jornalistas e atores da sociedade civil africanos que se dediquem à recolha automatizada (scraping) de dados acessíveis ao público a partir dos seus serviços para fins legítimos de interesse público, em particular nos casos em que a plataforma não disponibilize mecanismos de acesso alternativos.
    ii. As plataformas devem ser obrigadas a desenvolver e fornecer ativamente mecanismos de acesso robustos, seguros, auditáveis e não discriminatórios (por exemplo, APIs, acordos de partilha de dados, ambientes *sandbox*) para as partes interessadas que procurem dados não acessíveis ao público ou acesso estruturado a dados de acesso público. Tais mecanismos devem ter um preço razoável (se aplicável) para utilizações sem fins lucrativos e devem oferecer acesso atempado a dados em tempo real.
    iii. Devem ser estabelecidos critérios claros sobre o que constitui «investigação de interesse público legítimo», abrangendo áreas como, entre outras, estudos sobre viés algorítmico, danos online aos direitos humanos, desinformação e/ou discurso de ódio, concorrência de mercado, aspetos socioeconómicos e psicológicos e compreensão científica mais ampla.
    iv. Essa investigação deve respeitar as diretrizes éticas, as leis de proteção de dados e as normas de integridade académica, jornalística ou outra integridade profissional.
    v. Existem mecanismos para a verificação de pedidos de dados de boa-fé com base em critérios de interesse público e normas éticas, bem como para a aplicação de decisões, resolução de litígios e revisão periódica do cumprimento do presente Código de Conduta, geridos pelo Regulador da Informação (ou equivalente), pelo Instituto Nacional de Estatística ou por uma instituição de investigação nacional (ou equivalente).

ANEXO B: MEDIDAS INSTITUCIONAIS

Divulgação proativa

1. Os organismos públicos devem ser obrigados, mesmo na ausência de um pedido específico, a publicar proativamente dados de interesse público, incluindo informações sobre as suas funções, competências, estrutura, responsáveis, decisões, orçamentos, despesas e outras informações relacionadas com as suas atividades.
2. Quando organismos privados realizam atividades em nome de organismos públicos, e para as quais são utilizados fundos públicos ou são desempenhadas funções ou serviços públicos, os organismos públicos devem exigir que esses organismos privados publiquem proativamente dados decorrentes dessas atividades no interesse público; ou facilitar a publicação desses dados no interesse público.

Priorização da divulgação de conjuntos de dados de elevado valor

3. Os organismos públicos devem divulgar proativamente «conjuntos de dados de elevado valor» (HVD) de forma gratuita, em formatos legíveis por máquina e acessíveis através de Interfaces de Programação de Aplicações (API).
4. As categorias temáticas para os HVD incluem dados geoespaciais, estatísticos, de propriedade de empresas e meteorológicos, entre outros.

Formatos abertos, interoperáveis e legíveis por máquina

5. Os organismos do setor público devem disponibilizar documentos e dados para reutilização em formatos abertos e legíveis por máquina. Esta medida visa facilitar a reutilização e a interoperabilidade sem descontinuidades em toda a UA.

Transparência nas condições de reutilização

6. Os organismos públicos devem ser transparentes quanto às condições de reutilização dos dados. Isto inclui a publicação da licença padrão ou de outra licença aberta e a disponibilização online de informações sobre os dados disponíveis, incluindo metadados, de forma facilmente acessível.

Acesso justo e não discriminatório

7. Os organismos do setor público estão proibidos de celebrar acordos exclusivos para a reutilização de dados públicos, exceto em circunstâncias muito limitadas e excecionais, a fim de garantir uma concorrência leal no mercado dos serviços baseados em dados.

Políticas de acesso aos dados

8. As políticas dos organismos públicos em matéria de acesso aos dados devem abranger a recolha, o armazenamento, a partilha, a qualidade, a conservação, a eliminação e a segurança, no âmbito de disposições mais amplas e abrangentes de gestão de dados. Para proteger os dados contra o acesso não autorizado, violações ou perda, é necessário que existam medidas técnicas e organizacionais robustas, incluindo armazenamento seguro, encriptação e controlo de acesso.

Cobrança de custos marginais

9. Os dados do setor público devem estar disponíveis gratuitamente. Nos casos em que são aplicadas taxas, estas limitam-se geralmente aos custos marginais incorridos com a reprodução e a divulgação.

ANEXO C: ARQUITETURA INSTITUCIONAL PARA O ACESSO A DADOS

Órgão de supervisão independente:

Um mecanismo de supervisão independente e imparcial, idealmente uma Comissão de Informação (ou híbrida ou equivalente) estabelecida por lei, tem o mandato de monitorizar, promover e proteger o direito de acesso à informação e aos dados e de resolver litígios. Isto implica que:

a. A independência de tal órgão deve ser garantida por lei, que deve estipular um processo de nomeação transparente e participativo, um mandato claro e específico, remuneração e recursos adequados, e responsabilidade final perante o poder legislativo. A Comissão de Informação requer capital humano adequado, ou seja, pessoas com competências atualizadas para utilizar dados e conceber políticas e regulamentos.
b. Os organismos públicos e os organismos privados relevantes devem ser obrigados a reconhecer as decisões da Comissão de Informação como juridicamente vinculativas em todas as matérias relacionadas com o acesso aos dados, incluindo a resolução de litígios.

c. Os poderes da Comissão da Informação incluirão a competência para emitir ordens a organismos públicos, obrigando-os a divulgar informações, bem como a possibilidade de tomar medidas punitivas contra os funcionários que se recusem a cumprir essas ordens.
d. A Comissão de Informação deve acreditar Intermediários de Dados para facilitar o cumprimento das normas de governação e acesso aos dados e promover um mercado competitivo na intermediação de dados.
e. A Comissão de Informação assegura que as partes interessadas sejam responsabilizadas, de acordo com as suas funções, pela integridade dos dados que disponibilizam e pela implementação sistemática de medidas de gestão de risco ao longo de todo o ciclo de valor dos dados, incluindo medidas para proteger a segurança, a confidencialidade, a qualidade e a disponibilidade dos dados. Para o efeito, a Comissão de Informação irá:
    i. Promover a adoção de avaliações de impacto e auditorias, bem como a gestão responsável do acesso aos dados.
    ii. Supervisionar a adoção de normas de serviço público (por exemplo, tempos de resposta, processos de recurso), implementar mecanismos de consulta, criar uma cultura de confiança na função pública e desencorajar a aversão indevida ao risco na divulgação de dados.
    iii. Clarificar as funções e responsabilidades entre as agências detentoras de dados nas instituições públicas, apoiar o reforço de capacidades, a alocação de recursos e o desenvolvimento de competências, e promover parcerias para apoiar estas iniciativas.
    iv. Incluir nas suas funções a promoção da literacia de dados junto do público em geral, bem como no currículo da função pública.
    v. Operar um mecanismo de comunicação pública regular sobre o estado da abertura de dados e dos pedidos de acesso, e fornecer relatórios de transparência sobre o seu próprio funcionamento na adjudicação e promoção do acesso aos dados.

Institutos Nacionais de Estatística:

a. O papel dos Serviços Nacionais de Estatística (SNE) dos Estados enquanto coletores de dados deve ser reforçado para que desempenhem a função de gestor central de dados e coordenador num Quadro Integrado de Gestão Nacional de Dados.
b. O NSO deve colaborar com os detentores de dados, os intermediários de dados e os organismos públicos para apoiar o acesso e a partilha de dados, garantindo que os ativos de dados de um país sejam utilizados de forma eficaz e ética para o bem público.
c. O NSO deve estabelecer e manter normas para a recolha, o tratamento e a divulgação de dados e colaborar com a Comissão de Informação (ou equivalente) para promover o desenvolvimento de competências nos organismos públicos para a implementação de normas de dados, e ajudar a garantir que os dados provenientes de diferentes fontes sejam consistentes, coerentes e interoperáveis.
d. Para incentivar e promover a adoção de normas em todo o setor público, o INE deve avaliar e articular os benefícios da adoção de normas de dados, formular e implementar processos para ajudar a identificar e demonstrar a implementação de normas, ou projetos-piloto de novas normas para demonstrar o valor da sua adoção.
e. Para efeitos da implementação do Quadro Nacional Integrado de Gestão de Dados, o INE deve garantir:
    i. a confiança entre as partes interessadas na proteção dos dados, de modo a maximizar o valor público e, simultaneamente, prevenir a utilização indevida.
    ii. iniciativas de financiamento para o acesso e utilização de dados, incluindo financiamento para infraestruturas e competências.
    iii. incentivos adequados para que os organismos públicos produzam, protejam e partilhem dados.
    iv. medidas adequadas para garantir a capacidade de procura de dados e uma cultura de utilização de dados.

Conselho Consultivo Nacional de Dados:

a. Os Estados podem considerar a criação de um Conselho Consultivo Nacional de Dados ou de outro órgão semelhante, no âmbito da Comissão de Informação existente ou das entidades reguladoras nacionais de dados/informação. O Conselho deve ajudar a desenvolver o Quadro Nacional Integrado de Gestão de Dados, aconselhar o governo nacional, a Comissão de Informação (ou equivalente), o Instituto Nacional de Estatística e as instituições nacionais de investigação. Deve realizar monitorização e formular recomendações.
b. A composição do Conselho deve incluir representantes do governo, da Comissão de Informação (ou equivalente), do Instituto Nacional de Estatística e de centros de investigação nacionais, bem como de partes interessadas não estatais do setor privado, do meio académico, dos meios de comunicação social e da sociedade civil.

Poder Judicial:

a. As autoridades judiciais promovem a justiça aberta, facilitando a partilha de dados e o acesso aos mesmos através da publicação atempada de decisões judiciais em formatos abertos, bem como da divulgação proativa de informações sobre como as pessoas podem ter acesso à justiça.
b. Para equilibrar o direito de acesso aos dados com outros direitos e obrigações, as decisões judiciais relativas ao acesso alinhar-se-ão com as normas internacionais de: (i) Adequação (a medida deve ser adequada para alcançar o objetivo pretendido); (ii) Necessidade (deve ser utilizado um meio menos restritivo, se este for igualmente eficaz); e (iii) Proporcionalidade no sentido estrito (a medida não deve ser excessiva em relação ao objetivo).

Órgãos de Gestão Eleitoral e Dados:

a. Os órgãos de gestão eleitoral (OGE) são instados a estabelecer e aplicar um conjunto acordado de princípios relativos aos dados que possam ajudar a promover a transparência eleitoral e a definir normas e expectativas claras para os partidos políticos, candidatos e meios de comunicação social, no que diz respeito à criação, gestão e acesso aos dados aplicáveis.
b. Os OGE podem desenvolver e implementar medidas para dar maior destaque a dados precisos e a fontes de dados oficiais nas plataformas digitais.
c. Estes órgãos podem operar quadros normalizados para salvaguardar a integridade dos dados eleitorais, a divulgação responsável de dados e a partilha de dados sobre tendências de desinformação, contramedidas eficazes e opinião pública.
d. Devem ser assegurados canais de comunicação eficazes entre as plataformas online e as partes interessadas nas eleições, e devem existir medidas algorítmicas para dar prioridade ao acesso a dados precisos sobre as eleições.
e. Os OGE facilitam relações eficazes com organizações de monitorização eleitoral, a sociedade civil, investigadores, jornalistas e outras partes interessadas no processo eleitoral, bem como com plataformas digitais, para permitir o acesso rápido aos dados eleitorais e respostas atempadas a ameaças à integridade dos dados e à desinformação baseada em dados.
f. É necessário reforçar as obrigações legislativas nacionais aplicáveis às plataformas, incluindo as plataformas de publicidade, que são importantes detentoras de dados, de modo que sejam obrigadas por lei a fornecer dados sobre:
    i. As suas avaliações de impacto em matéria de direitos humanos no que diz respeito às eleições
    ii. Os seus planos de mitigação de riscos eleitorais
    iii. Os seus acordos de cooperação, por exemplo, com organismos eleitorais, meios de comunicação social, sociedade civil e verificadores de factos.