União Africana

An Integrated, Prosperous and Peaceful Africa

QUADRO DA POLÍTICA DE DADOS DA UA

ÍNDICE

PREÂMBULO

Os países africanos compreendem o enorme potencial de uma economia digital robusta para criar novas oportunidades de negócio, aumentar a eficiência, contribuir para o desenvolvimento sustentável e mudar a vida das pessoas. A explosão do volume de dados como um ativo estratégico e um elemento preponderante da economia e sociedade contemporâneas tem desempenhado um papel central na formulação de políticas, na inovação e na criação de emprego.

A adoção da Estratégia de Transformação Digital (DTS) para África 2020-2030, juntamente com a operacionalização da Zona de Comércio Livre Continental (ZCLC), traz grandes oportunidades para mercados mais interligados e interoperáveis e abre caminho à prosperidade de start-ups tecnológicas e negócios eletrónicos. Neste contexto, a Comissão desenvolveu o Quadro da Política de Dados da UA, que foi aprovado pelo Conselho Executivo da UA em fevereiro de 2022.

De igual modo, o Quadro de Política de Dados da UA representa um passo importante com vista à criação de um ambiente de dados consolidado e sistemas harmonizados de governação dos dados digitais para possibilitar a circulação dos dados, de forma livre e segura, no continente, respeitando os direitos humanos, salvaguardando a segurança e garantindo o acesso e a partilha dos benefícios, de forma equitativa.

Este quadro estabelece uma visão comum tal como os princípios, as prioridades estratégicas e as principais recomendações que devem servir de orientação aos países africanos no desenvolvimento de sistemas nacionais de dados e competências para utilizarem os dados efetivamente e ex traírem valor dos mesmos.

A aprovação deste documento de política continental pelos órgãos da União Africana ilustra o compromisso e a vontade política dos líderes africanos de investir em dados mediante o reforço da colaboração intersectorial e o desenvolvimento da infraestrutura relacionada para alojar, autogerir, processar e usar os dados gerados pelas pessoas e pela indústria, para ajudar à formulação de políticas e aos processos decisórios. No âmbito deste quadro, os países africanos concordam em introduzir os mecanismos e os regulamentos necessários para permitir, de forma colaborativa, a circulação de dados em África e lançar as bases para a concretização do Mercado Único Digital.

A nossa abordagem aos dados é inclusiva, transformadora e orientada para o futuro. Pretendemos aproveitar o potencial da revolução dos dados para capacitar pessoas, instituições e empresas, promover o comércio digital intra-africano, contribuir para os esforços de integração económica, sensibilizar os cidadãos para as questões relacionadas com a proteção e a privacidade dos dados, promover a investigação e a inovação, salvaguardar a soberania e a apropriação por parte dos Estados, reforçar a confiança no ecossistema de dados e fortalecer a participação de África como uma frente unida e com uma posição uniforme nos fóruns multilaterais sobre várias áreas baseadas nos dados.

A internalização deste quadro por parte dos países africanos e a implementação das suas principais recomendações e intervenções propostas aos níveis nacional, regional e continental, juntamente com o desenvolvimento das capacidades necessárias em termos humanos e institucionais, posicionarão África como um parceiro forte e permitirão que os jovens africanos participem e prosperem na economia e na sociedade digitais à escala global.

Dr. Amani Abou-Zeid
Comissão da UA de Infra-estruturas e Energia

AGRADECIMENTOS

O Quadro da Política de Dados da UA foi preparado sob a orientação geral de Sua Excelência o Dr. Amani Abou-Zeid, Comissário de Infraestruturas e Energia, e um grupo de trabalho composto por Moses Bayingana, Diretor da Divisão da Sociedade de Informação, e Souhila Amazouz, Oficial Senior de Políticas (Coordenadora de Equipa), com os preciosos contributos de: Towela Nyirenda-Jere, Tichaona Mangwende e Gideon Nimako (AUDA- NEPAD); Jean Pierre Gashami e Omar Elmi Samatar (BAfD); Miriem Slimani (ATU); Aretha Mare e Jan Krewer (Smart Africa); Tunde Fafunwa, Mactar Seck e Linda Bonyo (UNECA); Torbjorn Fredriksson e Pilar Fajarnes Garces (CNUCED); Amr Farouk Safwat e May Ragab Abdelhamid (Presidente do secretariado do STC-CICT); Philip Sauerbaum (UE); Caroline Gaju (UIT); Seyni Fati (GSMA); Tapiwa Ronald Cheuka (CUA/ETIM); Marguerite Ouedraogo Bonane e Patricia Poku (Rede Africana de Autoridades de Proteção de Dados); Tania Priscilla Begazo Gomez, Marelize Gorgens e Mark Williams (Banco Mundial).

O Quadro beneficiou de apoio financeiro da GIZ e de apoio técnico de Research ICT Africa.

Os comentários foram recebidos em várias fases de produção deste Quadro por parte de especialistas africanos dos Estados-Membros da UA, das Comunidades Económicas Regionais e de Instituições Especializadas da UA que participaram na oficina de validação virtual e no 4.º Comité Técnico Especializado sobre Comunicação e TIC.

O Quadro da UA de Política de Dados foi aprovado pelo Conselho Executivo durante a sua 40.ª Sessão Ordinária nos dias 2 e 3 de fevereiro de 2022 por via da Decisão EX.CL/Dec.1144(XL).

Addis Abeba, fevereiro 2022

SUMÁRIO EXECUTIVO

Os dados são cada vez mais reconhecidos como um bem estratégico, integrante da elaboração de políticas, da inovação do sector privado e público e da gestão do desempenho, e criando novas oportunidades empresariais para empresas e indivíduos. Quando aplicadas aos serviços governamentais, as novas tecnologias podem gerar enormes quantidades de dados digitais e contribuir significativamente para o progresso social e o crescimento económico. O papel central dos dados requer uma perspetiva política e estratégica de alto nível que possa equilibrar múltiplos objetivos políticos – desde a libertação do potencial económico e social dos dados até à prevenção de danos associados à recolha e processamento em massa de dados pessoais.

O objetivo do presente documento é fornecer o quadro político para os países africanos maximizarem os benefícios de uma economia baseada em dados através da criação de um ambiente político favorável aos investimentos privados e públicos necessários para apoiar a criação de valor e a inovação baseada em dados. Este ambiente propício exige que os países trabalhem em conjunto em todos os setores, instituições e partes interessadas, alinhem as suas prioridades de desenvolvimento e harmonizem as políticas em todo o continente de forma a proporcionar a escala e o âmbito necessários para criar mercados globalmente competitivos.

De uma perspetiva política, a abordagem adotada é centrada nas pessoas, posicionando-as em relação ao papel dos dados na economia e sociedade contemporânea, identificando os elementos e ligações no que se pode chamar o "ecossistema de dados", a fim de identificar os pontos exatos da intervenção política. Isto permite uma avaliação sistémica dos desafios inter-relacionados decorrentes dos desenvolvimentos globais que têm impacto nas economias de dados nacionais emergentes e dos que surgem no contexto de uma atividade económica crescente com base em dados, de dotes institucionais desiguais, e do desenvolvimento humano em muitos países africanos. Isto permite a conceção de um quadro político de dados contextualmente fundamentado, mas orientado para o futuro, que utiliza a regulamentação económica para orientar os decisores políticos na realização de oportunidades de criação de valor a partir dos dados. O quadro indica as formas como as oportunidades podem ser concretizadas e como os riscos associados podem ser mitigados através da criação de um ambiente propício e de confiança.

A construção de uma economia de dados positiva nacional e regional exigirá níveis de colaboração sem precedentes entre os intervenientes para responder as pressões económicas e políticas já sentidas na economia global de dados. A fim de assegurar um acesso equitativo e seguro aos dados para a inovação e concorrência, os Estados-membros devem estabelecer uma abordagem jurídica unificada que seja clara, inequívoca e que ofereça proteção e obrigações em todo o continente. Sempre que necessário, os instrumentos jurídicos e instituições existentes devem ser revistos para garantir que não entrem em conflito entre si e que ofereçam níveis complementares de proteção e obrigações.

Uma estratégia global de dados incluirá necessariamente a harmonização entre a concorrência, o comércio e as políticas e leis fiscais, tanto a nível nacional como regional. Desta forma, um ecossistema de dados otimizado para África ajudará a equilibrar a mobilização de receitas com a necessidade de evitar distorções nos mercados locais e no sistema fiscal global. As leis de propriedade intelectual também devem ser revistas para esclarecer que não impedem geralmente os fluxos de dados ou a proteção de dados. Ao mesmo tempo,

os governos precisam de desenvolver políticas e estratégias digitais transversais para coordenar atividades em todo o sector público e entre os sectores público e privado para cumprir os objetivos nacionais.

Embora existam muitas definições diferentes do termo "dados", todas elas reconhecem que existem muitos tipos diferentes de dados. Existem também muitas formas de classificar os dados, o que influencia a escolha de uma política e de uma regulamentação adequadas para cada categoria, a fim de atenuar os riscos potenciais associados ao processamento, à transferência ou à conservação desses dados. Uma distinção essencial é a que existe entre dados pessoais e dados não pessoais, consistindo a proteção de dados em garantir o respeito pela privacidade das pessoas em causa. As diretrizes sobre a categorização dos dados devem ser uma das primeiras ações da autoridade reguladora da informação sobre dados, uma instituição fundamental para o desenvolvimento de um sistema nacional integrado de dados, que deve ser criado em parceria com todas as partes interessadas. Essencial para o desenvolvimento de um ambiente favorável à economia de dados é assegurar a infraestrutura digital fundamental e os recursos humanos necessários para desenvolver os dados como um bem estratégico. Deve ser dada a devida atenção ao desenvolvimento de sistemas robustos de identificação digital para a entrega de valor público e privado aos cidadãos e consumidores.

Conforme o quadro também sublinha, isto só pode ser devidamente alcançado através da indução de uma cultura de confiança no ecossistema de dados. Isto significa criar sistemas de dados seguros e protegidos, baseados em regras e práticas eficazes de segurança cibernética e de proteção de dados, bem como códigos de conduta éticos para aqueles que definem a política de dados, a implementam e para aqueles que utilizam os dados, quer no sector público quer no privado. No entanto, não é suficiente. A confiança na governação dos dados e num sistema de dados nacional é estabelecida através da legitimidade. Isso inclui sistemas e padrões que garantem a conformidade do setor público e privado, o próprio governo que adere às regras de proteção de dados pessoais e compartilha dados públicos.

O quadro sublinha a importância da colaboração e dos processos políticos baseados em provas para o enquadramento da política proposta. A governação e as disposições institucionais devem atribuir papéis claros ao governo como decisor político, e a reguladores independentes ágeis e capacitados para aplicarem a política e regularem eficazmente a economia dos dados, de modo a garantir que a concorrência leal produza resultados positivos para o bem-estar dos consumidores. A criação de reguladores de dados e da informação, para promover e salvaguardar os direitos dos cidadãos e a sua participação e representação justa na economia e sociedade de dados, terá de ser uma prioridade para os países que ainda não os tenham estabelecido. A coordenação com outros reguladores para alcançar este objetivo será essencial. O ecossistema jurídico deve ser harmonizado e reequilibrado.

O acesso aos dados é um pré-requisito para a criação de valor, o empreendedorismo e a inovação. Quando os dados são de má qualidade ou não interoperacionais, limitam a capacidade das empresas e do sector público de se envolverem na partilha e análise que podem fornecer valor económico e social aos dados. Estas estruturas de processamento devem alinhar-se com os seguintes princípios: consentimento e legitimidade; limitações à recolha; especificação da finalidade; limitação da utilização; qualidade dos dados; salvaguardas de segurança; abertura (que inclui a comunicação de incidentes, uma correlação importante com os imperativos da segurança cibernética e do crime cibernético); responsabilidade; e especificidade dos dados. Os modelos de segurança também precisam de ser transversais, com ênfase específica no armazenamento e processamento de dados sensíveis/proprietários na nuvem, na gestão de API e no apoio a economias de dados equitativas.

É necessário prestar atenção ao acesso a dados de qualidade, interoperacionais e fiáveis – principalmente do Estado, mas também do sector privado e de outros sectores – com um ressurgimento dos princípios de governação aberta em todo o continente. O reforço das capacidades deve ser uma prioridade nacional e regional fundamental, devendo ser atribuídos recursos a este respeito nas áreas de proteção de dados, segurança cibernética e governação de dados institucionais nas agências relevantes. As competências e uma compreensão do ecossistema de dados também terão de ser construídas em instituições estatais, entre outros sectores e comunidades.

O quadro é orientado pelos princípios gerais da transparência, responsabilidade das instituições e dos intervenientes, inclusão dos intervenientes, equidade entre os cidadãos e concorrência leal entre os intervenientes no mercado. Os princípios que norteiam o quadro incluem confiança, acessibilidade, interoperacionalidade, segurança, qualidade e integridade, representatividade e não discriminação.

Como o quadro sublinha, a colaboração transversal precisa de ser sustentada com mecanismos para estimular a procura de dados, o que inclui incentivar comunidades de dados inovadores, e, do lado da oferta, assegurar a qualidade, interoperacionalidade e relevância dos dados, tanto no sector público como no privado, e na sociedade civil.

Como o quadro sugere, existem vários processos, mecanismos e instrumentos regionais que podem e devem ser utilizados para impulsionar os esforços do continente com o objetivo de desenvolver um quadro político de dados coesos. Estes incluem o Acordo da Zona de Comércio Livre Continental Africana (ZCLCA), que proporciona uma oportunidade para a cooperação em vários aspetos importantes do quadro político. A colaboração entre as partes interessadas nacionais e regionais é também necessária para que os países africanos se tornem mais competitivos nos fóruns de definição de políticas globais onde são estabelecidos regulamentos para a economia global de dados, e onde os estados africanos têm sido, em grande parte, "seguidores de normas" elaboradas pelos outros atores.

Reconhece-se que os Estados africanos têm capacidades económicas, técnicas e digitais diferentes, pelo que as recomendações e ações devem ser interpretadas tendo isso em conta. Prevê-se, no entanto, que as diferentes exigências da construção de um ecossistema de dados sejam progressivamente realizadas pelos países. Ao mesmo tempo, há várias áreas que podem ser atendidas independentemente das capacidades económicas ou técnicas, incluindo o estabelecimento de independência regulamentar, a promoção de uma cultura de confiança e ética, a construção de quadros de colaboração para os sectores relevantes, o desenvolvimento de políticas e regulamentos transparentes, baseados em provas e participativos, a participação em processos e mecanismos regionais de colaboração, e a ratificação da Convenção da UA sobre Segurança Cibernética e Proteção de Dados Pessoais.

O quadro apresenta um conjunto de recomendações pormenorizadas e medidas conexas para orientar os Estados-Membros na formulação de políticas no seu contexto nacional, bem como recomendações para reforçar a cooperação entre países e promover os fluxos de dados intra-africanos. As principais recomendações gerais de alto nível são aqui delineadas. Recomenda-se que os Estados-Membros:

- em cooperação, permitam os fluxos de dados no continente, salvaguardando os direitos humanos, a proteção de dados, mantendo a segurança e assegurando a partilha equitativa dos benefícios;

- cooperem para criar as capacidades necessárias para aproveitar as tecnologias e serviços dependentes de dados, incluindo a capacidade de governar os dados para que estes beneficiem os países e cidadãos africanos e permitam o desenvolvimento;
- promovam uma política de dados transversal e uma regulamentação ágil para navegar na emergência de novos modelos de negócios dinâmicos orientados para os dados que possam fomentar o comércio digital intra-africano e o empreendedorismo com base em dados;
- criem quadros co jurisdicionais para a coordenação da concorrência autónoma, do sector e dos reguladores de dados para regular eficazmente a economia da sociedade de dados, formular, implementar e rever a política de dados de uma forma dinâmica, prospetiva e experimental;
- elaborem legislação nacional sobre proteção de dados pessoais e regulamentos adequados, particularmente em torno da governação de dados e plataformas digitais, para assegurar que a confiança seja preservada no ambiente digital;
- instituam ou mantenham autoridades de proteção de dados (APD) independentes, bem-dotadas e eficazes, reforcem a cooperação com as APDs dos membros da União Africana e criem mecanismos a nível continental para desenvolver e partilhar práticas regulamentares e apoiar o desenvolvimento institucional para assegurar um elevado nível de proteção dos dados pessoais;
- promovam a interoperacionalidade, a partilha de dados e a capacidade de resposta à procura de dados através da definição de normas de dados abertos na produção de dados em conformidade com os princípios gerais de anonimato, privacidade, segurança e quaisquer considerações sobre dados específicos do sector para facilitar a acessibilidade de dados não pessoais e certas categorias de dados pessoais a investigadores, inovadores e empresários africanos;
- promovam a portabilidade dos dados para que os sujeitos dos dados não fiquem presos a um único fornecedor e, desta forma, promovam a concorrência, a escolha do consumidor e permitam aos cibernautas deslocarem-se entre plataformas;
- melhorem as infraestruturas que estão desenvolvidas de forma desigual em todo o continente, aproveitando os esforços regionais das CER existentes para apoiar uma cobertura de rede de banda larga eficiente, um fornecimento de energia fiável e infraestruturas e sistemas (de dados) digitais fundacionais (IDE) (identidade digital (Digital ID)), pagamentos interoperáveis de confiança, infraestruturas de nuvem e de dados e sistemas abertos de partilha de dados, para o comércio digital transfronteiriço e o comércio eletrónico;
- estabeleçam um sistema nacional integrado de dados para permitir a criação de valor público e privado, operando com base em quadros de governação harmonizados que facilitem o fluxo de dados necessários para uma economia de dados vibrante, mas com salvaguardas suficientes para ser confiável, seguro e protegido;
- governem o sistema nacional integrado de dados de acordo com os princípios de acesso, disponibilidade, abertura (onde o anonimato pode ser preservado), interoperabilidade, segurança, qualidade, integridade;
- integrem códigos ou diretrizes de dados específicos do sector e peritos em regimes nacionais e continentais de gestão de dados;

- os que ainda não ratificaram a Convenção da UA sobre Segurança Cibernética e Proteção de Dados Pessoais o façam o mais rapidamente possível, como etapa fundamental para a harmonização do processamento de dados;
- forneçam orientações para promover o acesso aos dados para apoiar a inovação local, o empreendedorismo e os objetivos pró-concorrenciais nas próximas negociações sobre os protocolos relativos ao comércio de serviços e ao comércio eletrónico, bem como sobre os protocolos relativos à concorrência e à propriedade intelectual, na zona de comércio livre continental africana.;
- deem prioridade a parcerias politicamente neutras que tenham em conta a soberania individual e a propriedade nacional para evitar interferências estrangeiras que possam afetar negativamente a segurança nacional, os interesses económicos e a evolução digital dos Estados-membros da UA; e
- promovam a investigação, o desenvolvimento e a inovação em várias áreas baseadas em dados, incluindo, as Análises de macrodados, a Inteligência Artificial, a Computação Quântica, bem como o Blockchain.

Recomenda-se ainda que a Comissão da União Africana, as CER e as Instituições Regionais:

- facilitem a colaboração entre as várias entidades que lidam com dados em todo o continente através do estabelecimento de um quadro de consulta no seio da comunidade do ecossistema digital para salvaguardar os interesses de cada ator;
- promovam e facilitem os fluxos de dados dentro e entre os Estados-membros da UA, desenvolvendo um Mecanismo de Fluxos de Dados Transfronteiriços que tenha em conta os diferentes níveis de prontidão digital, maturidade dos dados, bem como os ambientes legais e regulamentares;
- facilitem a circulação de dados através de sectores e fronteiras, desenvolvendo um Quadro Comum de Categorização e Partilha de Dados que tenha em conta os amplos tipos de dados e os níveis associados de privacidade e segurança;
- trabalhem em estreita colaboração com as autoridades nacionais responsáveis pela proteção de dados pessoais dos membros da UA, com o apoio da Rede Africana de Autoridades (RAPDP), para estabelecer um mecanismo e um órgão de coordenação que supervisione a transferência de dados pessoais dentro do continente e assegure o cumprimento dos regulamentos existentes que regem a segurança de dados e informações a nível nacional;
- criem ou confiram poderes a um mecanismo no seio da União Africana para centralizar e conferir poderes aos compromissos regionais relativos às normas de dados;
- criem mecanismos e instituições, ou habilitem os já existentes, no âmbito da União Africana para reforçar as capacidades e prestar assistência técnica aos Estados-membros da UA para a aplicação interna deste quadro da política de dados;
- apoiem o desenvolvimento de infraestruturas de dados regionais e continentais para albergar tecnologias avançadas orientadas para os dados (tais como os macrodados, a Aprendizagem Automática e a Inteligência Artificial) e o necessário ambiente facilitador e mecanismo de partilha de dados para assegurar a circulação através do continente;

- trabalhem para construir um espaço cibernético seguro e resiliente no continente que ofereça novas oportunidades económicas através do desenvolvimento de uma Estratégia de Segurança Cibernética da UA e do estabelecimento de Centros Operacionais de Segurança Cibernética para mitigar riscos e ameaças relacionadas com ciberataques, violações de dados e a utilização indevida de informação sensível;
- permitam a partilha de dados e uma maior interoperacionalidade entre os Estados-membros da UA e outros mecanismos da UA, incluindo o Mecanismo de Cooperação Policial da União Africana (AFRIPOL);
- criem um Fórum Anual de Inovação de Dados para África para sensibilizar os decisores políticos sobre o poder dos dados como um fator impulsionador de uma economia e sociedade digitais, de modo a facilitar os intercâmbios entre países e permitir a partilha de conhecimentos sobre a criação de valor e a inovação baseada em dados e as implicações da utilização dos dados na privacidade e segurança das pessoas;
- reforcem as ligações com outras regiões e coordenem as posições comuns africanas sobre as negociações internacionais relacionadas com dados para assegurar a igualdade de oportunidades na economia digital global;
- elaborem um plano de implementação que tenha em consideração a soberania digital dos Estados, bem como os diferentes níveis de desenvolvimento, a vulnerabilidade das populações e a digitalização nos Estados-membros da UA, nomeadamente aspetos relacionados com a lacuna das infraestruturas das TIC e a falta de políticas e legislações em matéria de segurança cibernética.

1. INTRODUÇÃO

Os dados estão no centro da transformação digital que está a ocorrer a um ritmo e a uma escala sem precedentes em todo o mundo. A utilização de tecnologias baseadas em dados para transformar a maioria dos aspetos da nossa vida quotidiana e do nosso trabalho em dados quantificáveis que possam ser rastreados, monitorizados, analisados e monetizados tornou-se um fenómeno tal que o termo "dataficação" foi criado para o descrever.

Estes processos – que se aceleraram durante o que foi referido como a primeira "pandemia de dados" – podem transformar organizações públicas e privadas em empresas baseadas em dados, melhorando os fluxos de informação e a eficiência, e criando economias mais competitivas. A melhoria dos fluxos de informação nas condições certas pode também reduzir as assimetrias de informação entre governos e cidadãos, reforçando, em última análise, a boa governação.

Alguns desses processos têm sido incrementais e alguns disruptivos, mas todos têm sido altamente irregulares. A utilização de dados é um dos fatores-chave para acelerar a realização da Agenda 2063 e dos Objetivos de Desenvolvimento Sustentável (ODS), uma vez que a falta de dados de qualidade é um dos principais obstáculos à avaliação dos progressos realizados na consecução dos objetivos subjacentes. Especificamente, sistemas de dados integrados melhorados contribuem diretamente para a realização de vários dos objetivos, tais como a melhoria dos sistemas de saúde, identidade e educação, mas sem uma intervenção política direta, a atual distribuição desigual das oportunidades e danos resultantes da dataficação entre países e dentro dos mesmos será exacerbada.

Se os Estados africanos podem criar as condições para o aproveitamento destes processos de digitalização e publicação de dados para criar valor acrescentado, aumentar a eficiência e a produtividade, melhorar os serviços sociais e criar novas formas de trabalho, dependerá das políticas adotadas e implementadas. Isto exige uma resposta africana colaborativa.

A maximização dos benefícios de uma economia baseada em dados e a minimização dos riscos estão altamente dependentes de quadros políticos e regulamentares que aumentem a legitimidade e a confiança pública na gestão de dados. Uma infraestrutura de dados que permita um sistema de dados integrado é um bem estratégico fundamental para os países, mas a escala, extensão e velocidade da mudança provocada pelas tecnologias digitais baseadas em dados tornam a regulamentação complexa e intensiva em recursos. À medida que as novas tecnologias se tornam mais importantes para a economia de dados, a diversidade das partes interessadas e a multiplicidade de plataformas envolvidas na sua regulamentação também aumentam drasticamente, tornando cada vez mais difícil aos decisores políticos permanecerem envolvidos e informados (Banco Africano de Desenvolvimento, 2019). As novas tecnologias avançadas como a IA são suscetíveis de desafiar cada vez mais a eficiência das abordagens legislativas tradicionalmente díspares na elaboração das leis.

Os dados são de natureza global, o que significa que, por um lado, os regulamentos têm implicações transfronteiriças, e que, por outro lado, a precedência regulamentar é mais frequentemente estabelecida pelos países desenvolvidos, ricos em dados e com grande volume de dados. A pressão do mercado é também imposta por empresas de oligopólio, nomeadamente Google, Apple, Facebook, Amazon e Microsoft (ou GAFAM). A natureza dos dados permite a estas empresas que negoceiam em mercados digitais globais de dados aproveitarem a sua vantagem competitiva em dados e algoritmos em todo o mundo. Isto

acaba por afetar a concorrência local e inibir a competitividade global dos participantes da economia de dados nacionais. Existem, portanto, questões de propriedade intelectual e acesso aos dados, comércio justo, concorrência e direitos dos consumidores que têm impacto na política de dados num contexto global e suscitam a necessidade de uma governação e colaboração globais.

Estes fatores também sublinham que muito do que impulsiona o desenvolvimento da economia de dados local, tem estado fora do controlo dos intervenientes africanos, que têm sido, em grande parte, "seguidores de normas" na governança global. Também sublinham a necessidade de colaboração e parcerias em muitos ecossistemas de dados africanos, independentemente da maturidade digital e das dotações económicas mais amplas.

Este quadro político apresenta, portanto, oportunidades para os países assegurarem que as leis permitam proactivamente o acesso aos dados para fins de desenvolvimento, inovadores e competitivos. Ao mesmo tempo, demonstra a necessidade de estes estarem em harmonia uns com os outros para criar a escala e o alcance no mercado necessários à criação de valor e inovação baseadas em dados que podem catalisar o mercado digital único previsto na Estratégia de Transformação Digital da União Africana.

2. MANDATO

O papel central dos dados **requer uma perspetiva política estratégica e de alto nível que esteja fortemente enraizada no contexto local** e possa equilibrar vários objetivos políticos. Estratégias de dados nacionais e abordagens interoperacionais internacionais podem ajudar a libertar o potencial económico e social dos dados, prevenindo simultaneamente danos e atenuando os riscos (OCDE, 2019).

Este quadro da política de dados decorre da Estratégia de Transformação Digital (DTS) adotada pela União Africana em 2020 para transformar as sociedades e economias africanas de forma a permitir que o continente e os seus Estados-membros aproveitem as tecnologias digitais para a inovação local que irá melhorar as oportunidades de vida, reduzir a pobreza e a desigualdade através da facilitação da entrega de bens e serviços.[1] A realização dos objetivos da DTS é fundamental para a concretização da Agenda 2063 da União Africana, o quadro estratégico pan-africano para a unidade, autodeterminação, liberdade, progresso e prosperidade coletiva, e para a realização dos Objetivos de Desenvolvimento Sustentável das Nações Unidas.

O Quadro da Política de Dados baseia-se em instrumentos e iniciativas existentes tais como a Estratégia de Transformação Digital para África 2020-2030 (DTS), o Acordo da Zona de Comércio Livre Continental Africana (ZCLCA), a Iniciativa Política e Regulamentar para a África Digital (PRIDA), o Programa para o Desenvolvimento de Infraestruturas em África (PIDA), a Visão de Smart Africa para Transformar o continente africano num Mercado Único Digital até 2030, a Livre Circulação de Pessoas (FMP), o Mercado Único Africano de Transportes Aéreos (SAATM), O Mercado Único da Eletricidade em África, o Quadro de Interoperabilidade sobre a Identificação Digital, a Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais (Convenção de Malabo), a Declaração sobre Governação da Internet e Desenvolvimento da Economia Digital Africana de 2018, as Diretrizes para a Proteção de Dados Pessoais em África, as leis-modelo regionais sobre proteção de dados e segurança cibernética e a Carta dos Direitos Humanos e dos Povos da União Africana.

Este Quadro de Política de Dados estabelece uma visão comum, princípios, prioridades estratégicas e recomendações fundamentais para orientar os Estados-membros da União Africana no desenvolvimento dos seus sistemas e capacidades nacionais de dados, de modo a obterem valor efetivo dos dados que estão a ser gerados pelos cidadãos, entidades governamentais e indústrias. O potencial das soluções baseadas em dados para ultrapassar a maioria dos desafios de desenvolvimento de África é possível se os Estados-Membros adotarem uma estratégia comum em matéria de dados, apoiada por uma abordagem de governação coerente. Além disso, o desenvolvimento de sistemas de dados integrados é fundamental para otimizar os fluxos de informação e os ganhos de produtividade da digitalização e da datificação.

Este Quadro de Política de Dados visa reforçar e harmonizar os quadros de governação de dados em África e assim criar um espaço de dados partilhados e normas que regulem a intensificação da produção e utilização de dados em todo o continente. Isto deve passar

1 O Conselho Executivo na sua 30ª Sessão Ordinária realizada em 6-7 de fevereiro de 2020 aprovou a Estratégia de Transformação Digital para África (2020-2030), referida na decisão [EX.CL/Dec.1074 (XXXVI)], como o plano diretor que orientará a Agenda de Desenvolvimento Digital do continente, tendo os Dados como um dos seus temas transversais e como um alicerce para o estabelecimento da economia e sociedade digital de África. Para permitir a criação da economia e sociedade digital de África, o Conselho Executivo adotou ainda uma decisão [EX.CL/1180(XXXVI)] relacionada com o desenvolvimento de um quadro continental sobre política de dados e a sua apresentação ao CTE-CICT 4 em 2021 para apreciação e aprovação.

pela criação de um ambiente digital seguro e digno de confiança para impulsionar o desenvolvimento de uma economia digital inclusiva e sustentável que fomente o Comércio Digital Intra-africano, em conformidade com as iniciativas de integração económica regional em curso no âmbito da ZCLCA.

CASO DE UTILIZAÇÃO DE DADOS PARA CRIAÇÃO DE VALOR

Os desertos de dados em muitos países africanos reflectem a fratura digital, uma vez que muitas pessoas não têm acesso aos serviços e sistemas utilizados para gerar os dados necessários para formar algoritmos ou efetuar análises para a tomada de decisões. Os conjuntos de dados gerados pelos utilizadores, tais como as atualizações das redes sociais e os registos detalhados de chamada (CDR), são uma parte importante da revolução dos dados, desde que sejam recolhidos de forma responsável. Estes conjuntos de dados podem ser combinados e reestruturados com outros dados, tais como dados anónimos dos cidadãos para refletir as experiências vividas de milhões de indivíduos e fornecer informações valiosas sobre muitas comunidades vulneráveis diferentes que podem informar a elaboração de políticas, melhorar as intervenções e estimular a atividade económica em vários casos de utilização. Por exemplo, no Senegal foram utilizados macrodados para mapear CDR, mobilidade e atividade económica. No Quénia, os grandes volumes de dados sobre as transações de dinheiro móvel M-Pesa têm sido utilizados para criar produtos de crédito e poupança para os assinantes e perfis de crédito para os pequenos agricultores para empréstimos de insumos e colheitas, um sector da economia que geralmente não tem acesso a instalações bancárias formais.[2]

2.1 VISÃO

O Quadro da Política de Dados prevê o potencial transformador dos dados para capacitar os países africanos, melhorar a vida das pessoas, salvaguardar os interesses coletivos, proteger os direitos (digitais) e impulsionar o desenvolvimento socioeconómico equitativo.

Na prática, o processo visa traduzir esta visão num quadro que, uma vez implementado, permitirá :

Capacitar os africanos a exercerem os seus direitos através da promoção de sistemas de dados fiáveis, seguros e integrados com base em normas e práticas comuns;

Criar, coordenar e capacitar instituições de governação para regular, conforme necessário, o panorama dos dados em evolução e aumentar a utilização produtiva e inovadora dos dados para fornecer soluções e criar novas oportunidades, atenuando simultanea-mente os riscos;

Garantir que os dados possam fluir através das fronteiras o mais livremente possível, conseguindo ao mesmo tempo uma distribuição equitativa dos benefícios e uma abordagem dos direitos humanos e dos riscos para a segurança nacional.

2 *https://www.developlocal.org/the-big-data-in-africa-report/*

2.2 ÂMBITO E OBJECTIVOS

Tendo em conta que os dados estão agora presentes em todos os aspetos da nossa vida quotidiana, mas em circunstâncias muito diferentes em todo o continente, o **quadro fornece orientações baseadas em princípios** aos Estados-membros para a sua apropriação da política de dados continental em função das suas condições e propõe um instrumento ou mecanismo continental para integrar e coordenar os esforços continentais. O Quadro Africano para a Política de Dados visa **reforçar os sistemas nacionais de dados** para uma utilização eficaz dos dados, criando um ambiente favorável que estimule a inovação e o empreendedorismo para impulsionar o desenvolvimento de economias baseadas no valor dos **dados e que facilite a interoperabilidade dos sistemas e dos fluxos de dados transfronteiriços necessários à realização do mercado digital único africano**. A criação de tal ambiente, harmonizado em todos os mercados africanos, proporciona a segurança regulamentar e a escala e o âmbito conducentes aos investimentos necessários para a criação de valor público e privado baseado em dados, com os impactos distributivos e multiplicadores não económicos associados.

No que diz respeito ao âmbito do quadro, é importante ter em mente que a política se preocupa com a **governação de dados que inclui dados pessoais, não pessoais, industriais e públicos**, e não apenas com a proteção de dados pessoais que tem estado no centro das atenções a nível internacional e no continente nos últimos anos.

Os objetivos específicos e abrangentes do Quadro Africano de Política de Dados são os seguintes:

- permitir que os Estados cooperem em matéria de governação dos dados para alcançar objetivos comuns relacionados com o desenvolvimento sustentável das suas economias e sociedades;
- informar e apoiar a domesticação da política continental por parte dos países africanos;
- garantir que os dados possam fluir através das fronteiras o mais livremente possível, promovendo simultaneamente uma distribuição equitativa dos benefícios e abordando os riscos relacionados com violações dos direitos humanos e outros interesses legítimos dos Estados como o combate ao branqueamento de capitais, à evasão fiscal e aos jogos de azar em linha, e a preservação da segurança nacional;
- promover e facilitar os fluxos de dados transfronteiriços e aumentar as oportunidades de negócio, assegurando simultaneamente um nível adequado de dados pessoais e privacidade;
- Estabelecer mecanismos de confiança colaborativos que permitam a circulação dos dados o mais livremente possível entre os Estados-membros, preservando simultaneamente a soberania dos Estados-membros e a sua capacidade de regular a economia digital;
- permitir que os Estados, o sector privado, a sociedade civil e as organizações intergovernamentais coordenem os seus esforços em matéria de dados em todo o continente para realizar um mercado único digital e competir de forma mais eficaz na economia global;
- permitir a competitividade na economia global através de uma cooperação estreita e sustentável por parte dos governos africanos, do sector privado e da sociedade civil, através de oportunidades de reestruturação para otimizar os benefícios da dataficação da economia e da sociedade;

- garantir que os dados sejam utilizados de forma sustentável, que beneficie a sociedade no seu conjunto e não prejudique a privacidade, a dignidade e a segurança das pessoas;
- garantir que os dados estão amplamente disponíveis no âmbito de salvaguardas adequadas para a sua utilização comercial e não comercial; e
- facilitar formas inovadoras de promover os benefícios públicos através da utilização de dados de novas formas que permitam uma maior valorização dos dados em África na tomada de decisões, no planeamento, na monitorização e na avaliação do sector público.

Para permitir à política de dados continental cumprir os seus objetivos previstos e refletir os interesses de todas as partes interessadas, **a formulação do quadro político é fundamentada por iniciativas e documentos anteriores**, tanto do continente africano como de outras regiões do mundo. O processo incluiu uma consulta pública aberta. Os contributos obtidos através desta consulta em linha e de um webinar público contribuíram para o desenvolvimento do projeto de quadro político.

A CUA coordenou o desenvolvimento do Quadro da Política de Dados da UA em colaboração com organizações pan-africanas e agências e instituições especializadas da UA, nomeadamente: as Comunidades Económicas Regionais, a AUDA-NEPAD, o Secretariado da Smart Africa, o Banco Africano de Desenvolvimento, a União Africana das Telecomunicações (ATU), a Comissão Económica das Nações Unidas para África, a União Internacional das Telecomunicações (UIT), a Conferência das Nações Unidas sobre Comércio e Desenvolvimento (CNUCED) e o Banco Mundial bem como outras instituições parceiras.

Quadro da Política de Dados

Formulação	Nacionalização	Monitorização e Avaliação
Identificação dos princípios de alto nível dos desafios da política e das recomendações e ações	Implementação de ações (sistemas de dados integrados nacionais) Estratégias para a criação progressiva das condições de habilitação	Indicadores Metas Medição
Iniciativas, Mecanismos, Instrumentos Continentais		
Governação Global		

3. A ASCENSÃO DA ECONOMIA DE DADOS – NECESSIDADE DE REPENSAR A POLÍTICA

É necessária uma mudança na abordagem à regulação de dados para que os países beneficiem adequadamente da economia global de dados emergente. Esta mudança fundamenta o presente quadro. Os elementos fundamentais desta abordagem integrada para a formulação de políticas de dados são descritos abaixo.

3.1. DADOS COMO BASE PARA UM NOVO CONTRATO SOCIAL E UMA ECONOMIA DA INOVAÇÃO

Os dados, por si só, têm pouco valor, e é apenas através do seu processamento, transmissão, armazenamento e combinação que o valor é acrescentado. Em termos económicos, os dados podem ser entendidos como um bem público na medida em que são inerentemente não rivais (a nível técnico, são infinitamente utilizáveis sem diminuir a capacidade de outra pessoa de os utilizar). São naturalmente não excludentes, o que significa que não existem barreiras naturais à utilização simultânea dos mesmos dados por várias pessoas. Embora existam tentativas de tornar os dados excludentes através de meios tecnológicos e por vezes legais, estas não são características inerentes aos dados. As tentativas de limitar o acesso, para fins de comercialização ou segurança, podem ser regulamentadas de modo a garantir a não-exclusão. Por exemplo, os dados abertos ao abrigo de uma licença reconhecida internacionalmente ou as estatísticas públicas podem ser regulados para serem acessíveis como a radiodifusão pública gratuita, enquanto bem público clássico.

Os dados também não geram valor automaticamente. Em vez disso, existem diferentes utilizações de dados e diferentes métodos para medir o valor económico e social dos fluxos de dados (OCDE, 2019). No sentido económico, é o que as empresas fazem que conduz à criação de valor, tanto internamente na empresa como externamente, através da rede de dados alargada. Teoricamente, este valor pode ser quantificado através da atribuição de valor monetário tendo em consideração as variáveis geradoras de custos e rendimentos, tais como a forma como as organizações cobram pelos dados gerados pelos utilizadores, ou a reconciliação dos custos de gestão de dados, tais como a recolha, manutenção e publicação de dados. A valorização dos dados a partir de uma perspetiva de benefícios socioeconómicos – ou valor de dados não baseados no mercado – surge quando existem condições fundamentais ou fatores que permitem que os governos forneçam serviços públicos mais eficientes e ofereçam uma gestão ambiental eficaz, e quando os cidadãos vivem vidas mais saudáveis e economicamente seguras através da influência dos dados (Banco Mundial, 2021). Um exemplo de criação de valor a partir de dados públicos, inclui o uso de dados para fundamentar as necessidades de alocação dos recursos a fim de melhorar a prestação de serviços.

Estas características dos dados foram enquadradas em outros lugares como **o potencial dos dados para fornecer a base de um novo contrato social** (Banco Mundial, 2021). A formulação de orientações políticas a partir desta abordagem enfatiza a necessidade de dados abertos, normas de interoperacionalidade e iniciativas de partilha de dados para aproveitar o potencial dos dados para impulsionar o desenvolvimento; assegurar uma melhor distribuição dos benefícios dos dados; fomentar a confiança através de salvaguardas que protejam as pessoas

dos danos da má utilização dos dados; criar e manter um sistema nacional integrado de dados que permita os fluxos de dados entre um vasto leque de utilizadores de uma forma que facilite a utilização e reutilização seguras dos dados.

A confiança é fundamental para um ambiente de dados robusto e próspero. A confiança é frequentemente equiparada no contexto da governação digital à segurança técnica e à confiança no sistema técnico que permite o funcionamento do comércio eletrónico. Embora a segurança técnica possa ser uma condição necessária para a confiança, não é suficiente. Em vez disso, a criação de confiança permeia todo o ecossistema de dados, desde a formulação centrada nas pessoas de políticas e regulamentos que preservam os direitos, até garantir o acesso e a utilização de dados para permitir uma inclusão mais equitativa na economia de dados.

Embora os danos associados à concentração de dados e informações e às assimetrias de poder sejam universais, os impactos são desiguais, tanto entre como dentro dos países. A criação de políticas que atenuem o risco diferencial para diferentes categorias de pessoas, como crianças, ou categorias de dados em diferentes sectores, como os dados de saúde, ou a garantia de que a crescente centralidade dos dados não perpetua as injustiças históricas e as desigualdades estruturais exigirá uma regulamentação muito mais granular e adaptável. Embora um quadro de política de dados que preserve os direitos seja essencial, as noções individualizadas de privacidade, liberdade de expressão e acesso à informação (direitos de primeira geração) nos atuais quadros normativos de proteção de dados não serão suficientes para garantir resultados mais justos e equitativos. Os direitos sociais e económicos de segunda geração também são relevantes para várias áreas de governação de dados em relação à disponibilidade, acessibilidade, usabilidade e integridade dos dados que requerem a governação de dados para influenciar a inclusão equitativa. Isto sublinha a necessidade de ir além apenas da regulamentação negativa de conformidade para uma regulamentação positiva que permita criar um ambiente para os Estados e cidadãos africanos participarem eficazmente na economia digital. A criação de condições que permitam o acesso necessário aos dados, salvaguardando ao mesmo tempo os direitos, exigirá a criação de capacidades institucionais no seio do Estado e a capacidade de regulamentar de forma ágil para aproveitar o potencial dos dados para resolver alguns dos problemas mais difíceis do continente.

Para isso, **os decisores políticos precisam de equilibrar algumas das tensões na valorização dos dados para otimizá-los para estes fins**. A transformação dos dados em informações úteis para orientar a tomada de decisões gira em torno da cadeia de valor dos dados, onde as empresas e determinadas entidades públicas estão adequadamente equipadas com quadros potenciadores para apoiar um ecossistema de dados coerente. A geração de valor a partir dos dados pode melhorar os interesses privados, como melhorar a eficiência operacional da empresa, aumentar a sua base de clientes e criar produtos e serviços inovadores que beneficiem atividades comerciais e pessoas com dados pessoais. Para os governos, o valor público dos dados é conseguido assegurando que os benefícios socioeconómicos dos dados se concretizem para permitir a realização de objetivos socioeconómicos mais amplos. Embora a avaliação de dados públicos e privados tenha intenções e resultados diferentes, não se excluem mutuamente. Com efeito, o valor de mercado e o valor não mercantil não devem ser correlacionados com o sector privado e o sector público. O valor não mercantil também pode estar ligado à investigação ou à sociedade civil. O sector público também pode criar valor de mercado abrindo determinados conjuntos de dados e estabelecendo novos fluxos de receitas. Há igualmente interações inovadoras entre atores públicos e privados que podem melhorar o ecossistema global de dados para satisfazer as necessidades de desenvolvimento socioeconómico e de bem-estar.

Com a crescente complexidade e adaptabilidade do sistema global de comunicações, tanto as formas mais recentes como as mais tradicionais de governação estão indiscutivelmente a revelar-se incapazes de fornecer ferramentas adequadas para a governação de bens públicos globais, tais como dados. Do ponto de vista político, há uma crescente distinção entre a criação de valor a partir dos dados e as características de extração de valor dos atuais modelos industriais e de comportamento industrial e de modelos de negócios com uso intensivo de dados e orientados para plataformas (Mazzucato et al., 2020). Tem havido pouca restrição, quer da concorrência quer dos reguladores de dados, na ascensão de plataformas globais monopolistas que produzem e extraem grandes quantidades de dados privados, que foi modificada com aparentemente pouco respeito pelas implicações sociais e negativas para os titulares dos dados pessoais (Zuboff, 2018). Isto pode exigir respostas regulamentares específicas e transversais, a fim de preservar as obrigações positivas da governação dos dados.

3.2 NECESSIDADE DE UMA GOVERNAÇÃO DOS DADOS – CRIAR VALOR, PREVENIR DANOS

A governação dos dados a um nível macro surge como uma oportunidade para utilizar padrões, regras, normas e princípios como mecanismos tanto para atenuar os riscos e danos de dados identificados, como para promover o desenvolvimento da economia de dados e os dividendos digitais.

Por conseguinte, a política de gestão de dados dispõe de alguns mecanismos práticos:

- O alinhamento dos princípios para sublinhar a governação dos dados como uma função normativa;
- A atribuição de funções e responsabilidades para a implementação de políticas a nível macro e micro;
- A identificação e garantia da clareza jurídica e política dos mecanismos de aplicação da governação dos dados;
- A identificação e incentivo da colaboração entre grupos verticais e horizontais de partes interessadas;
- Equilibrar da necessidade de circulação de dados para aumentar a criação de valor com a criação de incentivos económicos para investimentos em infraestruturas e serviços de dados, etc.; e
- O estabelecimento de mecanismos de confiança para apoiar a partilha de dados em termos e condições acordados por todas as partes sobre regras para a utilização de dados e questões de responsabilidade (precisão dos dados, por exemplo).

Essa simplificação da política de governação dos dados deve ser contextualizada dentro dos desafios e oportunidades descritos abaixo. Ao fazê-lo, as prioridades de governação são as seguintes:

Definição de dados – Fornecem especificidade e detalhes sobre os tipos de dados a serem regulamentados e em que medida, para garantir a maximização dos benefícios para diferentes atores na implementação da política de dados. Isto deve ser feito com conhecimento do valor e da natureza dos dados.

Coordenação regional – Fornecer mecanismos e prioridades de coordenação regional para reforçar uma posição regional no âmbito da governação global e fornecer apoio à domesticação regional.

Capacidade institucional interna – Atribuição de obrigações, responsabilidades e poderes aos atores institucionais a nível nacional que podem ajudar a criar um ambiente interno consistente para que as comunidades de dados (públicas e privadas) possam instituir atividades relacionadas com os dados.

Colaboração interna – Garantir o alinhamento de políticas, identificar participantes de várias partes interessadas e promover mecanismos para uma domesticação bem-sucedida.

Apoio político – Fornecer normas e soluções implementáveis que se concentrem na consecução de uma qualidade saudável dos dados nacionais, no controlo, no acesso e na interoperacionalidade, no processamento e na proteção, e na segurança como meio para o crescimento de uma economia de dados.

Clareza – A garantia de clareza, que facilita o cumprimento, não tem restrições involuntárias, mas pode também servir de base para a coordenação transfronteiriça (e entre silos).

4. CONTEXTO

4.1. VISÃO GERAL DAS TENDÊNCIAS DA POLÍTICA REGIONAL INTERNACIONAL E DA LEGISLAÇÃO

Muitas jurisdições em todo o mundo não têm política de dados, com cerca de um terço a não ter legislação de dados em vigor. A CNUCED constatou, em 2020, que 66% dos países do mundo têm algum tipo de legislação, 10% têm projetos de legislação, 19% não têm legislação e 5% não têm dados.

A nível global, vários instrumentos influentes surgiram neste contexto, sendo o RGPD 2016/679 da UE, possivelmente, o mais influente. Outros instrumentos regionais incluem o Quadro de Privacidade da APEC e o Acordo de Parceria Trans-Pacífica (PTP). Estes acordos adotam abordagens ligeiramente diferentes para a proteção de dados e podem servir como pontos de referência úteis para os esforços concertados da África na proteção dos dados.

O RGPD 2016/6 da UE é muito abrangente, com uma definição alargada do que são os dados pessoais. O seu vasto âmbito territorial aplica-se dentro e fora da UE, prevê sanções graves para quem subverter o regulamento, exige uma abertura e transparência consideráveis e, o mais importante, concede aos indivíduos direitos substanciais que podem ser aplicados contra as empresas. Esta abordagem à proteção de dados está centrada em torno de uma agenda de direitos hu manos no ecossistema digital.

O Quadro de Privacidade da APEC, aplicado desde 2005 pelos Estados-membros da APEC, é constituído por um conjunto de princípios, criados para garantir o livre fluxo de informações em apoio do desenvolvimento económico. O quadro da APEC adota uma abordagem diferente à proteção de dados, alinhando o mandato do quadro com a promoção do comércio e do investimento. Um destaque importante do quadro é a forma como sublinha que a regulamentação da privacidade deve ter em consideração a importância dos interesses empresariais e comerciais, para além das culturas e outras diversidades das economias dos Estados-membros.

O Acordo Abrangente e Progressivo para a Parceria Transpacífica (CPTPP) centra-se no comércio aberto e na integração regional entre os Estados-membros. O acordo permite a transferência transfronteiriça de informações por meios eletrónicos, incluindo informações pessoais, quando esta atividade é "para a realização de atividades", mas os países podem exigir a proteção dos dados que são transferidos.

Fora destes acordos multilaterais, os objetivos públicos de proteção de dados centram-se mais tipicamente na proteção da privacidade dos indivíduos e comunidades; na salvaguarda de dados valiosos contra fugas, perda e roubo; e na manutenção e aumento da confiança do público, dos investidores e dos clientes. Numa tentativa de alcançar estes objetivos, muitos países incluíram nas suas leis internas barreiras potenciais ao fluxo de dados, tais como requisitos de localização de dados e, em alguns casos, requisitos mais rigorosos de processamento e recolha de dados. Estes podem atrasar ou contrariar inadvertidamente os objetos de enquadramentos políticos regionais mais abrangentes.

Na evolução das políticas nacionais para a economia digital, cristalizaram-se várias estratégias globalmente, tais como a abordagem liderada pelo governo (como defendida pela UE), a abordagem liderada pelo sector privado (como promovida nos Estados Unidos), a abordagem política descendente (exemplificada por Singapura), e a abordagem ascendente (por exemplo, em Hong Kong). Essas abordagens têm efeitos complementares variáveis na implementação, implantação, impactos, inovação, agilidade e estabilidade das políticas.

4.2 POLÍTICA AFRICANA E CONTEXTO LEGISLATIVO

De acordo com os precedentes internacionais, a maioria dos esforços na regulamentação de dados no continente tem-se concentrado na proteção de dados, com o principal objetivo de observar e salvaguardar os direitos de privacidade dos utilizadores da Internet. Embora a utilização e o processamento de dados sejam uma preocupação transversal, que tem impacto numa série de áreas de política tradicionalmente em silos, não existem exemplos de leis-quadro que regulem todos os aspetos dos dados. Em vez disso, os dados foram regulamentados em cinco ramos da lei: a proteção de dados, a concorrência, a segurança cibernética, as comunicações e transações eletrónicas e a propriedade intelectual, que potencialmente entram em conflito nalguns casos e deixam lacunas noutros.[3]

Estima-se que **32 dos 55 países africanos tenham promulgado ou adotado alguma forma de regulamentação com o objetivo principal de proteger os dados pessoais**. Regionalmente, instrumentos legislativos como o Quadro Comunitário das Leis Cibernéticas da África Oriental de 2008, a *Lei Complementar de 2010* relativa à proteção de Dados Pessoais da Comunidade Económica dos Estados da África Ocidental (CEDEAO), e a lei-modelo da Comunidade de Desenvolvimento da África Austral de 2013 que harmonizam as políticas para o mercado das TIC na África Subsariana foram desenvolvidos. A nível continental, a União Africana desenvolveu o primeiro quadro Pan-africano com a Convenção da União Africana sobre Segurança Cibernética e proteção de Dados Pessoais (*Convenção de Malabo*) em 2014, que não entrou em vigor, mas está atualmente a ser ratificada.

As leis e protocolos regionais sobre concorrência nas Comunidades Económicas Regionais (CER) estabelecidas aplicam-se a empresas que processam dados, embora na sua maioria não se refiram explicitamente a dados. Incluem os Regulamentos da Concorrência e as Regras da Concorrência da COMESA de 2004, a Lei da Concorrência da EAC (2006) e o Protocolo do Mercado Comum da EAC e o Protocolo sobre o Estabelecimento de uma União Aduaneira da EAC, a Lei Suplementar da CEDEAO sobre a "Adoção de Regras de Concorrência Comunitárias e as modalidades da sua aplicação na CEDEAO", o Protocolo da SADC sobre o Comércio (2006) e a Declaração da SADC sobre a Cooperação Regional em Políticas de Concorrência e do Consumidor (2009). Abordam as práticas anti-concorrenciais, incluindo o abuso de posição dominante e também a estrutura do mercado através da regulamentação das fusões e aquisições. No entanto, os pormenores e as abordagens diferem, o que coloca desafios às empresas que operam em várias regiões.

3 As dimensões continentais destes desafios são abordadas através da colaboração digital a nível continental.

OUTRAS INICIATIVAS IMPORTANTES NO CONTINENTE EM MATÉRIA DE POLÍTICA DE DADOS

Iniciativa de Política e Regulamentação para a África Digital (PRIDA)[4] : No âmbito da implementação deste projeto, a Comissão da União Africana criou um Grupo de Trabalho de peritos que contribuiu para a identificação dos principais indicadores de harmonização e para o desenvolvimento de um Modelo e Ferramenta de Monitorização e Avaliação (M&A) sobre Proteção e Localização de Dados que está pronto a ser utilizado pelos Estados Membros da UA e pela Organização Regional para avaliar o grau de harmonização e alinhamento das leis e dos regulamentos nacionais.

Smart Africa apoia a criação de um quadro harmonizado para políticas e regulamentação da proteção de dados em África e mecanismos de colaboração e confiança intercontinentais através do Grupo de Trabalho para a Proteção de Dados de Smart Africa. O Grupo de Trabalho irá proceder a um levantamento dos quadros jurídicos, das orientações de implementação para os Estados-membros e das recomendações sobre harmonização e mecanismos de colaboração entre as Autoridades de Proteção de Dados (APD).

4.3 ANÁLISE SITUACIONAL PARA A ECONOMIA DE DADOS EM ÁFRICA

Efetuar uma análise situacional do continente como um todo, com os seus diversos sistemas jurídicos, regulamentares e políticos, e considerar o desenvolvimento económico desigual e a preparação digital dos países é inerentemente limitado e demasiado generalizado. O objetivo da análise SWOT de alto nível é identificar os pontos fortes e fracos amplamente aplicáveis dos países a nível regional e identificar as potenciais oportunidades e riscos conhecidos associados aos processos globais de digitalização e dataficação que caracterizam o desenvolvimento da economia de dados para todos os países, mas também o que estes significam especificamente para os países africanos, dentro do seu contexto de desenvolvimento mais alargado.

4 O PRIDA é uma iniciativa conjunta da União Africana (UA), da União Europeia (UE) e da União Internacional das Telecomunicações (UIT) que visa permitir ao continente africano colher os benefícios da digitalização, abordando várias dimensões da procura e da oferta de banda larga em África e reforçando as capacidades dos intervenientes africanos no espaço da governação da Internet.

PONTOS FORTES	PONTOS FRACOS
• Instrumentos de governação de dados regionais fundacionais. • Comunidades Económicas Regionais (CER) para apoiar os aspetos económicos das iniciativas de política de dados. • Tribunais regionais e continentais para permitir a resolução harmonizada de litígios. • Centros de inovação emergentes na região para demonstrar as melhores práticas em todas as jurisdições. • Poucas leis em matéria de concorrência, dados e propriedade intelectual e menos desenvolvidas no domínio dos dados, o que pode favorecer a harmonização rápida a nível continental das leis que permitem o comércio transfronteiras.	• Conectividade e utilização dos dados subaproveitada. • Regime de governação de dados não harmonizado. • Inconsistências no processamento de dados nas leis de proteção de dados, concorrência e propriedade intelectual nos países. • Regras de localização que limitam os fluxos transfronteiriços de informações necessários à criação de valor local e ao estabelecimento do mercado único. • Restrições de recursos na evolução e implementação de quadros de governação de dados. • Infraestrutura de dados inadequada. • Insuficiência de dados governamentais abertos para satisfazer a procura de dados. • Fornecimento ou acesso inadequado a dados de qualidade. • Desenvolvimento desigual das normas de dados. • Baixa penetração da identificação digital de base. • Número limitado de Autoridades de Proteção de Dados (APD), muitas das quais não dispõem de recursos suficientes e/ou não estão plenamente capacitadas). • Necessidade de capacidades em termos de segurança cibernética.

OPORTUNIDADES	AMEAÇAS/RISCOS
• Se estiverem reunidas as condições prévias e criados ambientes propícios, há oportunidades para a criação de valor a partir dos dados públicos e privados, através da melhoria dos fluxos de informação e de melhor eficiência. • Utilização de dados para melhorar o planeamento público, a prestação de serviços e a coordenação dos sectores público e privado. • A existência de dados abertos e de normas interoperáveis subjacentes a um sistema nacional integrado de dados pode reduzir os obstáculos à entrada no mercado e aumentar as oportunidades de desenvolvimento empresarial e de inovação. • Esforços globais para desenvolver e harmonizar a política de dados e os quadros de governação. • Esforços globais para coordenar a tributação dos serviços digitais e de dados que, em grande parte, não têm contribuído para os esforços de mobilização de recursos nacionais. • Oportunidades de trabalho emergentes para jovens com conhecimentos tecnológicos podem melhorar. • o empreendedorismo local, o desenvolvimento de conteúdos locais e a inovação.	• Incapacidade de alguns países para superar os desafios de criar ambientes favoráveis necessários para a realização das oportunidades. • Falta de harmonização dos quadros políticos e regulamentares de modo a permitir economias de escala e de âmbito para a criação de valor a partir dos dados e para que todos os países possam usufruir dos benefícios de um mercado digital comum. • Riscos relativos à proteção de dados e à privacidade em constante mudança. • Risco de decisões discriminatórias automatizadas (baseadas em algoritmos) resultante da invisibilidade, da sub-representação de categorias de pessoas em conjuntos de dados e de deficiências na modelação de algoritmos. • Concentração nos mercados globais de dados, impedindo a concorrência leal nos mercados locais. • Níveis inadequados de cooperação política internacional para lidar com questões de dados globais - acesso, integridade, segurança, equidade, direitos e ética.

4.4. DESAFIOS POLÍTICOS EMERGENTES NA CONCRETIZAÇÃO DAS OPORTUNIDADES E NA ATENUAÇÃO DOS RISCOS

A distribuição desigual das oportunidades e riscos associados ao desenvolvimento da economia de dados correlaciona-se em grande parte com os níveis de desenvolvimento humano e económico dos países e com as desigualdades entre e dentro dos países. Estes refletem-se nos pontos fortes e fracos acima salientados. A capacidade dos países e das regiões em África para contrariar estas tendências depende da sua **capacidade em criar um ambiente propício à criação de valor a partir dos dados, inclusivo e equitativo**.

O objetivo do Quadro de Política de Dados é fornecer um quadro para os países superarem alguns dos desafios da formulação de políticas nesta área dinâmica e em rápida mudança através de um objetivo comum e de uma ação coletiva. Graças à criação de um ambiente favorável harmonizado, os pontos fortes dos países podem ser aproveitados e os pontos fracos podem ser mitigados para o desenvolvimento de uma economia de dados continental integrada muito mais poderosa do que as suas partes individuais.

Não devem ser subestimados os desafios políticos que têm de ser ultrapassados para criar um ambiente propício à concretização das oportunidades oferecidas pelos processos globalizados de digitalização e de informatização e para atenuar de forma eficaz os riscos identificados para os países no mundo inteiro. Estes desafios são atualmente objeto de vários relatórios de organizações multilaterais (CNUCED 2021, Banco Mundial 2021). Embora alguns dos desafios estejam relacionados com a criação de condições para a criação de valor a partir dos dados a nível nacional que são destacados na análise situacional acima e discutidos abaixo, a natureza internacional e transfronteiriça dos dados como bens públicos globais exige mais do que nunca uma **cooperação regional e global** para que sejam realizados a nível nacional e para mitigar os riscos associados que possam surgir da utilização de dados para além das fronteiras nacionais. Embora o Quadro da Política de Dados forneça um quadro de alto nível para os países desenvolverem políticas nacionais, estas devem basear-se em processos consultivos nacionais que tenham em conta o contexto local, as necessidades e os dotes institucionais dos países.

Ao criar este ambiente propício nos Estados membros da União Africana e na região, são assinaladas as considerações abaixo, decorrentes da análise situacional, que podem afetar a capacidade dos países para responder às necessidades de uma nova economia de dados.

A digitalização e a dataficação atravessam os sectores público e privado, a economia formal e informal e as esferas social e cultural, e requerem uma mudança das políticas sectoriais tradicionais. A política para a economia e sociedade digital e de dados precisa de ser transversal para coordenar atividades em todo o sector público e entre os sectores público e privado para cumprir objetivos nacionais e regionais. Ao mesmo tempo, é importante considerar as **políticas sectoriais específicas em matéria de dados** para otimizar e salvaguardar as diversas utilizações de diferentes tipos de dados (por exemplo, dados de saúde ou dados climáticos). Para além da observação deste princípio, o desenvolvimento efetivo das várias políticas sectoriais que terão de ser desenvolvidas ultrapassa o âmbito deste quadro de alto nível. É essencial uma regulamentação eficaz dos mercados globalizados, que são cada vez mais complexos, para que a estrutura de base ubíqua e os serviços contínuos necessários à implantação de serviços e aplicações de dados satisfaçam as diversas necessidades económicas e sociais, melhorem a concorrência e promovam a inovação africana. Tal como em países de todo o mundo, os

decisores políticos terão de rever e renovar os acordos institucionais para a governação da economia de dados. São necessários reguladores especializados, como os reguladores de dados ou de informação, para lidar com as novas questões da governação dos dados, e tanto os reguladores novos como os já estabelecidos terão de se empenhar em níveis elevados de coordenação nacional e regional. Para assegurar que o mercado único africano se torne operacional, a harmonização regulamentar é também fulcral para a integração dos mercados, juntamente com os sistemas comuns de pagamento online , a facilitação do comércio transfronteiriço e a normalização dos impostos e taxas transfronteiriças. Os Estados africanos precisarão de se reunir e desenvolver posições comuns para assegurar resultados mais favoráveis em fóruns de governação global e assim servir melhor os interesses africanos.

Uma política transversal digital e de dados pode gerir a importante interação entre a concorrência, o comércio e a fiscalidade numa economia de dados. Isto representa uma oportunidade para os Estados africanos coordenarem políticas sectoriais para apoiar uma economia de dados florescente. Em muitos países africanos, um risco que precisa de ser mitigado desde cedo é a tendência para a concentração do mercado e a criação desigual de riqueza devido a efeitos de rede indiretos associados a economias de escala e de gama. Os mercados digitais baseados em dados são propensos a que o "vencedor leva tudo". Entre outros fatores, a hiper-globalização e a interdependência digital contribuem para a monopolização. Em última análise, isto afeta a concorrência local e inibe a competitividade global dos ecossistemas de dados nacionais. Os desafios da concentração do mercado, da interdependência digital e da distribuição desigual da riqueza, nomeadamente devido à erosão da base tributável e à transferência de lucros, criam a possibilidade de incentivos que encorajam uma maior integração entre as prioridades que se reforçam mutuamente para estratégias políticas habitualmente isoladas em matéria de concorrência, comércio e fiscalidade. Devido à importância crescente da governação regional e global, as comunidades económicas regionais têm um papel importante a desempenhar na implementação da política regional de dados através de leis-modelo e no apoio à criação de capacidades institucionais e humanas.

SMART AFRICA – IDENTIDADE DIGITAL

Em 2020, o Benim defendeu um projeto emblemático de Smart Africa para desenvolver o Plano de Identidade Digital, que foi adotado pelo Conselho de Smart Arica, incluindo os seus 32 Estados-membros, a UA e a UIT, com o apoio de uma série de outras organizações multilaterais e doadores. O Projeto em ação propõe a SATA como uma plataforma para facilitar o reconhecimento fiável da identidade digital entre vários atores através de mecanismos federados de certificação. Prevê-se a realização de projetos-piloto da SATA entre o Benim, o Ruanda, a Tunísia, e outros Estados-membros de Smart Africa. A SATA servirá como uma solução ágil e adaptável para permitir a interoperacionalidade entre vários esquemas de identidade públicos e privados no continente.

Considerando o contexto africano específico e o ritmo lento dos esforços de harmonização, a abordagem federada da SATA deverá permitir o reconhecimento unilateral de quadros jurídicos adequados por parte dos Estados africanos, com o apoio de uma autoridade de certificação central e de confiança. Para este fim, os Estados devem reforçar as suas capacidades de aplicação, em particular as capacidades das autoridades de proteção de dados no controlo e aprovação das transferências transfronteiriças de dados. O quadro proposto irá abranger as tecnologias mais avançadas e respeitar as legislações e regulamentos dos países. Os governos não devem ser obrigados a utilizar tecnologias específicas. A utilização de normas e padrões abertos deverá garantir uma grande diversidade de escolhas tecnológicas por parte dos Estados.

No contexto do ecossistema africano de dados, **o alinhamento dos objetivos de política fiscal e de política de dados, particularmente no contexto da viabilização do Mercado Único Digital, tem sido um desafio político incontornável para muitos países**. Medidas legislativas e políticas recentemente introduzidas por países africanos selecionados, no contexto dos vários esforços multilaterais e unilaterais de tributação da economia digital, podem não ser conducentes nem à criação de um mercado único nem ao acesso a recursos internacionais para a concretização de bens públicos a nível mundial e para satisfazer algumas das condições prévias para uma economia de dados competitiva no continente. O aproveitamento de novas fontes de receitas fiscais poderá permitir aos países africanos eliminar os impostos especiais sobre o consumo de redes sociais e serviços de dados, reduzindo distorções tanto no mercado local como no sistema fiscal global. A harmonização do regime fiscal para bens e serviços digitais a nível regional, e o alinhamento a nível global, podem mitigar os riscos associados à incapacidade das pequenas economias de dados de gerarem valor significativo e competirem nos mercados globais. Estas pequenas economias de dados são tipicamente incapazes de contribuir para a escala e o alcance necessários para a criação de valor a partir dos dados e trabalhar com bases fiscais limitadas.

A clareza e a segurança jurídicas em relação às questões emergentes em matéria de dados são necessárias para apoiar uma transformação digital fiável e sustentável. Um desafio global é que a natureza dos fluxos de dados e da infraestrutura digital ameaça a soberania dos dados nacionais. Exercer um controlo sobre os dados para salvaguardar a soberania requer infraestruturas e legislação, mas também a capacidade técnica para o fazer de uma forma que possa criar confiança. As políticas transversais proporcionam uma oportunidade de certeza em questões como a apropriação ou custódia de dados e os direitos conexos, ao mesmo tempo que estabelecem um sistema abrangente de supervisão sobre o acesso, a aquisição, a análise, o armazenamento e a divulgação de dados tanto pessoais como não pessoais. Assegurar a proteção do consumidor, que permite simultaneamente a inovação, é igualmente fundamental para o desenvolvimento económico e a inclusão. Além disso, porque diferentes abordagens jurídicas sectoriais servem interesses diferentes, é dada aos países a oportunidade de reinventar um sistema jurídico harmonizado que equilibre adequadamente os interesses empresariais e os direitos digitais relevantes.

A criação de sistemas de dados nacionais integrados e interoperacionais em resposta aos desafios emergentes aumenta a eficiência e permite uma maior transparência e responsabilidade. Um desafio comum encontrado em todo o mundo é que quando os dados são de má qualidade ou não interoperacionais, limitam a capacidade das empresas e do sector público de se envolverem na partilha e análise que pode fornecer valor económico e social aos dados. As vias de acesso insuficientes e o compromisso limitado de abrir os dados governamentais, entre outros desafios, também impedem um ambiente que fomenta uma forte economia de dados. O forneci mento de bons dados requer a construção de uma procura de dados entre locais institucionais (ou seja, o sector público, instituições e empresas, etc.). A extração de valor dos dados requer não só controlo, mas também o desenvolvimento de uma capacidade analítica e técnica nos sectores públi co, privado e outros.

Apesar de vários países introduzirem sistemas de identificação digital, **os sistemas de identificação digital omnipresentes e interoperacionais continuam a ser um grande desafio socioeconómico no continente**. Os sistemas de identificação digital permitem a identificação para efeitos de transação e interação num ecossistema de dados fiável. A identidade fundacional e funcional facilita os serviços digitais, mas a cobertura completa da identidade fundacional em particular continua a ser um desafio social e económico. Os quadros regionais emergentes sobre identidade digital estão a começar a lidar diretamente com este desafio.

Há oportunidades para que a identidade descentralizada e funcional seja incorporada nos quadros de proteção de dados. Estes podem proporcionar identidade funcional, reduzindo ao mesmo tempo os riscos associados aos dados pessoais.

Outro grande desafio a este respeito é a disparidade entre os dados económicos e sociais e, particularmente, e a falta de indicadores digitais em muitos países, para informar a formulação de políticas baseadas em provas e para fornecer uma imagem precisa às bases de dados públicas globais, tais como no âmbito do sistema estatístico da ONU. Com o reconhecimento do valor estratégico dos dados, é necessário dar prioridade à recolha e armazenamento de dados de qualidade para criar valor público e reduzir a informação existente e as assimetrias de poder associadas dentro do sector público, entre o sector público e privado, e entre os sectores público e privado e os cidadãos e consumidores.

Os países africanos enfrentam vários desafios bem documentados e inter-relacionados no que diz respeito aos seus níveis desiguais de **prontidão digital** (União Internacional das Telecomunicações, 2019; Fórum Económico Mundial, 2016) que têm um impacto variável na sua capacidade de responder aos desafios nacionais e globais. Estes incluem a elaboração pontual de políticas e legislação, desafios em torno da harmonização regional de políticas, a falta de capacidade institucional, a concorrência ineficazmente regulada entre os prestadores de serviços, baixos níveis de cobertura, a falta de acessibilidade e qualidade da conectividade de banda larga (Gillwald & Mothobi, 2019; Hawthorne, 2020).

Apesar da adoção de cartas continentais, convenções e leis-modelo das comunidades económicas regionais que tentam harmonizar a **resposta de África aos desafios colocados pela digitalização e transformação dos processos em dados, a ratificação e implementação das mesmas tem sido variada**. A adoção mais ampla de bases de apoio ao digital para as iniciativas continentais, como a ZCLCA, será essencial para concretizar os benefícios de uma maior cooperação económica. A existência de regras normalizadas para os fluxos transfronteiriços é uma condição prévia para a concretização dos benefícios previstos da ZCLCA. Isso pode passar pela operacionalização do Acordo para facilitar uma melhor interoperacionalidade dos dados transfronteiriços e proporcionar uma abordagem continental harmonizada da economia digital baseada nos dados. Para tal, será necessário promover os benefícios socioeconómicos do comércio digital e do comércio eletrónico, garantindo simultaneamente a segurança das informações sensíveis e o respeito da regulamentação pertinente em matéria de proteção dos dados pessoais.

Em resposta a anteriores ondas de inovação tecnológica, económica, regulamentar e social, **os países africanos tenderam a adotar normas tomadas por outros atores em vez de as criarem**. As organizações multilaterais, desde a OCDE e a Organização Mundial da Propriedade Intelectual à Organização Mundial do Comércio, estão a reagir aos desafios da governação global de dados. Embora África e os países africanos, com algumas exceções, não tenham liderado políticas digitais globais, existe uma oportunidade para alterar esta situação. As pressões comerciais multilaterais, plurilaterais e bilaterais para permitir os fluxos de dados com poucas restrições são acompanhadas de pressões para a concessão de direitos de propriedade intelectual sobre os dados, de modo que os países africanos se veem confrontados com a probabilidade de os seus dados serem explorados e apropriados por outros. Na ausência de uma política comum e de um compromisso com padrões comuns em todo o continente, será difícil para a maioria dos países africanos escapar às correntes de uma dinâmica global em rápida mutação. Por conseguinte, é necessária uma ação coordenada por e para África para desbloquear coletivamente o enorme e transformador potencial dos dados para desenvolver uma economia digital africana inclusiva e sustentável e uma sociedade moderna.

INOVAÇÃO EM CASO DE UTILIZAÇÃO POR COMUNIDADES DE DADOS

Exemplos tipicamente citados de sucesso na inovação a partir dos dados abertos são a emergência de polos de inovação particulares em toda a região, principalmente em zonas urbanas. Os polos de inovação, conforme defendido noutros locais, podem certamente ser um local de sucesso de dados abertos sociais e económicos; no entanto, há exemplos de inovação baseada em dados abertos que podem ocorrer de forma mais orgânica apenas através do fornecimento de dados governamentais abertos de qualidade. Estes podem ser impulsionados pelas necessidades de sectores específicos – por exemplo, na agricultura, iCow foi uma aplicação lançada por um empresário queniano que ajudou a melhorar em 100% os rendimentos do gado bovino para agricultores individuais. Outras inovações na agricultura mais centralmente envolvendo dados abertos incluem, no Gana, Farmerline e Esoko. As empresas inovadoras podem surgir de dados abertos, como os exemplos sul-africanos de OpenUp (Cidade do Cabo) e Open Cities Lab (Durban), que são empresas socialmente focadas, ambas impulsionadas por dados abertos. Ushahidi é uma organização (e uma empresa de software como serviço) centrada em torno de uma plataforma de código aberto, que integra dados abertos de origem pública e os mapeia, e tem sido utilizada para um incrível efeito social e de governação na monitorização de eleições e na resposta a crises em toda a região. Os dados abertos podem ter economias diretas de custos públicos em resultado de inovações que emergem de iniciativas de dados, criando um ciclo virtuoso: numa parceria precoce entre OpenUp (então Code for South Africa) e o Programa da África Austral sobre Acesso a Medicamentos e Diagnósticos, uma ferramenta desenvolvida com base em dados abertos relativos a preços de medicamentos, demonstrou ao governo namibiano as diferenças entre os preços que recebia sobre o medicamento Nifedipina, o que, após renegociação, os levou a uma poupança direta de custos de 1 bilião de USD por ano.

5. QUADRO DA POLÍTICA DE DADOS

Os dados são cada vez mais reconhecidos como um bem estratégico, integrante da elaboração de políticas, da inovação do sector privado e público e da gestão do desempenho, criando novas oportunidades empresariais para empresas e indivíduos. Quando aplicadas aos serviços governamentais, as novas tecnologias podem gerar enormes quantidades de dados digitais e contribuir significativamente para o progresso social e o crescimento económico. O papel central dos dados requer uma perspetiva política estratégica e de alto nível que possa equilibrar vários objetivos políticos. Para estimular o potencial económico e social dos dados, protegendo eficazmente a privacidade, a propriedade intelectual e outros objetivos políticos, devem ser formuladas estratégias nacionais de dados no contexto do reforço da interoperabilidade internacional.

O desenvolvimento de um Quadro da Política de Dados da UA é necessário para realizar a visão partilhada e os princípios comuns de um ecossistema africano integrado de dados. Este ecossistema de dados deve apoiar a criação de um Mercado Único Digital Africano (DSM), fomentar o comércio digital intra-africano, e impulsionar o desenvolvimento do empreendedorismo e das empresas inclusivas e com base em dados. Isto está previsto tanto na Estratégia de Transformação Digital da UA (DTS) como nas próximas negociações das Fases II e III da ZCLCA, onde se prevê a definição de diretrizes sobre o Comércio de Serviços e o Protocolo de Comércio Eletrónico.

O Quadro fornece orientações de alto nível baseadas em princípios aos Estados-membros no seu desenvolvimento de políticas de dados, adequados às condições do país. Identifica os princípios fundamentais de uma governação eficaz dos dados e as estratégias de implementação a nível nacional, continental e internacional. Isto inclui orientações sobre os procedimentos e salvaguardas institucionais, administrativos e técnicos apropriados que devem ser implementados. O objetivo é assegurar que os ecossistemas de dados nacionais e sub-regionais sejam construídos sobre infraestruturas e processos digitais fiáveis e interoperacionais que promovam um sistema de dados continental harmonizado e permita assim um crescimento e desenvolvimento económico equitativo e sustentável para todos os povos de África.

O Quadro reafirma a importância do empenho da UA em quadros regulamentares estáveis, harmonizados e previsíveis e em políticas contextualmente relevantes para facilitar:

- incentivos ao investimento eficiente em infraestruturas de dados digitais fundacionais e sistemas digitais fundacionais;
- acordos institucionais que permitam uma interação ótima entre o Estado, os mercados e as instituições reguladoras, de modo a permitir um valor público e privado;
- a criação de capacidades digitais humanas e institucionais;
- a criação de valor a partir de uma utilização responsável dos dados, promovendo um crescimento equitativo sustentável, e aumentando a prosperidade partilhada a partir da economia de dados;
- uma melhor distribuição das oportunidades tanto para a utilização de serviços de dados como para a produção e criação de valor com base nos dados dentro e entre países; e
- ambientes eficazmente regulados que promovam a concorrência leal e a eficiência na atribuição de recursos que produzem resultados positivos no bem-estar dos consumidores.

5.1. PRINCÍPIOS ORIENTADORES DO QUADRO

O Quadro de Política de Dados deve alinhar-se com o direito internacional e os valores da UA para alcançar uma maior unidade e solidariedade entre os países africanos e os seus povos, assegurando um desenvolvimento económico equilibrado e inclusivo, com a promoção e proteção dos direitos dos povos através da Carta Africana dos Direitos Humanos e dos Povos e outros instrumentos relevantes.

No espírito de fomentar a prosperidade regional, o crescimento económico e o desenvolvimento, e para integrar e coordenar os esforços continentais, os seguintes princípios de alto nível orientam o quadro.

Cooperação: Os Estados-membros da União Africana devem cooperar no intercâmbio de dados, reconhecendo os dados como um contributo central da economia global e a importância da interoperacionalidade dos sistemas de dados para um próspero mercado único digital africano;

Integração: o Quadro promoverá os fluxos de dados intra-africanos, eliminará as barreiras jurídicas aos fluxos de dados, apenas sob reserva da segurança necessária, dos direitos humanos e da proteção de dados;

Equidade e inclusão: na implementação do Quadro, os Estados-membros devem garantir que este seja inclusivo e equitativo, oferecendo oportunidades e benefícios a todos os africanos e, ao fazê-lo, procurar corrigir as desigualdades nacionais e globais, respondendo às vozes das pessoas marginalizadas pelos desenvolvimentos tecnológicos;

Confiança, segurança e responsabilização: Os Estados-membros devem promover ambientes de dados dignos de confiança que sejam seguros e protegidos, responsáveis perante as pessoas em causa, e éticos e seguros por conceção;

Soberania: Os Estados-membros, CUA, CER, as Instituições Africanas e as Organizações Internacionais devem cooperar para criar a capacidade que permita aos países africanos autogerirem os seus dados, tirarem partido dos fluxos de dados e governarem adequadamente os dados;

Abrangente e virado para o futuro: o quadro permitirá a criação de um ambiente que incentive o investimento e a inovação através do desenvolvimento das infraestruturas, da capacidade humana e da harmonização dos regulamentos e da legislação; e

Integridade e justiça: Os Estados-membros devem assegurar que a recolha, o processamento e a utilização dos dados é justa e lícita, e os dados não devem ser utilizados para discriminar injustamente ou infringir os direitos dos povos.

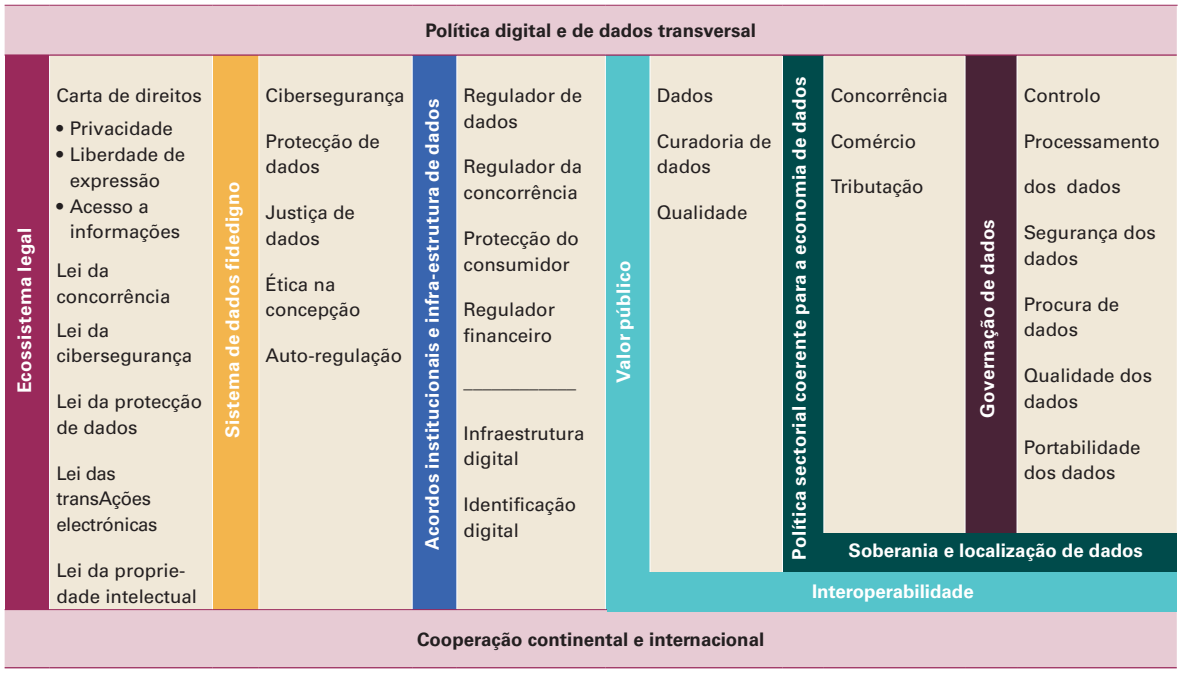
5.2 DEFINIÇÃO E CATEGORIZAÇÃO DE DADOS

Não há acordo sobre como os dados são definidos, provavelmente como resultado dos muitos tipos diferentes de dados recolhidos e usados e seus diferentes propósitos e valores. Sem reconhecer estes diferentes tipos de dados e as várias funções que podem desempenhar, os governos não poderão abordar de forma eficaz questões como a proteção dos dados pessoais ou a concorrência. Uma melhor medição dos dados e fluxos de dados e do seu papel na produção e cadeias de valor também ajudará a apoiar a elaboração de políticas.

5.2.1 DADOS PESSOAIS E NÃO PESSOAIS

Embora os dados, concetualmente, tenham significados diferentes para comunidades diferentes e dependendo do contexto, um conceito importante que está no centro do regulamento sobre a proteção de dados é o de dados pessoais. A definição de tipos específicos de dados como pessoais pode ajudar as autoridades de proteção de dados a proteger os direitos das pessoas em causa de forma mais eficiente, mas esta abordagem tem limites.

Quadro político facilitador em matéria de dados



Existem inúmeras formas de categorizar os dados que afetam a política e regulamentação adequadas de cada categoria, e entre as dimensões mais importantes estão a intenção pública ou privada e os métodos tradicionais ou de nova recolha (Conferência das Nações Unidas sobre Comércio e Desenvolvimento, 2021; Banco Mundial, 2021).

À medida que as autoridades de proteção de dados começam a aplicar a legislação sobre a proteção de dados pessoais, devem proporcionar à indústria uma definição clara sobre a forma de diferenciar entre dados pessoais e não pessoais, para permitir a recolha, o armazenamento e o processamento de dados pelas empresas, em conformidade com a regulamentação em matéria de proteção de dados. Isso também reduzirá o risco de não conformidade durante a recolha, armazenamento e processamento de dados. É importante que as políticas de dados e os regulamentos sobre dados partilhem as mesmas categorias de dados para assegurar a coesão política e permitir o seu cumprimento.

5.3 FACTORES IMPULSIONADORES DO VALOR NA ECONOMIA DE DADOS

Para tirar partido dos benefícios dos dados, é necessário criar quadros regulamentares e políticos que facilitem a obtenção de dados úteis; reforçar as capacidades humanas, institucionais e técnicas para criar valor a partir dos dados; incentivar a partilha e a interoperabilidade dos dados; e aumentar a legitimidade e a confiança do público no Estado na gestão responsável dos dados dos cidadãos. Além disso, a infraestrutura de dados que permite um sistema de dados integrado é um ativo estratégico fundamental para os países. O ambiente criado pela interação de elementos no ecossistema de dados e a natureza das relações e processos não lineares entre eles e dentro deles, determinam as intervenções apropriadas para criar incentivos aos investimentos tecnológicos que são necessários para impulsionar o crescimento da economia de dados. Estas condições são moldadas pela estrutura do mercado, a competitividade dos serviços que dele resultam e a eficácia com que o mercado é regulado.

A economia digital abrange várias indústrias e atividades sociais, e a política de dados deve ser localizada no contexto do ecossistema digital complexo e adaptativo mais vasto. Tal como abordado, isto tem implicações para outras áreas políticas, incluindo o comércio e a fiscalidade. Os Estados devem investir em capacidades em matéria de dados e ativos complementares para apoiar a política.

Os investimentos em inovação baseada em dados e investigação e desenvolvimento (I&D), bem como em capacidades para harmonizar normas, competências e infraestruturas, podem permitir aos governos que desenvolvam melhores políticas em matéria de dados em todos os domínios. As questões de confiança e de ética são igualmente importantes, sendo necessário dar prioridade a regulamentos baseados em provas e consultivos.

RECOMENDAÇÕES

- Os Estados-membros da União Africana devem promover a investigação, desenvolvimento e inovação em várias áreas relacionadas com os dados, incluindo, as análises de macrodados, a inteligência artificial, a computação quântica, bem como o Blockchain.
- Todos os grupos de partes interessadas, incluindo os governos, devem criar capacidades analíticas e de gestão de dados para facilitar a utilização de dados de qualidade e de sistemas interoperacionais de confiança. Contudo, é importante lembrar que em muitos países o maior produtor e coletor coletivo de dados é o Estado. Por conseguinte, muitas das observações incluídas na discussão sobre a governação dos dados que se segue têm particular incidência nas ações dos governos.

5.3.1 INFRAESTRUTURA DE DADOS FUNDAMENTAL

5.3.1.1 ACESSO E UTILIZAÇÃO DE BANDA LARGA E DADOS

Definição do problema

Existem barreiras de acesso às infraestruturas de banda larga que impedem as pessoas de aderirem à economia de dados, mesmo como utilizadores. De acordo com a Comissão de

Banda Larga da UIT, que liga África através do **Relatório sobre a Banda Larga**:[5] "É necessário ligar cerca de 1,1 mil milhões de novos utilizadores únicos para conseguir um acesso universal, acessível e de boa qualidade à Internet de banda larga até 2030, e estima-se que sejam necessários mais 100 mil milhões de dólares para atingir este objetivo na próxima década".

Apesar disso, e de várias limitações contextuais, África tem uma posição privilegiada para desenvolver um ecossistema de dados inovador, sendo menos prejudicada pelas infraestruturas de dados herdadas e tendo uma utilização do espectro e níveis de congestionamento relativamente mais baixos (Saint & Garba, 2016). Enquanto a penetração da banda larga fixa na região é inferior a um por cento, a Internet móvel é mais omnipresente com um custo de adoção mais baixo.[6] Por conseguinte, a evolução do ecossistema de dados de África será possibilitada principalmente pelas redes móveis de banda larga.

RECOMENDAÇÃO

Para acelerar a transposição do quadro, os Estados membros da União Africana devem dispor de uma infraestrutura digital robusta e maciça, bem como de capacidade suficiente. Deve dar-se prioridade à obtenção de uma conetividade significativa e de uma Internet acessível que integre mais utilizadores e aumente a procura de serviços de infraestruturas. Para uma adoção e utilização mais eficazes dos dados na região, é necessário resolver os défices de infraestruturas complementares que limitam a utilidade dos dados.

→ AÇÕES

Os Estados-membros terão de desenvolver políticas para:

- banir as taxas proibitivas do "direito de passagem" dos cabos de banda larga e partilhar infraestruturas de apoio;
- impedir práticas anticoncorrenciais decorrentes de uma posição dominante nos mercados de infraestruturas;
- investir em Wi-Fi público e tecnologias complementares;
- adotar técnicas inovadoras de utilização do espectro, tais como a atribuição e acesso dinâmicos ao espectro, e o aproveitamento de espaços brancos de televisão (na sua maioria espectro não utilizado, em grande parte acelerado pela migração da radiodifusão analógica para a digital) para expandir o acesso à banda larga para as zonas rurais mal servidas;
- promover a transição e a adoção do IPv6[7] , à medida que os recursos de IPv4 se esgotam a nível mundial;
- investir na espinha dorsal nacional e em infraestruturas de conectividade transfronteiriça, tais como Pontos de Intercâmbio da Internet (IXP), tanto a nível nacional como regional, para potenciar a largura de banda internacional disponível, reduzir os custos de acesso à Internet e aumentar as velocidades de acesso aos dados na região; e
- aproveitar modelos inovadores para o financiamento da infraestrutura de dados.

5 *https://broadbandcommission.org/Documents/working-groups/DigitalMoonshotforAfrica_Report.pdf*

6 Divisão de Dados e Estatísticas das TIC, Departamento de Desenvolvimento das Telecomunicações, "Factos e Números das TIC 2016", União Internacional das Telecomunicações, Genebra, Relatório de 2016.

7 A versão 6 do Protocolo de Internet é a versão mais recente do Protocolo de Internet que fornece um sistema de identificação e localização de dispositivos em redes e encaminha o tráfego através da Internet.

5.3.1.2 INFRAESTRUTURA DE DADOS

Definição do problema

A infraestrutura de dados fundamentais que facilita os sistemas de dados e permite a partilha, recolha e armazenamento de macrodados, ou a manipulação das fontes de dados existentes, terá impacto na forma como os governos são capazes de responder aos desafios relacionados com a disponibilidade, qualidade e interoperacionalidade dos dados, e abordar considerações relacionadas com a legitimidade e a confiança do público.

A infraestrutura de dados de base refere-se a uma vasta gama de tecnologias que facilitam a utilização intensiva de dados de qualidade, incluindo infraestruturas materiais e imateriais que resolvem os atuais défices "tradicionais" da infraestrutura das TIC e que terão de ser implementadas em paralelo com a criação de uma arquitetura de apoio a uma maior dataficação. Também inclui recursos de infraestruturas tais como a Identificação Digital para permitir transações e presença virtual seguras. Este quadro centrar-se-á em três aspetos de infraestruturas de dados que requerem considerações políticas que se reforçam mutuamente e também influenciam a governação dos dados: os serviços na nuvem, os macrodados e a plataformização.

O desenvolvimento de valor dos dados públicos a partir de infraestruturas e software de computação em nuvem que complementem o grande processamento e a análise de dados terá de ser informado por modelos de segurança e confiança bem desenvolvidos para o armazenamento e o processamento de dados sensíveis ou proprietários, a gestão de API, e o apoio a mercados de ecossistemas de dados equitativos. Para além das insuficiências das infraestruturas digitais em muitos governos – incluindo a fraqueza dos facilitadores para acomodar um ambiente de fornecimento e consumo de serviços de computação em nuvem – os países africanos enfrentam uma multiplicidade de desafios na resposta aos requisitos de infraestrutura, uma vez que esta infraestrutura é frequentemente fornecida e adquirida por fornecedores privados de serviços estrangeiros.

Isto implica que para aproveitar as oportunidades associadas à transformação digital, outros desafios tais como responsabilidades intermediárias, fronteiras de jurisdição, interoperabilidade, e questões de soberania, para citar alguns, terão de ser considerados. Estes desafios sublinham a necessidade de colaboração e parcerias em muitos ecossistemas de dados africanos para reforçar os facilitadores fundamentais de mercados de atividade bem-sucedidos, orientados para os dados, em diferentes pontos da cadeia de valor dos dados, independente mente da maturidade digital interna e dos donativos.

A regulamentação e a legislação em vigor em matéria de tecnologia, organização, direito e comércio terão impacto na capacidade da infraestrutura partilhada em facilitar aos vários participantes no mercado de dados o acesso necessário para operarem no mercado de dados. Os ecossistemas de dados devem ser capazes de suportar vários domínios de aplicação e permitir o intercâmbio e a integração de dados em diferentes fases do ciclo de valor dos dados, preservando simultaneamente a sua proveniência e integridade.

SERVIÇOS EM NUVEM

É útil para efeitos de política distinguir entre "serviços em nuvem" e "serviços baseados na nuvem". O principal benefício oferecido pelos serviços em nuvem é a poupança de custos através de uma maior eficiência dos sistemas. Por exemplo, o sector público e as pequenas,

médias e microempresas (PME), com recursos limitados, podem reduzir as despesas de capital em equipamento informático, incluindo servidores internos, equipamento de rede, recursos de armazenamento e *software*, mudando para um modelo de serviços de computação em nuvem baseado em serviços de utilidade pública.

A interoperacionalidade no fornecimento de nuvem é um fator crítico, pois proporciona flexibilidade e permite aos utilizadores alternar entre um fornecedor de nuvem e outro. Outros benefícios da computação em nuvem incluem a redução das despesas com o consumo de energia, bem como uma menor procura de gestão e manutenção dos sistemas, transferindo a gestão dos recursos informáticos para terceiros. Consequentemente, os fundos podem ser desviados para atividades orientadas para o cliente e para uma melhor prestação de serviços públicos. No entanto, como existem certos fatores que apoiam um ambiente favorável aos serviços baseados na nuvem, a adoção de novas tecnologias deve ser feita em paralelo com a abordagem dos desafios da fratura digital estrutural (capital humano, infraestruturas, etc.). Estes processos devem reforçar-se mutuamente e ser adequados às realidades económicas dos Estados-membros. A criação de valor a partir dos dados da infraestrutura e do software de computação em nuvem, que complementa o processamento e a análise de grandes volumes de dados, implica modelos de segurança e confiança bem desenvolvidos para o armazenamento e o processamento de dados sensíveis/proprietários na nuvem, a gestão das API e o apoio a mercados de dados equitativos.

MACRO DADOS

Estão a ser produzidas grandes quantidades de dados – inclusive como subprodutos de outras atividades (tais como por plataformas de redes sociais quando criam perfis dos seus utilizadores para os anunciantes) – e utilizados para o desenvolvimento de produtos, serviços e formas de negócios inteiramente novas, com potencial para gerar ganhos substanciais de eficiência e produtividade. Isso também oferece um potencial para o sector público que se baseia em grandes quantidades de dados que poderiam ser utilizados para análises de macrodados, para melhorar a tomada de decisões e a previsão e permitir uma melhor segmentação e orientação dos consumidores. As vantagens de escala e alcance relacionadas com os efeitos de rede produziram posições de quase monopólio, que foram ainda mais reforçadas através de fusões de pequenos e novos fornecedores de serviços que, à primeira vista, não parecem estar no mesmo mercado, como o Facebook e o WhatsApp. Isto torna quase impossível a entrada de atores locais em concorrência (Arntz et al., 2016).

PLATFORMIZATION

A transformação do mundo em dados criou igualmente modelos empresariais e modos de criação e extração de valor inteiramente novos. Um deles é a plataformização, que facilita as transações e o trabalho em rede, bem como a troca de informações, agregando múltiplos vendedores e compradores numa única plataforma.

Com o comércio digital e as plataformas de comércio eletrónico cada vez mais subjacentes à atividade global e transfronteiriça, a integração de áreas tradicionalmente distintas de regulamentação e prioridades políticas tornou-se cada vez mais importante e entrelaçada para além das fronteiras geográficas. No entanto, políticas como a localização de dados não serão plausíveis sem a existência dos requisitos estruturais e institucionais necessários para a sua evolução e implementação efetivas, em particular a referência às capacidades digitais (Andreoni & Tregenna, 2020).

RECOMENDAÇÕES

- A utilização de dados como instrumento para melhorar os interesses públicos exigirá que os Estados reforcem as infraestruturas de dados nacionais e necessitará de um forte envolvimento das partes interessadas a nível nacional, regional e global. O desenvolvimento de quadros abrangentes de política de dados facilitadores deve ser acompanhado de estratégias de implementação sensíveis ao tempo através de diferentes mandatos internos para assegurar a responsabilização e a transparência.
- Os Estados-membros devem dar prioridade aos recursos para assegurar que existem incentivos para aumentar os investimentos em infraestruturas digitais, em plataformas de dados, e em capacidades de software para aproveitar os macrodados. Os investimentos em infraestruturas de dados devem apoiar o contrato social digital. Os esforços do Estado para melhorar a interoperacionalidade, a qualidade e a administração pública de dados devem também complementar e melhorar, tanto quanto possível, os sistemas digitais públicos, tais como as identificações digitais, os pagamentos digitais, e os fluxos de dados abertos. Por outro lado, a infraestrutura adequada é também uma componente necessária de qualquer sistema interoperável e integrado de partilha de dados. Além disso, a reutilização ou o reaproveitamento de dados exige normalmente sistemas de dados que funcionem bem e que facilitem o fluxo seguro de dados em formatos legíveis por máquina que tornem os dados úteis para muitos utilizadores.

→ AÇÕES

- Em vez de se concentrarem no investimento inicial significativo para substituir o equipamento de TIC obsoleto, os Estados-membros devem tirar partido das economias de escala e de gama para adotar infraestruturas que apoiem os benefícios oferecidos pelos serviços em nuvem e por outras novas tecnologias que apoiam a criação de valor a partir dos dados.
- As políticas fiscais, comerciais (incluindo o investimento e a inovação) e de concorrência devem ser coerentes, complementares e adaptadas à economia digital orientada para os dados, em particular para informar as estratégias de desenvolvimento de infraestruturas.
- Os Estados-Membros devem garantir que as empresas locais participem nas cadeias de valor dos fornecedores estrangeiros de software como serviço (SaaS), de infraestruturas como serviço (IaaS) e de plataformas como serviço (PaaS) para efeitos de contratos públicos e criar incentivos para que as PME locais participem nas cadeias de valor dos dados em todos os sectores. Para o efeito, é necessário assegurar que as políticas fiscais, comerciais (incluindo o investimento e a inovação) e de concorrência sejam coerentes, complementares e adaptadas à economia digital baseada nos dados.
- Adotar modelos de produção de eletricidade mais sustentáveis, a nível interno e em toda a região, para assegurar que a infraestrutura digital fundacional apoie atividades de dados domésticos e transfronteiriços sustentáveis que tenham menos impactos extrativos no ambiente natural.

GOVERNAÇÃO DE DADOS

- Criar direitos de portabilidade dos dados – inclusive para dados não pessoais, para facilitar aos clientes de serviços em nuvem a troca entre provedores.

- Desenvolver normas contratuais para organizações públicas (que também podem ser utilizadas pelas PME), que protejam os seus direitos de acesso, recuperação, eliminação, etc. dos dados (incluindo dados não pessoais) que são processados por fornecedores de nuvem.
- Desenvolver obrigações de licenciamento justas, razoáveis e não discriminatórias (FRAND) para plataformas e fornecedores de nuvem que tenham acesso a conjuntos de dados que se tornem um recurso vital para entrar no mercado.

5.3.1.3 IDENTIFICAÇÃO DIGITAL

Definição do problema

Enquanto o continente africano acolhe a maior percentagem de pessoas sem identidade legal e, consequentemente, sem registo civil e sem serviços sociais essenciais oferecidos pelos Estados, como os cuidados de saúde, o ensino básico ou serviços alimentares[8], a economia digital oferece oportunidades para corrigir desigualdades como as exclusões socioeconómicas e estruturais sofridas por grupos minoritários no continente.

A identificação digital (Digital ID), como forma de expressão de dados pessoais, deve ser construída e implementada de forma coesa e em conformidade com os quadros gerais de governação de dados. Essa ferramenta é facilitadora tanto para fins do sector privado como do sector público no âmbito de uma economia de dados, mas exige um quadro robusto orientado para a confiança, a fim de atenuar os potenciais danos, como a utilização abusiva de dados pessoais, a exclusão ou a discriminação com base numa representação inexata (ou injusta) dos dados, que podem acompanhar a sua implementação. Além disso, embora as parcerias público-privadas tenham potencial para expandir a prestação pública de serviços estatais e impulsionar a inovação socioempresarial, essas colaborações podem potencialmente exacerbar a desigualdade (através da utilização abusiva de dados), para além dos danos acima mencionados. Os quadros adotados pelas autoridades/agências nacionais de identidade existentes devem, por conseguinte, ser revistos de modo a refletir estas oportunidades, riscos e danos.

RECOMENDAÇÕES

Um sistema de identificação digital (Digital ID) justo e fiável é um pré-requisito fulcral para combinar e redirecionar dados administrativos públicos com outros tipos de dados em vários casos de utilização. As atividades da política de dados regional devem alinhar-se com as que ocorrem no âmbito de atividades simultâneas da identificação digital. As iniciativas de identificação digital do sector público devem permanecer orientadas por quadros de governação de dados, sejam eles fundacionais ou funcionais[9].

8 Ver *https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity*

9 A Comissão da União Africana está a desenvolver um Quadro de interoperacionalidade para a identificação digital, que fornecerá um conjunto detalhado de recomendações aos Estados-membros sobre a introdução e salvaguarda dos sistemas de identificação digital.

5.3.2 CRIAÇÃO DE SISTEMAS DE DADOS LEGÍTIMOS E FIÁVEIS

Definição do problema

Um ambiente de dados fiável exige que os utilizadores confiem em todo o sistema político e económico subjacente à economia de dados. Os aspetos fundamentais deste tipo de sistema incluem a salvaguarda dos direitos humanos básicos através do Estado de direito; disposições e regulamentos institucionais estabelecidos através de processos consultivos e transparentes; e a exigência que as instituições responsáveis pela supervisão da utilização de dados, bem como os produtores de dados públicos e privados, sejam responsáveis pela utilização de dados públicos e pessoais. A inclusão e diversidade de pessoas que gerem e supervisionam ambientes de dados, por exemplo, através de equipas diversificadas em termos de género, é importante para construir confiança. Vários países africanos já possuem muitos destes aspetos. O desafio continental é garantir que todos os países apresentam todos os aspetos necessários e que estes são devidamente adaptados à rápida evolução dos desafios tecnológicos e económicos em matéria de dados. O quadro estabelece todos os componentes essenciais para sistemas de dados legítimos e dignos de confiança, a fim de permitir que os países avaliem se têm alguns ou todos os componentes totalmente implementados.

A confiança nas transações de dados, nos dados estatísticos e na tomada de decisões com base em dados deve, portanto, ser sustentada por um quadro jurídico e regulamentar transparente e robusto que simultaneamente proteja contra danos causados pelos dados e apoie os elementos que facilitam o acesso aos dados, a partilha de dados e as alterações de dados de forma responsável. Um quadro forte e de confiança, junto com a capacidade institucional para apoiar este quadro, permitirão aos governos criar valor a partir dos dados, minimizar as assimetrias de dados entre os setores público e privado, e refrear comportamentos não competitivos nos ecossistemas de dados (Macmillan, 2020).

Neste contexto de construção de um ecossistema digital de confiança, três áreas-chave inter-relacionadas necessitam de uma consideração específica: a segurança cibernética, a cibercriminalidade, e a proteção de dados. O papel da conceção ética e da regulamentação positiva para assegurar resultados justos também merece destaque.

5.3.2.1 SEGURANÇA CIBERNÉTICA

À medida que a tecnologia evolui e tecnologias disruptivas são adotadas, novas ameaças e riscos indesejados são gerados. Isso não só tem impacto nos bens, infraestruturas e redes, mas também nas economias, sociedades, e pessoas, sendo os mais vulneráveis os mais afetados. Por este motivo, a utilização de tecnologias disruptivas e as normas, regras e práticas dos sectores público e privado para governar a segurança, podem ter impacto nos direitos fundamentais das pessoas em matéria de equidade, dignidade e segurança.

Embora as políticas, leis e regulamentos possam ser instrumentos utilizados para combater as ameaças e proteger as pessoas dos riscos, também podem ser utilizados para normalizar ou legitimar os sistemas de opressão e repressão. Por conseguinte, qualquer resposta de política cibernética destinada a reforçar a segurança dos dados deve considerar elementos de proporcionalidade (incluindo a legalidade, a legitimidade do objetivo, a necessidade e a adequação) como o requisito mais importante que deva ser satisfeito quando se pretende limitar de qualquer forma os direitos humanos em linha.

5.3.2.2 CRIMINALIDADE CIBERNÉTICA

O ecossistema de dados destaca tanto as oportunidades como os riscos de uma vasta rede de sistemas públicos e privados interligados. Devido à natureza transnacional da cibercriminalidade e das operações cibernéticas, a política de segurança de dados é, na sua maioria, moldada em fóruns multilaterais globais ou regionais. Embora a participação africana nestes fóruns tenha aumentado, o envolvimento de atores africanos não estatais é ainda limitado. Além disso, um desafio político emergente é avaliar que capacidade é necessária a nível nacional para implementar convenções acordadas a nível regional e global sobre a cibercriminalidade e as normas cibernéticas voluntárias e não vinculativas.[10]

5.3.2.3 PROTECÇÃO DE DADOS

Os riscos de posse ilegal de dados processados são suportados principalmente pelas próprias pessoas em causa, e não pela entidade que extrai valor. Por essa razão, os mecanismos e princípios para mitigar os riscos relativos à privacidade devem ser centrais em qualquer quadro político nacional e regional que procure aproveitar o potencial das economias de dados.

Embora tal exija o desenvolvimento de instituições e leis sólidas de governação dos dados, estas leis também têm de se adequar aos contextos específicos em que estão a ser implementadas. Devem ser consideradas nomeadamente as realidades socioeconómicas e tecnológicas e as capacidades do público. Dito de forma diferente, um quadro de política de dados deve desenvolver políticas e regulamentos capazes de reconhecer as realidades das capacidades e funcionalidades de um cidadão, juntamente com os riscos que acompanham os desenvolvimentos digitais e conduzam a uma distribuição desigual de benefícios e danos (Sen, 2001; van der Spuy, 2021).

Por exemplo, com um número significativo de pessoas que não sabe utilizar ferramentas digitais ou é analfabeta em África, os mecanismos digitais de consentimento informado podem não ser suficientes para proteger os direitos das pessoas. Existe o risco de os meios digitais de obtenção de consentimento, como clicar num botão ligado a um longo conjunto de termos legais, não corresponderem efetivamente a um consentimento informado, porque a ação que se pretende que constitua consentimento pode não ser um ato informado ou não ser de todo compreendida pela pessoa. Outros meios de gestão de dados, tais como os fideicomissos de dados, que estão a surgir a nível mundial e asseguram que os direitos das pessoas sobre os seus dados são respeitados, são discutidos a seguir. Além disso, o enquadramento dominante da governação dos dados é geralmente equiparado à proteção dos dados e a proteção dos dados à privacidade. É entendida, em grande medida, como um direito individual e um desafio individual. No entanto, há questões de direitos comunitários e coletivos que podem ser importantes em primeiro plano quando se trata de questões de interesse público.

10 Foram observados défices na capacidade de implementação em cinco dimensões: política e estratégia de segurança cibernética- ca; cultura e sociedade cibernética; educação, formação e competências em segurança cibernética; quadros jurídicos e regu lamentares; e normas, organizações e tecnologias.

5.3.2.4 JUSTIÇA DE DADOS

O conceito de justiça dos dados promove uma visão mais ampla do que a proteção de dados. Embora um quadro de política de dados que preserve os direitos seja essencial para salvaguardar os direitos das pessoas, as noções individualizadas de privacidade nos atuais quadros normativos de proteção de dados podem não ser suficientes para garantir uma inclusão equitativa no âmbito de uma economia de dados de confiança. A justiça dos dados é um conceito que tem vindo a ganhar força em resposta à adoção exponencial de tecnologias baseadas em dados em todo o mundo, particularmente a inteligência artificial (GPAI, 2021[11], Taylor, 2019). Procura garantir que a crescente dependência nos dados, especialmente no que diz respeito à tomada de decisões automatizada, não perpetue as injustiças históricas e as desigualdades estruturais. Aborda a questão da equidade em resposta ao grau em que as pessoas são visíveis, representadas, sub-representadas e discriminadas como resultado da sua produção de dados digitais.

A justiça dos dados estende-se também para além das noções de direitos políticos e justiça, aos direitos sociais e económicos e à regulamentação necessária para corrigir as desigualdades e permitir às pessoas o exercício dos seus direitos. Existem muitas outras áreas de governação de dados relativos à disponibilidade, acessibilidade, usabilidade e integridade dos dados que têm impacto na inclusão equitativa. Se estes forem regulados no interesse público, poderão contribuir para uma melhor distribuição das oportunidades não só para o consumo de serviços de dados, mas também para a produção de serviços.

RECOMENDAÇÕES

Os Estados-membros devem procurar estabelecer um ambiente de dados fiável através da segurança cibernética, da proteção dos dados pessoais, do Estado de direito e de instituições capazes, reativas e responsáveis. É necessário estabelecer a confiança na governação dos dados e num sistema nacional de dados, garantindo a legitimidade de todo o sistema. Isso inclui sistemas e normas que garantem a conformidade do sector público e privado, a adesão do próprio governo às regras de proteção dos dados pessoais e a partilha de dados públicos pelo governo.

→ AÇÕES

- Salvaguardar os direitos humanos fundamentais através do Estado de Direito.
- Garantir que os acordos e regulamentos institucionais sejam estabelecidos apenas através de processos inclusivos, consultivos e transparentes.
- Garantir que as instituições responsáveis pela supervisão da utilização de dados, bem como os produtores de dados públicos e privados, sejam responsáveis pela utilização de dados públicos e pessoais para aqueles cujos dados são utilizados.

11 A Parceria Global sobre Inteligência Artificial desenvolveu um projeto que visa preencher uma lacuna na investigação e prática de justiça de dados que fornece um quadro para ajudar os profissionais e utilizadores a ir além da compreensão da governação de dados como uma questão de conformidade de privacidade individualizada ou de conceção ética. O projeto procura incluir considerações de equidade e justiça em termos de acesso, visibilidade e representação nos dados utilizados no desenvolvimento de sistemas AI/ML. *https://gpai.ai/projects/data-governance/data-justice/*

- Reforçar a cooperação com outras APD para assegurar uma salvaguarda suficiente, a proteção recíproca dos dados pessoais, bem como os direitos digitais individuais e coletivos em todo o continente.
- Reforçar os acordos e atividades de assistência mútua entre Estados para a investigação e repressão da cibercriminalidade.
- Garantir que as instituições responsáveis pela supervisão do uso de dados pessoais tenham poderes de entrada e inspeção para fins de aplicação de leis e regulamentos de privacidade e proteção de dados.
- Além disso, garantir que o responsável institucional por supervisionar o uso de dados pessoais tenha os seguintes poderes corretivos em relação à correção da violação de aspetos de uso indevido e abuso de dados pessoais:
    - Emitir avisos a um responsável pelo processamento de dados ou a um processador de dados de que as operações de processamento pretendidas são suscetíveis de infringir as disposições das leis e regulamentos relevantes em matéria de proteção de dados;
    - Emitir repreensões a um responsável pelo processamento de dados ou a um processador de dados quando as operações de processamento infringirem as disposições das leis e regulamentos de proteção de dados relevantes;
    - Ordenar a um responsável pelo processamento de dados que comunique uma violação de dados pessoais aos titulares dos dados afetados;
    - Impor uma limitação temporária ou definitiva, incluindo a proibição do processamento de dados pessoais; e
    - Ordenar a suspensão dos fluxos de dados para um destinatário num país terceiro ou para uma organização internacional que não assegure uma proteção adequada semelhante à do país exportador de dados.
- As instituições responsáveis por supervisionar o uso de dados pessoais devem ter poderes para ajudar ou buscar indulgência do tribunal para ajudar uma pessoa que sofreu danos materiais como resultado de uma violação de seus dados pessoais para receber compensação de um responsável pelo processamento de dados ou processador de dados para os danos sofridos.

5.3.2.5 ÉTICA EM DADOS

Uma forma importante de reduzir os riscos e mitigar os danos ligados à aplicação de novas tecnologias de dados é através de uma ética de dados contextualmente apropriada. Os códigos de ética devem ser desenvolvidos por todos os grupos de interessados que trabalham com dados, incluindo investigadores, associações industriais e peritos em dados. Estes códigos de ética são valiosos para orientar a utilização de dados, e os processos de conceção e implementação de sistemas de dados, incluindo a sua incorporação em código informático no caso do desenvolvimento de algoritmos.

No entanto, os códigos de ética têm sido criticados como representando os pontos de vista de demografia limitada, definida na sua maioria pelas corporações e tecnólogos. Os códigos éticos podem igualmente aliviar as empresas da responsabilidade regulamentar quando

utilizados como forma de autorregulação, e podem ser insuficientes para garantir os direitos fundamentais das pessoas quando utilizam a tecnologia.

Os códigos de ética, juntamente com a lei, permitem que os sistemas de dados sejam fiáveis, uma vez que fornecem o tipo de pormenores práticos e técnicos que estão na base das leis, que são muitas vezes de aplicação mais geral do que os códigos de ética específicos, mas que por vezes também se adaptam menos rapidamente às novas tecnologias. A ética opera de forma prospetiva, permitindo a conceção ética enquanto as leis tendem a ser promulgadas e a funcionar de forma retrospetiva. Os códigos de conduta éticos devem incorporar os direitos digitais e apoiar o cumprimento da legislação internacional e nacional.

A UA apoia os esforços para tornar os códigos de ética mais inclusivos através de processos que tenham em conta as vozes dos cidadãos, dos consumidores, dos grupos marginalizados e das pessoas sub-representadas. No entanto, os mecanismos para garantir a adesão aos códigos de ética, bem como para atualizar esses códigos, estão subdesenvolvidos.

Os tratados de direitos humanos – enquanto produtos de processos de consenso entre os representantes legítimos dos cidadãos – gozam de maior legitimidade do que os códigos de ética, e são legalmente aplicáveis quando promulgados a nível nacional, e através de adjudicação regional. Embora estes tratados careçam por vezes da especificidade necessária para os ecossistemas de dados, os direitos digitais, que têm sido formulados de forma variada pela sociedade civil entre outros e se baseiam no quadro dos direitos humanos, proporcionam o tipo de especificidade que pode ser aproveitado. Embora os organismos de direitos humanos e os adjudicatários existentes tenham a capacidade necessária para desenvolver direitos em resposta a questões de dados, os seus mandatos legais podem não os habilitar suficientemente para o fazer.

RECOMENDAÇÕES

- Os Estados-membros devem incentivar o desenvolvimento e a adesão a códigos de ética que respondam ao contexto africano, e que promovam os direitos digitais e humanos. Isso significa que as pessoas que trabalham com dados, independentemente do sector em que trabalham, devem respeitar os direitos e aderir a estas normas éticas. Estes códigos devem ter em conta as considerações de género no contexto africano, assegurando que reduzem os danos e a exclusão das mulheres e meninas. É inexequível que os Estados Membros legislem no sentido de todas as tecnologias e fornecedores de tecnologia que lidam com dados aderirem a códigos éticos específicos, uma vez que muitas destas tecnologias são concebidas, construídas e operadas noutras jurisdições. Os Estados-membros devem, contudo, encorajar a adoção destes códigos de ética por eles próprios, utilizando apenas tecnologias e fornecedores de tecnologia que adiram aos códigos de conduta ética aprovados.
- Para além de qualquer recurso legal regulamentar ou judicial disponível num país, também é possível considerar a possibilidade de capacitar os mecanismos de direitos humanos existentes a nível nacional, regional e continental para adjudicar as utilizações de dados.

→ **AÇÕES**

- A indústria dos dados e as comunidades de investigação que utilizam dados devem formular e implementar códigos de prática, incluindo os princípios de responsabilidade e ética pela conceção através de processos que incluam aqueles cujos dados são afetados.
- Os Estados-membros devem exigir quadros éticos conformes com os direitos nos processos de contratos públicos.
- Os membros devem incluir a avaliação dos códigos de ética de dados nos mandatos dos organismos de direitos humanos existentes, tais como as Comissões de Direitos Humanos.

5.3.3 DISPOSIÇÕES INSTITUCIONAIS PARA A REGULAÇÃO DE SISTEMAS ADAPTATIVOS COMPLEXOS

As considerações seguintes são fundamentais para alinhar o contexto regulamentar de um país com os requisitos de uma economia de dados. A regulamentação nas economias de dados requer decisões regulamentares ágeis face à incerteza. Por isso, os reguladores exigem tanto o mandato como a confiança para regular proactivamente. A complexa regulação adaptativa responde não só aos desafios da rápida mudança e incerteza, mas também à complexidade dos ecossistemas de dados caracterizados por dinâmicas multifatoriais.

5.3.3.1 CONSTRUIR A CAPACIDADE DOS ORGANISMOS REGULADORES

A rápida intensificação dos processos de digitalização e dataficação apresenta novos desafios regulamentares nas áreas tradicionais de concorrência e proteção do consumidor, e em áreas de regulamentação inteiramente novas, incluindo a proteção dos dados pessoais das pessoas e a governação algorítmica para assegurar que as pessoas não sejam discriminadas. Embora os princípios tradicionais de independência, transparência e responsabilidade continuem a informar a regulamentação e governação eficazes dos dados, os decisores políticos e reguladores precisam de desenvolver novas capacidades para enfrentar os desafios.

5.3.3.2 SAIR DOS SILOS REGULAMENTARES

Embora as diferentes dotações institucionais determinem se os reguladores existentes têm capacidade para gerir novas áreas de governação, é evidente que terá de haver uma mudança da regulação dentro dos silos sectoriais tradicionais para uma ação reguladora integrada ou, no mínimo, coordenada. Isto é possível graças ao desenvolvimento de estratégias e políticas digitais transversais que reconheçam a natureza transversal da digitalização e da dataficação. É essencial para criar a coordenação necessária entre os vários sectores dos serviços públicos afetados pela economia de dados e, ao mesmo tempo, para satisfazer as necessidades específicas do sector na gestão dos dados.

Reguladores do sector	Tópicos de potencial colaboração com o regulador de dados
Telecomunicações	Disponibilidade e qualidade da infraestrutura fundamental para permitir os serviços de dados
Concorrência	Concentração, fusões e aquisições, prática anti-concorrencial nos mercados digitais e de dados, mas também efeito dos mecanismos de fixação e preços e estrutura de mercado na segurança
Protecção do consumidor	Dispositivos e serviços digitais, comércio electrónico
Comércio/transações	Tributação digital, comércio eletrónico, serviços digitais, serviços financeiros digitais
Finanças	Finanças Blockchain, segurança cibernética, inclusão financeira, serviços financeiros móveis, privacidade
Educação	Proteção em linha, conectividade das escolas, disponibilidade de dados para a aquisição de competências em matéria de dados

Fonte: Adaptado de TGM 2020 no Banco Mundial da UIT de 2020.

A REDE AFRICANA DE REGULADORES DA INFORMAÇÃO

Fornece um exemplo de colaboração regional para estabelecer reguladores nacionais de dados, aumentar a sensibilização para a governação das novas informações e dos dados, proporcionar a governação dos fluxos de dados transfronteiriços e cooperar com os reguladores a nível internacional. O seu objetivo é alinhar a governação dos dados, especialmente no que diz respeito à resposta proporcional e normalizada a violações de dados e de direitos.

Os reguladores e decisores políticos nacionais têm um papel a desempenhar na arena internacional. In Devem Intensificar a cooperação internacional em matéria de fluxos transfronteiriços de dados para garantir que os requisitos de localização de dados e outras restrições aos fluxos transfronteiriços de dados não interfiram indevidamente com as comunicações transfronteiriças e com os benefícios económicos e sociais que as redes globais de dados possibilitam e sejam minimamente restritivos do comércio, favorecendo ao mesmo tempo a confiança.

É preciso incentivar a cooperação regional e internacional em matéria de privacidade dos dados e iniciativas de segurança cibernética para simplificar uma miscelânea de regras e práticas de privacidade de dados e de segurança cibernética em normas e leis regionais ou globais comuns e permitir o livre fluxo de dados e o comércio digital (GSR, 2021).

5.3.3.3 REGULADOR DE DADOS

A capacidade dos reguladores sectoriais para serem eficazes é determinada, pelo menos em certa medida, pelos acordos institucionais e pela autonomia dos reguladores para implementar a política. Os níveis de eficiência e inovação que permitem a evolução do ecossistema dependem das aptidões e competências das pessoas e instituições em cada nó do ecossistema para aproveitar os benefícios associados às redes integradas para o desenvolvimento económico, e ao envolvimento social e político. O desenvolvimento de um sistema integrado de dados a nível nacional e regional depende também em grande medida da criação de quadros regulamentares e políticos que facilitem a obtenção de dados úteis, do reforço das capacidades humanas e técnicas para criar valor a partir dos dados, do incentivo à partilha e interoperabilidade dos dados e do aumento da legitimidade e da confiança do público no Estado para gerir os dados dos cidadãos de forma responsável. A criação de condições que permitam o acesso necessário aos dados, salvaguardando simultaneamente os direitos, exigirá a criação de capacidades e competências institucionais para otimizar o potencial dos dados, e o desenvolvimento de mecanismos de aplicação.

5.3.3.4 CONCORRÊNCIA

Como os reguladores em África esforçam-se por introduzir e aplicar a regulação da concorrência tradicional, existe o perigo de que a regulação estática da concorrência para governar sistemas dinâmicos e adaptativos possa inibir a inovação e danificar a tecnologia subjacente que permite a inovação. Por exemplo, a regulamentação que se concentra em restringir o predomínio apenas na camada de aplicativos da Internet pode ter um impacto negativo e até mesmo prejudicar toda a Internet e sua infraestrutura. Os reguladores devem ter cuidado ao aplicar instrumentalmente regras de concorrência de mercado unilaterais baseadas em modelos de eficiência estática a novas plataformas de dados e produtos baseados na eficiência dinâmica que podem produzir produtos complementares inovadores (como o WhatsApp) que aumentam o bem-estar e a escolha do consumidor ou até oferecem oportunidades de concorrência local nas suas plataformas, embora sejam dominantes no mercado global subjacente (Facebook).

As plataformas são diferentes dos operadores tradicionais dos mercados, uma vez que são constituídas por numerosos mercados relevantes que têm múltiplos "lados", cada um com dinâmicas de concorrência específicas. Do mesmo modo, os produtos e serviços Over-the-Top (OTT) podem parecer integrados verticalmente quando, de facto, são complementares e reforçam a concorrência. Estes tipos de desafios exigem reguladores igualmente adaptáveis, capazes de gerir a sua complexidade no interesse público.

5.3.3.5 DEFESA DO CONSUMIDOR

Como as autoridades de proteção do consumidor não são responsáveis por um sector específico, no exercício das suas funções têm geralmente confiado em outros reguladores específicos do sector. Regras claras, fortes e aplicáveis relacionadas com a gestão de dados podem proporcionar uma defesa adequada para a proteção do consumidor digital, ao mesmo tempo que podem fornecer um quadro previsível e estruturado para a realização de atividades comerciais digitais. Protocolos e mecanismos reguladores ágeis capazes de se adaptarem a tecnologias e condições em rápida mutação podem contribuir em muito para aumentar a

confiança no ecossistema digital. Estes incluem o cumprimento dos requisitos relativos ao acesso a dados não pessoais mantidos pelas plataformas digitais, a transparência de certos algoritmos essenciais utilizados pelos serviços digitais, a portabilidade dos dados essenciais das plataformas de estruturação e a interoperacionalidade e manutenção das APIs (União Internacional das Telecomunicações, 2020).

Uma forma de aumentar a transparência na utilização dos dados dos consumidores é a criação de um portal de transparência, mas tal depende de o facto do regulador de dados ter os recursos para estabelecer, controlar e fazer cumprir as infrações. Isto proporciona às pessoas um acesso seguro a um portal onde podem ver o histórico de quando e com quem os seus dados pessoais foram partilhados, permitindo-lhes contestar a partilha ou a utilização dos seus dados sem o seu consentimento. Esta disposição poderá não se aplicar a determinadas categorias de dados de interesse público, na medida em que a partilha de dados é efetuada através da pseudonimização ou anonimização dos mesmos.

RECOMENDAÇÕES

Os Estados-membros da UA devem ter regulamentos adequados, particularmente em torno da governação de dados e plataformas digitais, para assegurar que a confiança seja preservada no ambiente digital. Os reguladores de dados devem ter os poderes necessários para fazer cumprir os regulamentos de dados, tais como poderes para emitir avisos, penalizar por infrações, conceder indemnizações às vítimas de dados, e cooperar com outras agências, incluindo agências de execução.

→ ACTIONS

- Estados-membros com reguladores de dados devem avaliar se os poderes de execução existentes são suficientes.
- Os Estados-membros que estão a instituir reguladores de dados devem considerar uma série de poderes de execução e, ao abordar as restrições de recursos, a forma como os reguladores de dados podem potencialmente recorrer a outras agências para a execução.

5.3.4 REEQUILÍBRIO DO ECOSSISTEMA JURÍDICO

Definição do problema

Vários dos diferentes, mas sobrepostos, ramos do direito, tais como o direito de proteção de dados, o direito da concorrência, o direito da segurança cibernética, o direito das comunicações e transações eletrónicas, e as diferentes categorias do direito da propriedade intelectual tratam de dados. No entanto, podem entrar em conflito ou contradizer-se mutuamente. Em contraste com a proteção de dados que se aplica apenas aos dados que podem ser relacionados com um indivíduo, o regulamento da concorrência aplica-se aos dados quando o controlo dos dados tem um efeito anticoncorrencial. O controlo concentrado nos dados, inclusivo nos fluxos de dados e na análise de dados, implica não só barreiras à entrada no mercado, mas também obstáculos ao interesse público. A concentração de dados, fluxos de dados e sistemas de dados aumenta substancialmente a probabilidade de danos causados por ataques cibernéticos e violações de dados, uma vez que um único ou poucos pontos de falha que podem ter consequências em grande escala. Estas preocupações não

são da competência de muitas autoridades de concorrência, mas deveriam sê-lo, uma vez que se trata de preocupações de interesse público. As autoridades de concorrência podem ser mandatadas para evitar uma centralização estrutural que aumenta os riscos de ataques cibernéticos ou de violações maciças de dados à escala da sociedade. O acesso aos dados é geralmente pró-competitivo, mas pode estar em tensão com outras leis, tais como as reivindicações de propriedade intelectual sobre dados e bases de dados e a privacidade e proteção de dados.

Embora seja geralmente aceite que os dados em bruto não são protegidos por qualquer direito de propriedade reconhecido, foram feitas alegações sobre os dados com base nos diferentes tipos de propriedade intelectual: direitos de autor, proteção sui generis de bases de dados, segredos comerciais e patentes. Nenhuma destas subvenções concede propriedade sobre dados, como tal. A proteção de bases de dados sui generis é uma lei única da União Europeia, confinada à Europa. Em alguns países de direito comum, o direito de autor foi alargado a bases de dados e compilações de dados, mas mesmo estes países têm regras diferentes com alguns tribunais que alargam o direito de autor apenas para o esforço de compilação, enquanto outros exigem criatividade. Os direitos de autor destinam-se a recompensar autores humanos e a sua aplicação a bases de dados compiladas por computadores é indeterminada. As disputas entre concorrentes sobre a utilização excessiva de bases de dados padrão da indústria derivam dos direitos de autor e do direito da concorrência. Um acórdão do tribunal (Discovery Ltd e outros contra Liberty Group Ltd ZAGPJHC 67, 2000) oferece uma solução que defende tanto a proteção de dados como a concorrência: em tais litígios, se os dados forem de natureza pessoal, são "propriedade" da pessoa em causa e os concorrentes não podem excluir outros do acesso a essa informação. Embora a aplicação das leis de propriedade intelectual aos dados ainda esteja a ser resolvida, os direitos das pessoas sobre os seus dados pessoais devem ser tratados como mais fortes do que qualquer reivindicação de propriedade intelectual sobre esses dados, porque a proteção de dados é essencial na construção de economias de dados.

Os segredos comerciais podem também aplicar-se aos dados em algumas circunstâncias, mas não é claro quais são exatamente essas circunstâncias.

A aplicação das leis de propriedade intelectual é simultaneamente complicada e indeterminada, mas é pelo menos claro que as reivindicações sobre dados baseadas na propriedade intelectual, ainda que contestadas, podem potencialmente pôr em risco os fluxos benéficos de dados e a proteção de dados.

As leis em matéria de cibercriminalidade proíbem o acesso, a utilização ou a alteração de dados pessoais ou sistemas de identificação não autorizados. Tal como reiterado em todo o presente quadro político, a segurança e a proteção são essenciais para uma implementação eficaz da política e constituem um requisito mínimo, embora não suficiente, para a construção de um sistema digno de confiança. As leis relativas à cibercriminalidade, que determinam as formas de acesso, utilização e distribuição de dados, podem ter o efeito de aumentar as barreiras de entrada na economia de dados. A Convenção de Malabo, promulgada pela União Africana e especificamente adaptada à região, aborda tanto a cibercriminalidade como a proteção de dados. No entanto, não entrou ainda em vigor, uma vez que nem todos os países da União Africana a ratificaram.

Os Estados-membros têm a oportunidade de reinventar um sistema jurídico harmonizado que equilibre adequadamente os interesses concorrentes.

RECOMENDAÇÕES

Para garantir um acesso equitativo e seguro aos dados para a inovação e a concorrência, os Estados-membros devem estabelecer uma abordagem jurídica unificada que seja clara, inequívoca e que ofereça proteção e obrigações em todo o continente. Quando necessário, os instrumentos jurídicos existentes devem ser revistos regularmente para garantir que não entrem em conflito entre si e que ofereçam níveis complementares de proteção e obrigações dentro dos Estados-membros. De acordo com os seus sistemas jurídicos, os Estados-membros devem apoiar a racionalização destas políticas a nível subnacional para facilitar a implementação adequada a todos os níveis económicos. As leis de propriedade intelectual devem ser revistas para esclarecer que geralmente não impedem o fluxo de dados ou a proteção de dados.

→ AÇÕES

- Os contratos que pretendem renunciar aos direitos digitais e à proteção de dados pessoais e que inibem a concorrência devem, como regra geral, ser inexequíveis. Isto pode ser articulado na proteção de dados e na regulamentação da concorrência, que também pode considerar, caso a caso, se os efeitos pró-concorrenciais de tais contratos compensam os efeitos anticoncorrenciais.
- As comissões nacionais de reforma legislativa ou instituições jurídicas especializadas similares devem investigar e considerar como harmonizar os diferentes ramos da legislação, os regimes regulamentares e as autoridades de supervisão que lidam com dados.
- Os Estados-membros devem apoiar a atualização ou adoção de quadros e regulamentos de direito da concorrência que considerem os desafios de analisar as questões de concorrência, conceber soluções e fazer cumprir os seus poderes para salvaguardar a concorrência nos mercados orientados para os dados, bem como reforçar a capacidade dos reguladores da concorrência para implementar estas regras.
- As leis de propriedade intelectual devem ser alteradas para prever:
  - que, se os direitos de autor se aplicam a bases de dados e compilações de dados, só se aplicam ao trabalho de autores humanos que demonstrem originalidade ou criatividade e que os direitos de autor se estendem apenas à seleção e disposição originais dos dados numa base de dados ou compilação e não aos próprios dados;
  - que qualquer direito de autor ou outro direito de propriedade intelectual, incluindo segredos comerciais que permitam o controlo de dados, não se aplicam aos dados pessoais;
  - que qualquer direito de autor ou outro direito de propriedade intelectual, incluindo segredos comerciais que permitem o controlo de dados, é limitado pelas disposições da regulamentação da concorrência e pelos direitos alternativos que oferecem proteção às inovações locais não previstas nos quadros atuais; e
  - adaptações aos regimes de DPI existentes para pressionar as próximas tecnologias de ponta, permitindo, por exemplo, que a IA utilize dados.

5.3.4.1 COLABORAÇÃO COM PROCESSOS DE GOVERNAÇÃO REGIONAL E GLOBAL

A regulação das economias digitais e de dados ultrapassa cada vez mais o âmbito das autoridades reguladoras nacionais (ARN) individuais. Uma regulamentação eficaz exige que os reguladores colaborem com os reguladores das suas regiões e a nível mundial para assegurar a realização da Internet como um bem público, e a sua utilização produtiva e baseada em direitos na economia digital.

A regulação formal deve deixar espaço suficiente para a autorregulação, modelos reguladores híbridos e colaborativos e mecanismos de supervisão para a aplicação da lei. A gama de ferramentas e remédios que os reguladores podem explorar é ampla, desde incentivos e recompensas, passando pela indulgência, até obrigações específicas. Os instrumentos regulamentares expandiram-se para abranger caixas de areia regulamentares, quadros éticos, roteiros tecnológicos, avaliações de impacto regulamentar, investigação multivariada e simulação de macrodados para determinar a resposta regulamentar mais equilibrada, proporcionada e justa. A IA, a Internet das coisas (IoT) e a desinformação em linha são algumas das questões complexas à espera de serem abordadas (União Internacional das Comunicações, 2020).

5.3.4.2 REGULAMENTAÇÃO CONSULTIVA E BASEADA EM PROVAS

Para aproveitar os conhecimentos especializados das partes interessadas, a regulamentação deve igualmente ser o resultado de processos consultivos de uma multiplicidade de participantes centrados no interesse público. Devem também ser baseadas em provas e contextos. A melhoria dos dados administrativos através de uma melhor recolha e análise, e sobre os quais os reguladores podem tomar decisões, melhoraria grandemente a tomada de decisões dentro das agências. Isto permitir-lhes-ia também proporcionar maior segurança às partes interessadas num quadro flexível e adaptável, aumentando a sua credibilidade (Banco Mundial e UIT, 2020).

RECOMENDAÇÕES

- Ao criar disposições institucionais, os Estados-membros devem distinguir claramente entre os papéis do Estado enquanto decisor político e o da entidade reguladora, que deve ser suficientemente independente do Estado e da indústria, de modo a implementar políticas de interesse público e dos prestadores de serviços e operadores de plataformas.
- As instituições reguladoras devem ser estabelecidas com base nos princípios de autonomia, transparência, prestação de contas para evitar a captura estatal e reguladora. Os reguladores devem realizar Avaliações de Impacto Regulamentar numa fase precoce da regulamentação para implementar as melhores abordagens que equilibrem a regulamentação e o crescimento económico. Os reguladores devem publicar o desempenho dos esforços políticos e regulamentares para melhorar as estratégias regulamentares em todos os Estados, incluindo relatórios de participação pública sobre regulamentações emergentes. Os reguladores devem igualmente ser autofinanciados ou financiados através de dotações parlamentares para permitir a independência financeira. As decisões regulamentares devem basear-se em dados de qualidade e aproveitar o conhecimento do sector privado e da sociedade civil através de consultas públicas. As autoridades reguladoras da concorrência e setoriais devem evitar uma regulação instrumental da concorrência, adotando modelos de eficiência dinâmica em vez de modelos de eficiência estática.

→ **AÇÕES**

- Distinguir claramente entre os papéis do Estado como decisor político e a entidade reguladora, que deve ser suficientemente independente do Estado e da indústria, de modo a implementar políticas de interesse público.
- Criar ou manter autoridades de concorrência para lidar com a posição dominante no mercado e a concentração resultante de fusões e aquisições.
- Implementar procedimentos claros de co-jurisdição entre as autoridades sectoriais e da concorrência para assegurar a regulamentação coordenada do sector das infraestruturas e serviços digitais e para evitar o recurso ao "forum shopping", ou seja, a procura do órgão jurisdicional mais conveniente.
- Os reguladores de dados devem colaborar a nível regional e continental para harmonizar os seus quadros, particularmente em apoio à ZCLCA.
- As pessoas sujeitas a decisões das autoridades reguladoras devem ter mecanismos claros de recurso e reparação ouvidos por um órgão diferente do regulador, tomando as decisões de acordo com as regras da justiça natural e da ação administrativa justa.

5.3.5 CRIAR VALOR PÚBLICO

Definição do problema

Ter dados sem a capacidade humana, o controlo suficiente ou incentivos para a sua valorização, é praticamente o mesmo que não ter dados. Estes condicionalismos verificam-se em muitos países africanos. Existem também desafios na promoção de um sector público baseado em dados. A valorização dos dados depende em grande medida da existência de quadros regulamentares e políticos que facilitem a obtenção de dados úteis, reforcem as capacidades humanas, institucionais e técnicas para criar valor a partir dos dados, incentivem a partilha e a interoperabilidade dos dados e aumentem a legitimidade e a confiança do público no Estado para gerir os dados dos cidadãos de forma responsável. Além disso, a infraestrutura de dados que permite um sistema integrado de dados é um ativo estratégico fundamental para os países. O ambiente criado pela interação dos elementos do ecossistema de dados e a natureza das relações e dos processos não lineares entre eles e no seu interior determinam as intervenções para criar incentivos aos investimentos tecnológicos necessários para impulsionar o crescimento da economia de dados. Estas condições são moldadas pela estrutura do mercado, pela competitividade dos serviços que dele resultam e pela eficácia da regulação do mercado.

5.3.5.1 CAPACIDADE DO SECTOR PÚBLICO

As capacidades digitais e de dados do sector público são um fator determinante para a prestação de serviços em muitas áreas prioritárias. A criação de condições para que os dados sejam otimizados no sector público a fim de responder mais eficazmente às necessidades dos cidadãos, são condições necessárias para a inclusão social e económica. No entanto, existem desigualdades multidimensionais e ineficiências políticas que se sobrepõem e que limitam as capacidades humanas e institucionais para reforçar uma cultura de empreendedorismo digital, fomentar comunidades de inovação digital inclusivas e promover mercados de ecossistemas de dados justos e equitativos, onde os Africanos com diferentes capacidades possam trabalhar com tecnologias digitais de ponta e contribuir para o ciclo de valor dos dados ou participar em cadeias de valor de dados de uma forma mais inclusiva.

Para que um sector público baseado em dados se concretize, a função pública tem de ser renovada com liderança e vontade política para garantir que os funcionários públicos a todos os níveis tenham um conhecimento básico do modo como os dados podem ser utilizados para melhorar a prestação de serviços e a aplicação de políticas. Além disso, um sector público assente em dados exige uma abordagem comum e um modelo arquitetónico de infraestrutura de dados que possa abordar a potencial integração e intercâmbio de dados e de aplicações assentes em dados entre sectores, aplicações e plataformas.

5.3.5.2 CURADORIA DE DADOS PÚBLICOS

O sector público está mandatado para gerir os principais dados sobre o desenvolvimento económico. Estes dados incluem dados estatísticos e indicadores económicos utilizados para fins de comunicação com instituições multilaterais e dados administrativos, como a identificação digital. Estes dados são frequentemente tornados anónimos e combinados com outros dados em vários casos de utilização desde a hiperpersonalização comercial, como a avaliação da capacidade de crédito, até ao interesse público em subsídios sociais e gestão de catástrofes.

A criação efetiva de valor com base em dados no sector público exige uma abordagem transversal coerente para compreender a importância dos dados e a forma como podem ser utilizados para melhorar os esforços socioeconómicos e a prestação de serviços públicos. A falta de consenso geral sobre os quadros de governação dos dados, complementados pelas melhores práticas sectoriais adequadas (dependendo do caso de utilização), pode comprometer significativamente a interoperabilidade e os esforços de partilha de dados abertos e criar limitações à medida em que os governos adotam práticas para criar valor a partir dos dados no sector público. Facilitar a interoperabilidade é uma condição essencial. Os sistemas de dados abertos requerem uma abordagem comum e modelos de infraestruturas de dados que possam abordar a potencial integração e intercâmbio inter-sectorial, inter-aplicações e inter-plataformas de dados legíveis por máquinas e aplicações baseadas em dados. A partilha de dados e a interoperabilidade não dependem apenas dos sistemas de dados, dos protocolos técnicos, da infraestrutura ou da governação dos dados, exigem também liderança e vontade política para que haja consenso em torno de uma abordagem à interoperabilidade que apoiada e adotada em vários mandatos do sector público.

No sector público, os dados são frequentemente utilizados para melhorar o contrato social e mitigar as assimetrias de informação na formulação de políticas, monitorizar os impactos da intervenção e a prestação de serviços, incluindo decidir como são atribuídos os recursos governamentais. Os dados públicos anonimizados podem ser combinados com outros conjuntos de dados para uso comercial para reduzir os custos de entrada no mercado, perturbar as indústrias, aumentar a eficiência e facilitar o desenvolvimento de inovações, produtos, informação e oportunidades que podem estar disponíveis virtualmente, sem as limitações das fronteiras geográficas e físicas. No entanto, as instituições que curam dados públicos enfrentam vários desafios que são discutidos abaixo.

5.3.5.3 GARANTIR A QUALIDADE E A RELEVÂNCIA DOS DADOS DO SECTOR PÚBLICO

Existem várias teorias ou modelos para estudar desafios relativos à qualidade dos dados. Como resultado, a definição de determinantes e a relevância da qualidade dos dados de uma perspetiva técnica é informada por uma ampla variedade de cenários de aplicação, como a

disponibilidade de dados, o tipo de dados, as características do domínio e como e porquê os dados são utilizados e/ou recolhidos, entre outros (Wang et al., 2019; Wook et al., 2021). Por exemplo, na investigação sobre a saúde, um quadro de avaliação da qualidade dos dados consistiria em 30 ou mais indicadores de qualidade de dados, enquanto para os sensores de qualidade de dados recolhidos a partir de dispositivos IoT apenas duas dimensões podem ser consideradas (Schmidt et al., 2021; Teh et al., 2020). Além disso, o advento de análises de macrodados, incluindo ML e capacidades técnicas para além da ciência dos dados, tais como engenharia e gestão de dados, significa que os dados são processados (limpos) e podem melhorar a qualidade dos dados recolhidos, tornando-os disponíveis para uma grande variedade de casos de utilização (Wook et al.,2021, Svolba, 2019).

Com sistemas de ensino não adaptados à realidade digital e, por conseguinte, com fracos meios de competências STEM e TIC e digitais, os talentos existentes são limitados para explorar plenamente as técnicas de análise de macrodados e a ciência dos dados para criar valor a partir de dados acumulados ou produzidos. A curadoria e a partilha inadequadas de dados em todo o sector público inibem o desenvolvimento de sistemas de dados integrados e os benefícios que lhes estão associados.

RECOMENDAÇÕES

- Dado o ritmo vertiginoso da digitalização, o sector público, enquanto principal guardião dos dados dos cidadãos, tem de dispor de recursos adequados para tirar partido dos dados a fim de reforçar os interesses públicos de uma forma que salvaguarde os cidadãos. Uma forma de o fazer é através de formação específica e de iniciativas de co-criação de conhecimentos com outras agências internacionais – as instituições com poucos recursos que fazem a curadoria de dados públicos já albergam profissões analíticas existentes (estatística, economia quantitativa, investigação operacional e investigação social, etc.). Estes recursos existentes podem ser melhorados e utilizados para aumentar a criação de valor dos dados no contexto do sector público.

- Os Estados-membros devem comprometer-se com toda uma abordagem governamental à utilização de dados em várias prioridades políticas e as entidades públicas que curam vários tipos de dados devem receber mandatos claros e ser dotadas de recursos com capacidade técnica, institucional e humana. Tal pode ajudar a garantir que são responsáveis pela gestão de dados de qualidade que podem ser partilhados e reorientados de uma forma responsável para casos de utilização múltiplos.

- Para promover a confiança na gestão pública de dados, os reguladores do sector e os administradores de dados públicos devem assegurar a colaboração com as partes interessadas da indústria. Dado que as avaliações da qualidade dos dados do sector privado estão frequentemente fora do controlo do sector público, os esforços de gestão de dados da indústria são mais adequados para a elaboração de leis e regulamentos que promovam a utilização de dados de alta qualidade. Isto é necessário para acomodar vários casos de utilização que requerem diferentes indicadores de avaliação da qualidade dos dados. Estas diretrizes de avaliação devem ser feitas através de esforços de múltiplos intervenientes – a governação de dados deve ser considerada no contexto das realidades operacionais de vários casos de utilização de dados, em todas as indústrias.

→ **AÇÕES**

- Os reguladores sectoriais e os administradores de dados públicos devem funcionar dentro de diretrizes específicas sobre como as avaliações da qualidade dos dados devem ser implementadas, dependendo dos casos de utilização comum, algoritmos, e tipo de dados utilizados, estas diretrizes podem ser informadas pelas melhores práticas globais (incluindo sobre dados e governação da IA) mas devem ser adaptadas ao contexto dos casos de utilização de dados africanos. O intercâmbio, as combinações, o armazenamento estratégico e o reaproveitamento são necessários para criar valor nos dados. Uma estratégia eficaz de qualidade de dados em todo o sector público deve ser informada por realidades técnicas/práticas/operacionais e deve delinear as funções, responsabilidades e mandatos de várias agências governamentais na recolha e manutenção de dados de alta qualidade de uma forma que salvaguarde os cidadãos.
- Os Estados-membros precisam de participar nos esforços para estabelecer e adotar um quadro normativo para normas e sistemas de dados harmonizados destinados a estabelecer a interoperabilidade nacional, regional e internacional. Estes podem incluir intervenções específicas de formação humana, técnica e institucional, projetos de infraestruturas sub-regionais, e caixas de areia regulamentares das CER.
- Uma abordagem continental facilita economias de escala para incentivar o investimento privado em infraestruturas digitais fundacionais, incluindo tecnologias baseadas na nuvem. A harmonização regional dos regulamentos para a governação de dados poderia reduzir ainda mais os custos de conformidade e reduzir a incerteza e o risco operacional para os principais investimentos em infraestruturas relacionadas com as TIC.
- As instituições públicas que curam dados devem ser dotadas de recursos adequados a fim de contribuírem em fóruns multilaterais no que diz respeito a dados e serem administradores de acesso inclusivo e utilização responsável dos dados, guiados por normas técnicas e regulamentares, padrões e melhores práticas adequadas da indústria – que sustentem tanto as características informativas como económicas dos dados nas indústrias prioritárias.

5.3.6 POLÍTICAS SECTORIAIS COERENTES PARA AUMENTAR O VALOR DOS DADOS

Definição do problema

As políticas de concorrência, comércio e fiscalidade estão significativamente interligadas. Economias de dados locais competitivas, por exemplo, podem aumentar os serviços baseados em dados, e a abertura comercial pode estimular o comércio digital internacional e o investimento direto estrangeiro (IDE) nas economias de dados nacionais. No entanto, isto também pode reforçar o domínio dos oligopólios globais nos ecossistemas de dados nacionais, criando tensões comerciais relacionadas com os fluxos de dados transfronteiriços. Simultaneamente, os modelos de negócio digitais baseados em dados podem minar a concorrência nacional e reforçar a concentração do mercado, uma vez que as autoridades da concorrência têm dificuldade em quantificar, valorizar, estabelecer e acompanhar as cadeias de valor digitais devido a características como os fornecedores terceiros e a ausência de presença física como base para estabelecer a responsabilidade fiscal das empresas no sector baseado em dados.

Para os Estados-membros, a ação coletiva através de uma abordagem unificada proporcionará mais provavelmente melhores resultados, captando os contextos africanos ao abor dar a concorrência, o comércio e os desafios fiscais nos mercados de dados.

5.3.6.1 POLÍTICA DE CONCORRÊNCIA

Definição do problema

As características dinâmicas dos modelos empresariais baseados em dados criam desafios para a implementação de instrumentos tradicionais de política de concorrência, para a aplicação efetiva das regras de concorrência, para as medidas corretivas e para a regulamentação das fusões nos mercados digitais. A resolução destes desafios requer intervenções preventivas no mercado e colaboração contínua com políticas complementares nomeadamente em matéria de proteção dos consumidores, comércio, industrialização e investimento.

A política de concorrência deve ter em conta não só os efeitos económicos das estruturas do mercado de dados, mas também os efeitos em termos de segurança e privacidade, nomeadamente para evitar a concentração de corretores ou plataformas de dados, uma vez que tal cria o risco de um ponto único de falha do mercado. Assim, a aplicação da regulamentação em matéria de concorrência, a regulamentação ex ante e a conceção de políticas têm de ser reajustadas para a economia de dados.

5.3.6.2 POLÍTICA DE COMÉRCIO

Definição do problema

Os sistemas digitais já não funcionam dentro de jurisdições nacionais claramente definidas. A reforma da política comercial é necessária para orientar o crescente comércio digital e o comércio eletrónico. As diferentes influências geopolíticas, as dotações e as capacidades institucionais e humanas no continente podem ter influência nas abordagens unilaterais ao comércio digital e nos esforços de harmonização regional. A estratégia de dados transfronteiriços adotada a nível interno exigirá diferentes capacidades institucionais, só poderá ser eficaz com base nas dotações existentes do ecossistema de dados, influenciará a forma como o valor dos dados será criado ou extraído dentro e entre países africanos, e determinará quem beneficiará mais do ciclo de valor dos dados a nível interno e regional. Além disso, os fatores "offline", como a infraestrutura rodoviária física, a fiabilidade dos serviços de correio, a logística e a eficiência da cadeia de abastecimento, entre outros, são fatores cruciais que facilitam o comércio digital e o comércio eletrónico.

COMÉRCIO DE SERVIÇOS, FLUXOS DE DADOS TRANSFRONTEIRIÇOS E LOCALIZAÇÃO

Para que o comércio digital ocorra, os dados têm de ser transferidos para além das fronteiras. Embora a acumulação de dados possa ser uma forma segura de gerir dados, o açambarcamento de dados sem meios para os utilizar, trocar, ou redirecionar de uma forma segura pode também criar riscos de subutilização que podem diminuir a eficiência e limitar outros benefícios do comércio digital. A proteção dos dados nacionais e os regulamentos não afetam apenas as oportunidades de negócios locais, mas também o comércio intrarregional e a participação na economia digital global baseada em dados.

Enquanto os dados não pessoais são utilizados e trocados além-fronteiras, a importância dos dados gerados pelos utilizadores e dos serviços digitais como contributos em várias atividades industriais fornece um enorme campo de ação para aumentar as exportações de serviços digitais. Os serviços são igualmente contributos em muitos produtos manufaturados e em diferentes cadeias de valor de dados. Por esta razão, surgiram três regimes gerais

comuns de gestão de dados estilizados para os fluxos transfronteiriços de dados pessoais, que variam em termos de abertura, intervenção necessária, e atores responsáveis. Existem também variações dos três modelos estilizados, consoante o tipo de dados e o caso de utilização. Muitas vezes, os dados sensíveis, tais como dados pessoais, têm requisitos de dados transfronteiriços mais rigorosos do que os dados não pessoais. As regras e normas de proteção de dados também podem ser incorporadas em regulamentos sectoriais nas indústrias altamente regulamentadas, como a saúde e as finanças, que exigem avaliações de qualidade e considerações éticas mais rigorosas.

A escolha de um regime transfronteiriço estilizado de proteção de dados em detrimento de outro deverá estabelecer o equilíbrio entre a promoção de um desenvolvimento económico equitativo e o fornecimento de garantias adequadas em matéria de dados. Os Estados-membros precisam de compreender os efeitos económicos dos diferentes regimes transfronteiriços de gestão de dados, com base nas suas realidades económicas e prioridades de desenvolvimento.

Além disso, dadas as deficiências de infraestruturas de dados para muitos países africanos no que diz respeito ao armazenamento e acesso a grandes quantidades de dados, enquanto os serviços de dados em nuvem são uma alternativa mais rentável à criação e funcionamento de um centro de dados físicos, exigem determinados fatores que acomodem um ambiente de fornecimento e consumo de serviços em nuvem. Em última análise, as disposições transfronteiriças para serviços de computação em nuvem e centros de dados, tais como privacidade de dados, segurança e restrições sobre onde os dados são alojados (requisitos de localização), precisam de ser decididas tendo em consideração as prioridades de desenvolvimento económico mais amplas.

O quadro abaixo resume os principais prós e contras de cada regime de governação de dados, para ajudar os decisores políticos a decidir qual a melhor abordagem a seguir no contexto das suas prioridades soberanas e de desenvolvimento.

Três abordagens genéricas para governar os fluxos de dados transfronteiriços

Regime de governação de dados transfronteiriço	Descrição	Prós	Contras	Suposições
Regime de transferências abertas	Requisitos de aprovação obrigatória prévia relativamente baixos e o sector privado informa voluntariamente a livre circulação de dados (por exemplo, EUA, APEC)	Um fardo regulamentar mínimo permite uma maior flexibilidade na circulação dos dados Principalmente adequado para a comercialização de serviços digitais e a criação de valor dos dados A privacidade é um direito do consumidor	Risco de proliferação de diferentes normas entre as empresas e jurisdições, sem garantir quaisquer normas mínimas para a proteção de dados pessoais Requer a capacidade técnica, humana e institucional para monitorizar as empresas privadas e aplicar a responsabilização ex post Os direitos dos titulares dos dados são limitados - falta de consentimento para a utilização de dados pessoais	Sistemas de dados e infraestruturas interoperáveis Capacidade humana, técnica e institucional para criar valor a partir dos dados Pré-condições fortes (facilitadores) para impulsionar a economia digital baseada nos dados Titulares de dados com capacidades digitais para dar o seu consentimento
Regime de transferências condicionais	Salvaguardas de dados regulamentares estabelecidas numa base consensual e orientações regulamentares abrangentes por parte das autoridades de proteção de dados ou acordos internacionais (por exemplo, RGPD)	Oferece um maior equilíbrio entre a proteção de dados e a necessidade de abertura das transferências de dados com vista à criação de valor Encoraja a criação da autoridade nacional de processamento de dados (ANTD) Linhas de orientação claras e salvaguardas regulamentares obrigatórias que, depois de cumpridas, permitem a livre circulação de dados transfronteiras	Baseado em direitos fortes dos titulares de dados Determinadas condições têm de ser cumpridas ex ante Pode perpetuar os encargos de conformidade e os estrangulamentos do comércio digital	O mesmo que acima Influência da colaboração internacional para impor as condições ex ante
Modelo de transferências limitadas	Os fluxos de dados transfronteiriços são condicionais, baseando-se na aprovação governamental e nos requisitos de localização para armazenamento ou processamento de dados a nível nacional (por exemplo, China, Rússia)	Com base numa forte segurança nacional e em imperativos de controlo dos dados públicos	Aprovação regulamentar restritiva para transferências de dados internacionais e pode exigir a localização de dados explícita ou implícita e o armazenamento obrigatório	O mesmo que acima

Fonte: A própria interpretação resumida do autor de Ferracane e van der Marel (2021), WDR (2021).

COMÉRCIO ELECTRÓNICO

As plataformas de comércio eletrónico permitem aos consumidores beneficiar de uma maior variedade de escolhas a preços mais competitivos. As estratégias para melhorar o comércio eletrónico não podem ser formuladas isoladamente, uma vez que o comércio eletrónico se cruza com uma multiplicidade de outras questões, incluindo a Identificação Digital, a governação de dados, os direitos aduaneiros, os fluxos de dados transfronteiriços, a segurança cibernética, a interoperabilidade dos sistemas de pagamentos, a proteção do consumidor,[12] a concorrência, a fiscalidade e as normas, para citar algumas. Além disso, a melhoria da adoção do comércio eletrónico requer a abordagem de fatores como a penetração da Internet, a fiabilidade postal, a utilização dos serviços de pagamentos (contas bancárias ou dinheiro móvel) e servidores da Internet seguros.[13] Para os Estados-Membros, a ação coletiva através de uma abordagem unificada terá mais probabilidades de produzir resultados melhores que tenham em conta os contextos africanos ao abordar desafios que se sobrepõem e que afetam os diferentes mandatos governamentais nos mercados de dados em fóruns multilaterais.

Os acordos comerciais, por si só, não são instrumentos adequados para a governação transfronteiriça dos dados. A atual abordagem comum da utilização de acordos comerciais para regular os fluxos de dados transfronteiriços não conduziu a regras vinculativas, universais ou interoperáveis regendo Para os Estados-Membros, a ação coletiva através de uma abordagem unificada terá mais probabilidades de produzir resultados melhores que tenham em conta os contextos africanos ao abordar desafios que se sobrepõem e que afetam os diferentes mandatos governamentais nos mercados de dados em fóruns multilaterais. No entanto, no contexto da ZCLCA, uma abordagem harmonizada e coordenada para enfrentar os desafios associados à publicação de dados no mercado interno contribuirá para um melhor alinhamento com vários esforços sobrepostos de coordenação intrarregional do comércio digital e do comércio eletrónico para além dos próximos protocolos comerciais de comércio eletrónico[14] e serviços[15] previstos na estratégia.

RECOMENDAÇÕES

- Para favorecer ecossistemas de dados competitivos, seguros, fiáveis e acessíveis, as autoridades da concorrência precisam de encontrar formas coordenadas e eficazes de regular a concentração, preservando simultaneamente os benefícios que as empresas dominantes oferecem no contexto de diferentes necessidades de desenvolvimento em todo o continente. Isto inclui a regulamentação ex-ante de questões de concorrência antes que estas se intensifiquem no mercado.
- Os decisores políticos no panorama fiscal, concorrencial e comercial terão de criar capacidade humana e técnica para abordar questões emergentes que podem afetar os mercados orientados por dados, para além do tradicional mandato sectorial.

12 Proteção do consumidor online e devoluções de produtos, segurança do consumidor e responsabilidade do fornecedor.
13 *https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d12_en.pdf*
14 O protocolo de comércio eletrónico da ZCLCA é um instrumento importante para preservar o mercado africano consolidado na esfera digital, e exclui outros acordos que possam potencialmente prejudicar a agenda de liberalização e integração. Espera-se que as diretrizes sejam finalizadas na Fase III das negociações da ZCLCA.
15 A fase II da ZCLCA pretende abordar o comércio de serviços, os direitos de propriedade intelectual, o investimento e a política de concorrência

- Os Estados-membros devem promover a previsibilidade e a convergência de regimes em áreas políticas complementares, de uma forma que se reforce mutuamente. Isto tem de ser feito para navegar na emergência de novos modelos de negócios dinâmicos orientados para os dados que possam fomentar o comércio digital intra-africano e o empreendedorismo com base em dados. Ao mesmo tempo, os decisores políticos devem considerar as ligações bidirecionais entre os resultados económicos e a governação dos dados e ponderar cuidadosamente as soluções de compromisso.
- Os Estados-membros devem promover uma abordagem regional coordenada, abrangente e harmonizada dos desafios da governação global associados à economia digital global baseada em dados, por exemplo favorecendo:
  - A colaboração transfronteiriça na implementação de instrumentos de política de concorrência para abordar comportamentos anti concorrenciais em mercados digitais orientados para a informação;
  - A portabilidade dos dados através de regulamentação e outras atividades facilitadoras;
  - os esforços da Organização para a Cooperação e Desenvolvimento Económico (OCDE) para evitar a evasão fiscal em relação às empresas orientadas por dados;[16]
  - Acordos da Organização Mundial do Comércio (OMC) em matéria de serviços baseados em dados e comércio eletrónico;
  - O estabelecimento de infraestruturas regionais coordenadas de dados fundacionais e iniciativas de desenvolvimento de sistemas de dados digitais;
  - O reforço da capacidade humana, técnica e institucional para apoiar a interoperabilidade dos dados, a criação de valor, e a participação equitativa nas economias de dados; e
  - A contribuição na harmonização internacional das normas técnicas relativas à ética, governação, melhores práticas em matéria de dados, análises macrodados e IA.

→ AÇÕES

- Os Estados-membros devem encorajar uma reforma política e regulamentar dinâmica e a experimentação (por exemplo, através de caixas de areia regulamentares a nível da indústria e das CER).
- Os decisores políticos devem ter em conta as ligações bidirecionais entre os resultados económicos e a governação dos dados e ponderar cuidadosamente as soluções de compromisso. As entidades estatais individuais devem esforçar-se por estabelecer quadros de partilha de dados seguros e responsáveis que satisfaçam a procura de dados, facilitem a interoperabilidade dos dados, os fluxos de dados transfronteiriços e as cadeias de valor dos dados, bem como normas e sistemas de dados abertos em áreas prioritárias fundamentais identificadas pela Estratégia de transformação digital. Caso sejam impostas medidas corretivas, estas devem basear-se numa análise económica que tenha em conta os impactos a longo prazo nos incentivos ao investimento e à inovação.

16 *https://www.oecd.org/tax/beps/*

- Para que a utilização de dados seja eficiente, inclusiva e inovadora, serão necessárias uma colaboração entre instituições reguladoras em diferentes mandatos e uma regulação coordenada do mercado (em áreas políticas interrelacionadas, tais como telecomunicações, concorrência, comércio, fiscalidade e regulamentação dos dados).
- As autoridades de concorrência ou instituições relacionadas terão de criar a capacidade humana e técnica necessária para abordar questões de concorrência emergentes que possam afetar os mercados orientados por dados para além da concentração do mercado.
- Os instrumentos tradicionais da concorrência, tais como diretrizes sobre definições de mercado, avaliação de posição dominante, práticas anti concorrenciais (por exemplo, abuso de posição dominante, práticas coordenadas, e abuso do poder de compra), avaliação de concentrações, e teorias de danos e conceção de soluções terão de ser ajustadas para incorporar o dinamismo dos dados e as características das empresas baseadas em dados.
- Os signatários da ZCLCA terão de determinar de que forma o protocolo de comércio eletrónico funcionará em paralelo com as leis e políticas existentes e terão de ter em conta e apoiar os objetivos dos outros protocolos, tais como o investimento, a propriedade intelectual e a política de concorrência (a negociar na Fase II).
- Desenvolver e reforçar os mecanismos de diálogo público-privado para melhorar a elaboração de políticas relacionadas com o comércio eletrónico.

5.3.6.3 POLÍTICA FISCAL

Definição do problema

Existe uma incoerência entre a atual tributação dos lucros das plataformas globais e a forma como o valor é criado a partir dos dados na economia digital. Em África, a maioria dos países são essencialmente mercados de dados para plataformas globais, com os utilizadores a contribuírem significativamente para a geração de lucros das plataformas sem que exista um mecanismo plausível de captura de valor. Atualmente, o tráfego de dados em África está a crescer a uma taxa anual de 41% (CNUCED, 2019), o que implica uma maior utilização e adoção dos serviços prestados pelas plataformas digitais globais na região. Embora as instituições multilaterais se tenham empenhado, principalmente impulsionadas pelo Quadro Inclusivo da OCDE sobre a Erosão da Base e a Transferência de Lucros (BEPS) (embora não seja totalmente inclusivo para África, uma vez que apenas 23 países participam), não se chegou a um consenso global para as diferentes opções propostas (Pilares 1 e 2) para a tributação digital.

Vários países africanos, relutantes em atrasar a tributação dos serviços digitais ou não convencidos dos benefícios das reformas internacionais para os seus países já estão a implementar mecanismos unilaterais. Estes incluem impostos sobre serviços digitais e taxas de equalização baseadas em dados económicos significativos para captar parte do valor dos dados através da tributação de algumas partes da economia digital dentro das suas jurisdições. Estes mecanismos incluem também a expansão da tributação específica do sector na indústria das telecomunicações, a tributação das transações de dinheiro móvel e a utilização de algumas aplicações de comunicação over-the-top (OTTs) na região, tais como a WhatsApp, Facebook, Twitter, Skype e Instagram. Embora estes impostos se destinem a aumentar as receitas governamentais, o seu impacto negativo nos consumidores atrasou o acesso e a inclusão digitais (devido à transferência dos custos para os consumidores) e restringiu o direito

dos cidadãos à liberdade de expressão. Do lado da oferta, o aumento dos impostos sobre o sector das telecomunicações tem um impacto negativo nos lucros dos operadores do sector residente (com consequências negativas para o tão necessário investimento em infraestruturas na região com recursos limitados), enquanto os OTT baseados em dados não são, em grande medida, tributados a nível local (CTO, 2020; ICTD, 2020; RIA, 2021).

Do ponto de vista da soberania e dos benefícios fiscais, todos os países têm o direito de tributar os lucros das plataformas digitais globais quando estas interagem economicamente com os seus cidadãos e residentes (em grande parte através da venda dos seus dados pessoais). No entanto, apesar de milhões dos seus cidadãos e residentes utilizarem aplicações de dados geridas por plataformas digitais globais, os países africanos, ao abrigo do atual regime fiscal internacional, não têm o nexo necessário para tributar os lucros destas entidades. Embora algumas das plataformas tenham uma certa forma de presença local nos países africanos, estas filiais são meros serviços de apoio administrativo e não detêm legalmente os ativos destas plataformas (que são em grande parte intangíveis e atualmente não estão incluídos nas propostas da maioria das fórmulas de atribuição), pelo que não recebem qualquer rendimento acumulável sobre os ativos.

Mais ainda, as diferentes propostas fiscais para a economia digital – que incluem repartições de fórmula, aplicação de Presença Económica Significativa (SEP), e a utilização de mecanismos indiretos como o imposto sobre o valor acrescentado (IVA) e mais retenção direta na fonte (WHT) – requerem todas o acesso a dados de transações, as quais as plataformas digitais globais não estão atualmente dispostas a partilhar (especialmente em mercados não residentes). Mesmo nos casos em que alguns destes dados são acedidos, terão de ser verificados e validados.

As recentes medidas legislativas e políticas introduzidas por alguns países africanos no contexto de vários esforços multilaterais e unilaterais para tributar a economia digital podem não ser conducentes à criação de um mercado único ou ao acesso a recursos internacionais para alcançar bens públicos mundiais e cumprir algumas das condições prévias para uma economia de dados competitiva no continente. A exploração de novas fontes de receitas fiscais poderia permitir aos países africanos eliminar os impostos especiais de consumo sobre as redes sociais e os serviços de dados, reduzindo as distorções tanto no mercado local como no sistema fiscal mundial.

RECOMENDAÇÕES

Os governos africanos têm de aumentar as atividades económicas dentro das suas jurisdições que tirem partido dos mecanismos de digitalização e de dataficação, uma vez que o aumento da competitividade nesta área irá multiplicar o potencial de aumento das receitas fiscais. Este processo exigirá o desenvolvimento de mais empresas locais baseadas em dados como parte da política industrial da região. Esta via pode ajudar a mitigar os riscos de cumprimento fiscal que são amplificados na situação atual em que uma parte significativa dos dados públicos na região é capturada e controlada por empresas de dados estrangeiras (Khan & Roy, 2019).

→ **AÇÕES**

- Os Estados-membros devem apoiar a harmonização do regime fiscal para bens e serviços digitais a nível regional, e o alinhamento a nível global, mitigar os riscos associados ao facto de os mercados de pequenas economias de dados não serem capazes de gerar valor significativo e competir nos mercados globais para contribuir para a escala e o âmbito necessários para a criação de valor baseada em dados e com bases fiscais geralmente limitadas.
- De forma complementar, poderia ser criado um fundo público de dados cofinanciado pelos países membros da UA, em colaboração com o sector privado, para construir a infraestrutura necessária para extrair estes dados de transações, onde os dados podem ser armazenados como parte de um fundo comum de dados regionais para além do domínio exclusivo da tributação.
- A criação de um fundo comum de dados públicos exigirá que os países africanos digitalizem os seus sistemas de administração fiscal para permitir uma avaliação e uma cobrança mais eficazes dos impostos provenientes das plataformas digitais. Um sistema de administração fiscal digital melhorará a capacidade de registo fiscal, a partilha de dados de transações com as autoridades fiscais nacionais e o intercâmbio de informações sobre obrigações fiscais com plataformas digitais para efeitos de conformidade, reduzindo simultaneamente os custos operacionais.
- Os Estados-Membros devem aproveitar a oportunidade de coordenar a tributação dos serviços digitais num mercado digital único para explorar novas fontes de receitas fiscais que lhes permitam eliminar os impostos especiais de consumo regressivos e contraproducentes do ponto de vista fiscal sobre as redes sociais e os serviços de dados e reduzir as distorções tanto no mercado local como no sistema fiscal mundial.

5.4 GOVERNAÇÃO DE DADOS

Para que a política de governação de dados seja eficaz, deve incentivar um ecossistema onde existam esforços de múltiplos intervenientes para melhorar o acesso e a utilização dos dados. Deve ser também encorajada a reordenação e combinação de dados de forma a limitar os danos e riscos associados aos processos de datafication, assegurando ao mesmo tempo que uma grande variedade de dados seja utilizada ao seu maior potencial económico e social. Algumas destas políticas envolvem a disponibilização de dados enquanto outras procuram restringir os fluxos de dados (Macmillan, 2020).

5.4.1 CONTROLO DE DADOS

Facilitar o controlo de dados para empresas e governos é um mecanismo importante para a extração do valor dos dados (Carrière-Swallow & Haksar, 2019; Couldry & Mejias, 2018; Savona, 2019, p. 201). A política ajuda a limitar a forma como o controlo pode ser exercido, mas também incentiva mecanismos de controlo que se alinhem com os objetivos estratégicos de uma política de dados. Um papel importante para a política é ajudar a garantir a clareza em termos de controlo para a atribuição de obrigações e responsabilidades (Carrière-Swallow & Haksar, 2019; Zuboff, 2018).

5.4.1.1 SOBERANIA DE DADOS

O controlo de dados também pode ser entendido a nível nacional em relação à soberania dos dados (Ballell, 2019). A soberania dos dados baseia-se no conceito de Estado-nação soberano e refere-se à visão de que os dados gerados ou que passam pela infraestrutura nacional da Internet devem ser protegidos e controlados por esse Estado (Razzano, Gillwald, et al., 2020). No contexto digital, pode ser entendida no sentido de um subconjunto da soberania cibernética definida como a sujeição do domínio cibernético (global por definição) a jurisdições locais (Polatin-Reuben & Wright, 2014). Existem duas abordagens à soberania dos dados, a soberania fraca e a soberania forte. A soberania de dados fraca refere-se a iniciativas de proteção de dados lideradas pelo sector privado, que se centra nos aspetos de direitos digitais da soberania de dados. A soberania forte dos dados, por outro lado, favorece uma abordagem liderada pelo Estado que se centra na salvaguarda da segurança nacional (Polatin-Reuben & Wright, 2014).

Em geral, a transferência de dados pessoais para um outro país terceiro só é permitida sob determinadas condições, por exemplo, quando outro país terceiro tem uma lei que exige garantias suficientes (incluindo o respeito da privacidade e a segurança) para o processamento de dados pessoais. Os Estados exercem frequentemente a soberania dos dados para a proteção dos direitos dos seus cidadãos, por exemplo, através de regimes de proteção de dados que regulam os fluxos transfronteiriços de dados para proteger os direitos das pessoas em causa, muitas vezes através de acordos que estabelecem normas de proteção de dados e proteção recíproca dos dados trocados. Embora sejam necessárias normas jurídicas suficientes para a reciprocidade, também é necessária a capacidade prática dos Estados para aplicarem as normas mutuamente acordadas. A implementação de boas práticas de governação de dados é um passo fundamental para alcançar a soberania dos dados.

5.4.1.2 LOCALIZAÇÃO DE DADOS

Definição do problema

Embora a localização dos dados seja frequentemente vista como uma expressão da soberania do Estado, enquanto opção política possível, tem de ser avaliada numa base de custo-benefício. Esta opção política pode representar um desafio prático. Embora a localização dos dados seja por vezes motivada pela necessidade de proteger as pessoas em causa, a localização de dados pode ser aplicada a dados não pessoais. É por isso que é essencial que a localização de dados seja lida no contexto do controlo, a fim de sublinhar politicamente a importância dos mecanismos de apoio que podem facilitar o ato de soberania.

A localização de dados envolve a criação de barreiras legislativas artificiais aos fluxos de dados, nomeadamente através de requisitos de residência de dados e de armazenamento local obrigatório de dados (Cory, 2017). Regras rigorosas de localização de dados que exigem que todos os dados sejam armazenados localmente, e não apenas copiados, sujeitam esses dados a ameaças à segurança, incluindo ciberataques e vigilância estrangeira.

Alguns países africanos enfrentam graves limitações na sua capacidade tecnológica, pelo que a procura de capacidade de localização pode exceder largamente a capacidade dos centros de dados nacionais. Concomitantemente, os requisitos de cópias duplicadas de dados podem impor obrigações financeiras indevidas às empresas locais.

RECOMENDAÇÕES

- Os Estados-membros devem dar prioridade a parcerias politicamente neutras que tenham em conta a sua soberania individual e propriedade nacional para evitar interferências estrangeiras que possam afetar negativamente a segurança nacional, os interesses económicos e o desenvolvimento digital dos Estados-membros da UA.
- Os Estados-membros da UA têm o direito de formular regras digitais e de dados de acordo com as suas prioridades e interesses, nomeadamente para proteger a segurança da informação do Estado e dos seus cidadãos, e para impedir que terceiros explorem injustamente os seus recursos e mercados locais.
- É necessário estabelecer acordos bilaterais e multilaterais para exercer a soberania e o controlo internos, sendo necessárias vias de recurso para as infrações.
- A localização precisa ser avaliada contra possíveis danos aos direitos humanos.
- Os requisitos de localização de dados requerem a especificidade dos dados. As soluções de localização de dados têm sido fortemente articuladas dentro de silos de dados sectoriais (verticais) em diferentes jurisdições; a Nigéria, por exemplo, instituiu certas formas de localização de dados financeiros, a Austrália prescreveu formas de localização de dados de saúde, etc. Esta é uma área em que a especificidade é fortemente necessária, tanto para facilitar fluxos mais amplos, na medida em que é conducente a imperativos políticos como a Zona de Comércio Livre Continental Africana, mas também para a clareza que pode ajudar a minimizar os custos para as empresas e inovadores locais e reduzir os riscos de consequências involuntárias.
- A política de dados exige clareza, o que implica não só especificidade, mas também uma categorização dos dados, que pode permitir aos Estados-Membros exercerem a sua soberania através do estabelecimento, por exemplo, de classificações de segurança ou de níveis específicos de sensibilidade dos dados. Estes devem ser aplicados de forma coerente em toda a política de dados (e de informação).
- O desenvolvimento de infraestruturas de dados deve ser explorado como um mecanismo para exercer controlo, mas deve ser contextualizado tendo em consideração os impactos ambientais, as infraestruturas de segurança e proteção, os custos duplicados para as comunidades de dados locais, e os custos globais.
- As capacidades do sector público devem ser investidas para informar iniciativas nacionais eficazes de monitorização de dados.
- Os direitos da pessoa em causa devem prever expressamente um controlo eficaz dos dados pessoais. Os fideicomissos de dados e as diligências devem ser explorados como outra forma de controlo eficaz dos dados pessoais (e outros dados).

→ AÇÕES

- As autoridades de proteção de dados (APD) necessitam de uma total capacitação, o que inclui a competência em matéria de soberania de dados.
- As APD são incentivadas a adotar práticas de cooperação internacional e regional, tendo em conta as diferentes fases de implementação e aplicação nos Estados-Membros;
- A avaliação de riscos e o envolvimento de várias partes interessadas devem ser utilizados para conceber soluções para a localização de dados nas políticas pelos redatores, incluindo a participação da sociedade civil;
- A política de infraestruturas de dados deve estar alinhada com os imperativos de controlo de dados dos redatores de políticas, mas deve ter em conta a segurança cibernética, a privacidade dos dados, os riscos ambientais e os custos;
- A administração pública e a política de investimento devem alinhar-se prioritariamente com as capacidades de controlo de dados.
- O desenvolvimento de capacidades em matéria de proteção de dados, segurança cibernética e governação institucional de dados nas organizações relevantes deve ser assegurado através de políticas e da atribuição de ativos.

MECANISMOS PARA EXERCER O CONTROLO DE DADOS

Existem mecanismos para exercer controlo sobre os dados, como os fideicomissos de dados. Os fideicomissos de dados e/ou a gestão de dados são formas alternativas de soluções de governação discreta no contexto dos dados. Um fideicomisso legal ou "legal trust" é um instrumento jurídico utilizado para gerir ativos, tanto tangíveis como intangíveis. Um fideicomisso permite que uma pessoa detenha ativos (de que não é proprietária) em benefício dos beneficiários do fideicomisso. A pessoa que detém os ativos foi autorizada e tem para com os beneficiários do fideicomisso o dever fiduciário de agir de forma responsável na gestão dos seus ativos. Esta estrutura jurídica tradicional tem sido apresentada como um meio de gerir coleções de dados em nome de grupos e de facilitar a partilha maciça de dados em situações em que os modelos de licenciamento ou de dados abertos podem não ser viáveis, como um meio de promover a inovação ao facilitar o acesso equitativo (Stalla-Bourdillon et al., 2019).

O Open Data Institute define os fideicomissos de dados como sendo "...a gestão independente e fiduciária dos dados" (Open Data Institute, 2018). O elemento fiduciário foi acrescentado à definição (em vez de a definir simplesmente como uma forma de confiança legal), uma vez que é um elemento essencial de responsabilidade e obrigação, que é uma base importante do conceito (Open Data Institute, 2020). Além disso, pode incluir soluções de privacidade através da conceção na arquitetura de qualquer mecanismo concebido para facilitar a confiança, garantindo assim a privacidade em substância e processo (Stalla-Bourdillon et al., 2019). Embora as leis de proteção de dados possam criar normas sobre a forma como os dados de um indivíduo podem ou não ser tratados, fora do consentimento ou da reparação de violações, os mecanismos para os indivíduos agirem sobre os seus dados são limitados - assim, os fideicomissos de dados ajudam a facilitar a realização do controlo dos dados. Os fideicomissos de dados oferecem aos titulares dos dados um mecanismo através do qual podem fornecer (ou "partilhar") os seus dados, ao mesmo tempo que eliminam a responsabilidade exclusiva de "assegurar" o cumprimento da proteção de dados por parte dos intervenientes dos sectores público e privado através do estabelecimento de uma relação fiduciária.

5.4.2 PROCESSAMENTO E PROTECÇÃO DE DADOS

Definição do problema

Enquanto os princípios de controlo de dados ajudam a delimitar e a definir as obrigações relativas aos dados pessoais e não pessoais, os princípios de processamento de dados visam definir as orientações políticas para o processamento de dados pessoais, como vimos acima. A regulamentação dos dados não pessoais é determinada pela categorização dos dados e por regimes de acesso específicos.

Estas formas de orientação são importantes enquanto mecanismo para a realização da privacidade e proteção de dados. O processamento de dados pessoais é uma componente crítica da governação de dados e da promoção de um ambiente de confiança. A construção da confiança é entendida como um elemento necessário para a promoção de dados sólidos e da economia digital. O facto de restringir as limitações do processo aos dados pessoais, permite que estas restrições não impeçam os fluxos de dados para o comércio digital; mas para garantir esta ausência de impedimento, é necessário ter políticas de dados consistentes em toda a região, baseadas em princípios comuns, mas flexíveis (Nações Unidas, 2017).

Os direitos da pessoa em causa, como aspeto do processamento de dados pessoais, também oferecem benefícios acessórios para ajudar a garantir a integridade e qualidade dos dados.

No desenvolvimento de tecnologias e sistemas digitais, pode ser adotada uma abordagem de privacidade desde a conceção, segundo a qual a privacidade será integrada na tecnologia e nos sistemas por defeito durante o processo de conceção e desenvolvimento (Cavoukian, 2009). Isto pode implicar, por exemplo, a incorporação da minimização na recolha de dados ou a automatização de uma anonimização rígida. Tal significa que um produto deve ser concebido tendo como prioridade a proteção da privacidade, a par dos outros objetivos prosseguidos pelo sistema. Esta conceção deve incorporar uma compreensão particular do modo como as pessoas utilizam os produtos e da sua capacidade de fazer valer o seu direito à privacidade.

As técnicas de desidentificação, incluindo a anonimização e a utilização de pseudónimos, podem facilitar algumas utilizações dos dados, proporcionando ao mesmo tempo uma proteção de dados pelo menos parcial. A pseudonimização pode ser realizada através da utilização de um significante ou máscara que só pode ser ligada a um indivíduo identificável por meio de dados adicionais. Embora tanto a anonimização como a pseudonimização possam permitir aos prestadores de serviços privados e ao sector público uma maior utilização de dados, estes dependem do estado atual da tecnologia e da matemática. À medida que novas abordagens matemáticas são desenvolvidas e o poder de processamento informático aumenta, os dados que foram considerados desidentificados podem tornar-se identificáveis. Embora os regulamentos de proteção de dados exijam frequentemente a desidentificação, estas técnicas são insuficientes senão houver fortes direitos legais para as pessoas em causa e um regulador com capacidade para fazer cumprir a proteção de dados.

RECOMENDAÇÕES

- É necessário criar APDs independentes, financiadas e eficazes. Além disso, para garantir a eficácia, são essenciais medidas de responsabilização que ajudem a APD a definir claramente o seu âmbito de ação. Devem ser estabelecidos quadros para o tratamento legal de dados com sanções dissuasivas claras para garantir o seu cumprimento. Devem abranger todos os intervenientes relevantes no tratamento de dados.
- A avaliação dos riscos associados aos dados pessoais deve ser obrigatória aquando da implementação do desenvolvimento tecnológico dos dados pessoais.
- Um subprincípio importante, que tem de ser acionado com quadros de processamento de dados para os intervenientes públicos e privados, é o da minimização. A minimização da recolha de dados pessoais é um dos mecanismos mais eficazes para atenuar os riscos e os danos dos dados.
- Os códigos de conduta devem ser explorados para promover dados e necessidades específicas do sector. Tais Códigos, aprovados pela APD pertinente, podem fornecer conhecimentos sectoriais e industriais especializados na gestão dos riscos e danos reais que podem estar associados ao processamento, e assegurar as melhores práticas na gestão desses danos. Pode também ajudar a considerar as exceções sectoriais que podem ser necessárias para que uma economia de dados construtiva possa prosperar, mas também contribuir para uma agenda de Desenvolvimento Sustentável mais ampla, tal como através da pronta facilitação da investigação (na área da saúde, ou outros domínios de desenvolvimento social).

→ AÇÕES

- Os quadros de tratamento de dados devem ser estabelecidos em parceria com todos os parceiros relevantes, mas idealmente liderados pela APD. Estes quadros devem ser alinhados com os seguintes princípios: consentimento e legitimidade, limitação da recolha, especificação da finalidade, limitação da utilização, qualidade dos dados, garantias de segurança, abertura (que inclui a comunicação de incidentes, uma correlação importante com os imperativos de segurança cibernética e de cibercriminalidade), responsabilidade e especificidade dos dados.
- As APD devem ser estabelecidas com urgência juntamente com as legislações nacionais sobre proteção de dados pessoais.

5.4.3 ACESSO AOS DADOS E INTEROPERACIONALIDADE

Definição do problema

O acesso e a acessibilidade aos dados são entendidos tanto em termos de formas reativas de acesso facilitadas por leis e regulamentos, como através de formas proactivas de acesso a dados (como através de dados públicos abertos) (Open Data Charter, 2015). A acessibilidade também implica a partilha de dados entre agentes ou departamentos, um benefício importante da natureza inigualável dos dados. No entanto, isso requer interoperacionalidade entre esses diferentes agentes (Jones &Tonetti, 2020). No contexto da concorrência, os dados não são facilmente transferíveis de forma a facilitar os efeitos de escala entre empresas (Rinehart, 2020). A exigência de formas de portabilidade dos dados continua a ser uma estratégia regulamentar fundamental para facilitar a concorrência e os benefícios para os consumidores, embora as realidades ainda não tenham sido estabelecidas como definitivamente benéficas (Mitre-

todis & Euper, 2019; Rinehart, 2020). Do ponto de vista da privacidade, para além das simples alterações de interoperabilidade, a natureza da recolha de grandes volumes de dados significa que a portabilidade dos dados tem impacto na privacidade de outros utilizadores (Nicholas & Weinberg, 2019).

RECOMENDAÇÕES

- Deve ser dada prioridade às normas de dados abertos na criação e manutenção de dados públicos. A criação de dados de acordo com estas normas não exclui a implementação de mecanismos para controlar ou limitar o acesso a categorias de dados definidas para fins imperativos.
- A portabilidade dos dados deve ser promovida. A portabilidade dos dados pode ser um direito da pessoa em causa, definido como o direito de obter os dados que um responsável pelo processamento de dados detém num formato estruturado, de uso corrente e de leitura ótica, e de os reutilizar para os seus próprios fins. A portabilidade pode ser facilitada através de uma política de portabilidade dos dados do sector público e do estabelecimento de direitos específicos de portabilidade dos dados em contextos de consumo.
- Deve ser dada prioridade às parcerias de dados (incluindo opções como os bancos de dados) como mecanismos para fazer avançar dados abertos de qualidade e que preservem a privacidade.
- Numa tentativa de facilitar a especificidade, a categorização dos dados pode ser um método para assegurar a coesão dos quadros de tratamento de dados no âmbito das autorizações de tratamento e dos princípios de segurança. A categorização aqui referida não é a das tipologias sectoriais consideradas de forma mais geral, mas sim um mecanismo específico para alcançar formas particulares de risco que se alinham com os tipos de dados e informações e podem incluir categorias sensíveis (como dados de crianças) e classificações de segurança relevantes, em relação a formas de dados que já são do domínio público.
- As restrições ao processamento devem ser claramente articuladas e limitadas, de modo a não interferir com o processamento de baixo risco que pode ser cada vez mais essencial para o treinamento da IA através do processamento de dados em grande escala.

→ AÇÕES

- Os Estados devem estabelecer uma política de dados aberta que estabeleça normas abertas para a produção e processamento de dados, de modo que, quando forem tomadas decisões para abrir os dados, sejam evitados os elevados custos de assegurar a sua capacidade de utilização e manipulação.
- As leis sectoriais e os códigos de conduta das APD devem ser revistos para garantir o acesso legal aos dados em conjunto com a política de dados.
- As APD devem ter uma dupla função de acesso à informação e de proteção da privacidade.
- Iniciativas de dados abertos multissectoriais devem ser implementadas em sectores de dados prioritários como a saúde, a investigação e o planeamento.

5.4.4 SEGURANÇA DE DADOS

Definição do problema

A segurança dos dados inclui todas as políticas, normas, regulamentos, legislação e práticas concebidas para proteger a confidencialidade, a integridade e a disponibilidade dos dados contra o acesso não autorizado, a corrupção ou o roubo, ao longo de todo o ciclo de vida dos dados. Estes princípios fundamentais da segurança dos dados também definem as três principais áreas de responsabilidade pela segurança da informação. O conceito de segurança dos dados engloba muitos aspetos, desde a segurança física do hardware do centro de dados e dos dispositivos de armazenamento até aos controlos de acesso administrativos e à segurança lógica das redes, do software e das aplicações. Inclui também procedimentos e políticas organizacionais.

A confidencialidade, a integridade e a disponibilidade dos dados, de um ponto de vista regulamentar, dependem das políticas e da legislação nacionais em matéria de segurança cibernética. A segurança dos dados (incluindo a confidencialidade, a integridade e a disponibilidade) não depende da localização física dos servidores que alojam os dados. Depende, sim, das regras prescritivas - incluindo normas, políticas, regulamentos, leis e protocolos (como normas de dados e interfaces técnicas), bem como da implementação de tecnologias e medidas de segurança (como encriptação, firewalls e controlos de acesso) - que são postas em prática pelos prestadores de serviços públicos ou privados na forma como armazenam, acedem, partilham e utilizam os dados.

O progresso da legislação sobre segurança de dados e as medidas técnicas podem tanto melhorar a confidencialidade, integridade e disponibilidade (segurança positiva) como prejudicar a liberdade fundamental e os direitos de privacidade, dignidade e segurança em linha (segurança negativa). Por exemplo, para proteger a segurança dos dados dos utilizadores, alguns países podem impor restrições à partilha e transferência de dados através da promulgação de legislação sobre segurança cibernética. Estas podem ser barreiras ao livre fluxo de dados. De uma perspetiva de segurança cibernética, alguns estados podem acreditar que os dados são mais seguros se forem armazenados dentro das fronteiras nacionais. Os Estados podem, erradamente, referir-se a estes procedimentos como princípios de soberania dos dados, quando, na realidade, estas medidas são simplesmente formas de protecionismo e de localização de dados.

Um princípio que é difícil de defender no que diz respeito à segurança dos dados é o da transparência. Embora os países continuem a testemunhar um aumento do número de ataques reportados às autoridades policiais, as melhorias nesta área têm sido impulsionadas quase inteiramente pelos regulamentos de proteção de dados, e os incidentes reportados são principalmente violações de dados. Por outro lado, o aumento da transparência na segurança de dados inclui tanto aspetos técnicos como a comunicação de vulnerabilidades de dia zero e a adesão a normas internacionais de segurança cibernética, como também aspetos políticos relacionados com a avaliação da maturidade da capacidade cibernética. A transparência na segurança de dados tem o potencial de melhorar os mecanismos técnicos e processuais de defesa contra ataques e de reforçar as práticas de colaboração baseadas na partilha de informação.

RECOMENDAÇÕES

- Os Estados-membros devem desenvolver políticas nacionais de segurança cibernética, bem como medidas jurídicas e técnicas necessárias para manter a confiança no seu espaço digital.
- Os Estados-membros são encorajados a cooperar a nível regional para desenvolver normas de segurança cibernética a serem cumpridas tanto no sector público como no privado para aumentar o crescimento económico regional.
- As políticas de dados devem alinhar-se com as políticas de segurança cibernética e de cibercriminalidade, e a legislação que trata da cibercriminalidade deve respeitar os direitos humanos.
- Deve ser estabelecido um regime conjunto de sanções para ataques cibernéticos.

→ AÇÕES

- Os Estados-membros, que ainda não adotaram medidas de segurança cibernética, devem desenvolver imediatamente planos de segurança cibernética e racionalizá-los no âmbito das estruturas de governação estatal para promover a robustez e reduzir as vulnerabilidades.
- Instituições de segurança cibernética como a CSIRT devem ser incorporadas no desenvolvimento de políticas de dados.
- As funções de processamento de dados como forma de proteção de segurança devem ser especificadas nas políticas pelos decisores políticos.
- O reforço das capacidades em relação à proteção de dados, segurança cibernética e governação de dados institucionais nas agências relevantes deve ser assegurado através da atribuição de políticas e bens, e pode ser apoiado pelas APD.

5.4.5 FLUXOS DE DADOS TRANSFRONTEIRIÇOS

Uma questão cada vez mais importante no comércio internacional e regional é a transferência transfronteiriça de dados pessoais e outros dados (Deloitte, 2016). No contexto africano, os quadros internacionais e regionais que facilitam as transações transfronteiriças e os fluxos de dados pessoais entre países são essenciais para a criação de mercados comuns e, em particular, para a concretização do Acordo de Comércio Livre Africano. A transferência transfronteiriça de dados pessoais, em particular, é moldada pela abordagem da soberania dos dados que um país deseja seguir, que se refere ao princípio jurídico de que a informação (geralmente em formato eletrónico) é regulada ou regida pelo regime jurídico do país em que esses dados residem. Como já foi referido, este conceito é posto em causa pela realidade moderna dos movimentos de dados. No entanto, devem ser reconhecidas as críticas à teoria dos "fluxos de dados" e a extensão dos seus benefícios para o dividendo digital no desenvolvimento, e deve ser reconhecido que quantidades significativas de fluxos de dados ocorrem de facto horizontalmente dentro das empresas e não entre elas (CNUCED, 2021).

Importa também mencionar a posição comum segundo a qual a transferência de dados depende do facto de o país recetor ter ou não um nível de proteção adequado (Razzano, Calandro et al., 2020). No entanto, o que corresponde a este nível "adequado" será frequentemente determinado pela Autoridade de Proteção de Dados de um país, ou similar. Assim, na ausência de uma lei de proteção de dados no país destinatário, não é possível submeter a transferência de dados pessoais a uma regulamentação adequada, a não ser que a lei de um país proíba

a transferência de dados para países que não tenham um nível de proteção adequado, ou através do estabelecimento de obrigações bilaterais por meio de um contrato entre as partes da transferência.

Na realidade, a existência de amplas limitações à transferência transfronteiriça de dados pode resultar na perda de oportunidades de negócio e reduzir a capacidade de uma organização para negociar internacionalmente, conduzindo a uma redução da sua presença geográfica e à perda de competitividade no mercado (Razzano et al., 2020). Uma regulamentação de dados que esteja em sintonia com a regulamentação de outras jurisdições contribui para a confiança mútua e estabelece as bases para o intercâmbio seguro de dados, incluindo (mas não se limitando a) dados pessoais. Neste sentido, a regulamentação da proteção de dados pessoais permite e reforça a confiança e o comércio na circulação transfronteiriça de pessoas, bens e serviços (Sociedade da Informação, 2018).

RECOMENDAÇÕES

- Os quadros de proteção de dados devem fornecer normas mínimas para os fluxos de dados transfronteiriços.
- O estabelecimento de normas e padrões deve assegurar expressamente a reciprocidade como princípio fundamental para permitir os fluxos transfronteiriços.
- É necessário dar prioridade à especificidade dos dados para evitar restrições involuntárias à partilha de dados produtivos.
- As considerações relativas à aplicação da lei devem ser incorporadas no processo de elaboração de políticas.
- Para assegurar uma resolução transfronteiriça eficaz, deve-se assegurar um grau de capacidade entre agências.
- Os Estados-membros da União Africana devem definir rigorosamente um quadro e modalidades para regular os fluxos de dados transfronteiriços, e identificar a entidade afri cana e as pessoas habilitadas a gerir este sistema.

→ AÇÕES

- As APD devem determinar normas mínimas para a transferência.
- O reforço das capacidades em relação à proteção de dados, segurança cibernética e governação de dados institucionais nas agências relevantes deve ser assegurado através da atribuição de políticas e bens, e impulsionado idealmente pelas APD em conjunto com instalações educativas, e programas e unidades de competências governamentais.

5.4.6. PROCURA DE DADOS

Embora as importantes recomendações sobre os dados e a economia digital visem contribuir para a criação de um ecossistema de dados mais vasto, são também necessárias intervenções políticas específicas para estimular a procura de dados. Os utilizadores de dados podem ser o sector público, empresas privadas (de diferentes dimensões), bem como utilizadores individuais e cidadãos. No entanto, as capacidades de todos estes perfis têm de ser desenvolvidas para estimular a procura de dados, as culturas de dados e a inovação. O papel da política

na promoção da utilização produtiva dos dados pelas partes interessadas é facilitado pelos domínios políticos anteriores, mas pode também exigir considerações mais específicas. Isto é especialmente verdade porque a realidade dos dados para muitas partes interessadas locais no ecossistema de dados é uma realidade de escassez de dados e não de saturação de dados.

RECOMENDAÇÕES

- As comunidades de dados devem ser consideradas prioritárias na política de inovação. Estas comunidades requerem incentivos e apoio por parte da política nacional, incluindo a promoção ativa de centros de dados e outras formas de inovação comunitária que podem ajudar a gerar competências e uma cultura de dados, e ser apoiadas pelos atores da sociedade civil em geral.
- A provisão regulamentar para a gestão de dados deve incluir a provisão de caixas de areia regulamentares para incentivar o desenvolvimento de dados locais.

→ AÇÕES

- As comunidades de dados devem ser incorporadas nos processos de elaboração de políticas de dados pelos decisores políticos.
- As comunidades de dados devem ser envolvidas no desenvolvimento de iniciativas de dados públicos abertos por parte dos responsáveis pela implementação dos serviços; e
- As universidades devem ser incluídas como intervenientes políticos relevantes para ajudar a estabelecer a "base de conhecimentos" da qual a economia de dados local pode retirar conhecimentos científicos e tecnológicos.

5.4.7 GOVERNAÇÃO DE DADOS PARA SECTORES E CATEGORIAS ESPECIAIS DE DADOS

Certas categorias de dados e certos sectores específicos, requerem uma gestão de dados adaptada que tenha em conta as questões particulares que afetam essa categoria ou sector. Categorias como os dados relativos à saúde ou às crianças não são iguais a tipologias sectoriais como os dados financeiros, mas ambas podem exigir um tratamento separado. No entanto, o tratamento especial cria a ameaça de silos de dados, tornando-os menos utilizáveis, e pode aumentar os custos de conformidade, especialmente se houver regulamentos ou requisitos incompatíveis. O tratamento especial é por vezes necessário, mas deve estar em harmonia com a governação global dos dados e com este quadro político.

Uma recomendação fundamental para o acesso aos dados e a interoperabilidade é que os tipos de dados que requerem uma atenção especial devem ser identificados e claramente especificados, de modo a que o acesso especial e outros requisitos para esses dados se enquadrem nas regras gerais relativas aos dados. Tal como referido na secção "Localização de dados", os tipos de dados claramente especificados estão por vezes sujeitos a requisitos de localização de dados, a fim de prosseguir objetivos políticos específicos desse tipo de dados. Nas recomendações sobre tratamento e proteção de dados, recomenda-se que os códigos de conduta, sujeitos a aprovação pela autoridade nacional de proteção de dados, possam ser utilizados para requisitos específicos do sector.

RECOMENDAÇÕES

- Os membros devem evitar regimes de dados especiais que não estejam integrados em regimes de dados nacionais e que não incorporem os princípios da boa governação dos dados.
- Os mecanismos e políticas de governação devem permitir o desenvolvimento da governação de dados específicos de categoria e sector para dados sobre crianças, dados de saúde e outros tipos de dados sensíveis ou dados específicos de sector que mereçam processamento distinto através de processos que estejam de acordo com os princípios do quadro.

5.5. GOVERNAÇÃO INTERNACIONAL E REGIONAL

A nível transnacional e continental – particularmente para proporcionar capacidade de segurança cibernética e para responder às preocupações de proteção de dados associadas às mudanças na economia de dados – a cooperação entre países é de importância crescente. O âmbito da cooperação necessária inclui o diálogo entre os governos, a colaboração com o sector privado e processos eficazes e integrados para investigar e processar violações transfronteiras. Uma arquitetura de confiança global que tenha em conta as limitações dos sistemas nacionais existentes ou outros sistemas fragmentados é essencial para assegurar uma economia digital e a inclusão digital (Banco Africano de Desenvolvimento, 2019).

Uma série de iniciativas internacionais e continentais estão a servir de marcos para acelerar a implementação.

As iniciativas da União Africana e regionais incidem, respetivamente, nos dados genéticos codificados digitalmente[17] e nos dados geográficos e ambientais. A Comissão da União Africana assegurará a harmonia entre estas iniciativas e o trabalho em curso sobre a política de dados.[18]

RECOMENDAÇÕES:

A União Africana, com o apoio de outras organizações pan-africanas, deve:

- facilitar a colaboração entre as várias entidades que lidam com dados em todo o continente através do estabelecimento de um quadro de consulta para diálogos políticos no seio da comunidade do ecossistema digital para salvaguardar os interesses de cada ator;

17 Embora a categoria de dados genéticos codificados digitalmente inclua os dados genéticos de seres humanos, quando se trata de indivíduos identificáveis, estes devem ser considerados como dados sensíveis e tratados como exigido pela Convenção de Malabo. Mas há outros tipos de dados genéticos codificados digitalmente que exigem um processamento específico/especial que não são sensíveis nem pessoais. Estes incluem os dados genéticos demográficos e os dados genéticos de organismos que não os humanos. A União Africana está atualmente a colaborar com outros países que são partes da Convenção sobre Biodiversidade (CBD) para garantir que os dados codificados digitalmente devem ser tratados como recursos biológicos, tal como o termo é utilizado na CBD. A convenção afirma que os recursos biológicos "incluem recursos genéticos, organismos ou partes dos mesmos, populações ou qualquer outro componente biótico de ecossistemas com uso ou valor real ou potencial para a humanidade". A convenção rege tanto o acesso como a partilha de benefícios para permitir a investigação e exigir que as pessoas que são guardiãs da biodiversidade partilhem os benefícios dessa investigação. A aplicação das regras da convenção permitirá um fluxo de dados benéfico, assegurando simultaneamente que os africanos beneficiem.

18 1A Estratégia Regional de Dados para a Gestão de Áreas Marinhas e Costeiras na África Ocidental promove uma gestão mais sustentável dos recursos naturais através da partilha mútua de dados.

- reforçar as ligações com outras regiões e coordenar as posições comuns africanas nas negociações internacionais sobre dados, a fim de assegurar a igualdade de oportunidades na economia digital global;
- apoiar o desenvolvimento de infraestruturas de dados regionais e continentais para albergar tecnologias avançadas baseadas em dados (tais como os macrodados, a Aprendizagem Automática e a Inteligência Artificial), o ambiente necessário facilitador e o mecanismo de partilha de dados para assegurar a circulação através do continente.

5.5.1 NORMAS DE DADOS CONTINENTAIS

Para facilitar a cooperação transfronteiriça, é importante chegar a um consenso sobre as normas de dados como parte integrante da promoção da interoperabilidade. Estas formas de consenso entre as várias partes interessadas devem referir-se ao trabalho realizado pela Organização Internacional de Normalização e a outras formas de consenso internacional alcançadas em contextos sectoriais específicos. No entanto, embora a normalização internacional seja importante para a competitividade, deve ter-se em conta que estas normas internacionais podem não ser suficientes para as necessidades da região. Isto é demonstrado, por exemplo, no caso dos desafios linguísticos encontrados no contexto dos dados espaciais ou geográficos.

RECOMENDAÇÕES

- O consenso sobre normas de dados deve fazer referência ao trabalho da Organização Internacional de Normalização, entre outros fóruns relevantes.
- No entanto, é necessário estabelecer normas com reflexões específicas sobre fatores contextuais que afetam o continente.

→ AÇÕES

- Estabelecer ou capacitar um mecanismo no seio da CUA para centralizar os comprom issos regionais sobre normas de dados.

5.5.2 PORTAL ABERTO DE DADOS E OUTRAS INICIATIVAS

Existem importantes iniciativas de dados abertos que já estão a ocorrer centralmente e que devem continuar a ser apoiadas em nome de uma economia regional de dados robusta. Estas incluem o portal central de dados abertos do Banco Africano de Desenvolvimento (*https://da- taportal.opendataforafrica.org/*). Além disso, existem iniciativas institucionalmente motivadas (como em *https://www.datafirst.uct.ac.za/dataportal/index.php/catalog/central/about*) e comunidades guiadas por voluntários (como em *https://africaopendata.org/*).

5.5.3 INSTRUMENTOS CONTINENTAIS

A vasta gama de instrumentos relevantes existentes é descrita no Capítulo 4, mas há dois domínios específicos que merecem destaque.

Mecanismo de fluxo de dados transfronteiras

É possível aproveitar este quadro para iniciar uma colaboração com vista à criação de um mecanismo regional de circulação transfronteiriça de dados, facilitado por um instrumento global como os da OCDE e da ASEAN.

Convenção da UA sobre Segurança Cibernética e Proteção de Dados Pessoais

Recomenda-se que a Convenção da UA seja ratificada o mais cedo possível para servir de etapa fundamental para a harmonização do processamento de dados. Os protocolos adicionais à Convenção devem também ser explorados para refletir as mudanças ocorridas desde a redação original.

Acordo da Zona de Comércio Livre Continental Africana

A ZCLCA oferece a oportunidade de cooperar numa série de aspetos importantes do quadro político, incluindo o desenvolvimento de acordos sobre concorrência, propriedade intelectual e investimento.

RECOMENDAÇÕES

- Promover e facilitar os fluxos de dados dentro e entre os Estados-membros da UA através do desenvolvimento de um Mecanismo de Fluxos de Dados Transfronteiriços que tenha em conta o contexto africano, nomeadamente os diferentes níveis de prontidão digital, maturidade dos dados, bem como ambientes legais e regulamentares.
- Facilitar a circulação dos dados entre sectores e entre fronteiras, desenvolvendo um Quadro Comum de Categorização e Partilha de Dados que tenha em conta os tipos alargados de dados e os seus diferentes níveis de privacidade e segurança.
- Trabalhar em estreita colaboração com as autoridades nacionais responsáveis pela proteção de dados pessoais dos Estados-membros da UA, com o apoio da Rede Africana de Autoridades (RAPDP), para estabelecer um mecanismo e órgão de coordenação que supervisione a transferência de dados pessoais dentro do continente e assegure o cumprimento das leis e regras existentes que regem a segurança de dados e informações a nível nacional.
- Permitir a partilha de dados e uma maior interoperabilidade entre os Estados-membros da UA e outros mecanismos da UA, incluindo o Mecanismo de Cooperação Policial da União Africana (AFRIPOL).
- Trabalhar para a construção de um ciberespaço seguro e resistente no continente que ofereça novas oportunidades económicas através do desenvolvimento de uma Estratégia de Segurança Cibernética da UA e do estabelecimento de Centros Operacionais de Segurança Cibernética para mitigar riscos e ameaças relacionadas com ciberataques, violações de dados e utilização indevida de informação sensível.
- Estabelecer ou reforçar mecanismos e instituições no seio da União Africana para desenvolver capacidades e prestar assistência técnica aos Estados-Membros da União Africana com vista à incorporação nacional deste quadro de política de dados.
- Recomenda-se que as negociações relativas ao capítulo "concorrência" da ZCLCA estabeleçam normas mínimas para garantir que os dados não pessoais, supostamente proprietários, sejam acessíveis aos inovadores, empresários e outros atores da cadeia de valor, a fim de promover a concorrência no continente.

- Os membros da ZCLCA devem considerar a inclusão de disposições no capítulo da concorrência que conferem às autoridades da concorrência o mandato para considerarem também os efeitos da estrutura do mercado em termos de segurança e privacidade. Isto é importante para evitar a concentração de corretores de dados ou plataformas, tanto a nível nacional como regional, uma vez que isso cria o risco de um único ou poucos pon tos de falha com consequências consideráveis.
- Os membros da ZCLCA devem igualmente considerar a inclusão de disposições que clarifiquem o estatuto dos dados relativa mente à propriedade intelectual no capítulo da propriedade intelectual da ZCLCA, em particular prevendo que:
  - se o direito de autor for alargado a bases de dados e compilações de dados, só se aplica se as bases de dados e compilações forem criadas por autores humanos e forem originais, e só se estende à reprodução da seleção e disposição originais dos dados na base de dados e não aos próprios dados;
  - qualquer direito de autor ou outro direito de propriedade intelectual, incluindo segredos comerciais, que permita o controlo de dados não se aplique aos dados pessoais; e
  - quaisquer direitos de autor ou outros direitos de propriedade intelectual, incluindo os segredos comerciais, que permitem o controlo dos dados sejam limitados pelas disposições da regulamentação em matéria de concorrência.

→ AÇÕES

- Os Estados-membros devem ratificar a Convenção da UA sobre Segurança Cibernética e Proteção de Dados Pessoais e desenvolver protocolos adicionais, conforme necessário, para refletir as alterações desde a redação original.
- Estabelecer, ou conferir poderes, a um mecanismo no seio da CUA para centralizar os compromissos regionais sobre normas de dados.
- Uma vez esse mecanismo adotado, alinhamentos com o processo da ZCLCA devem ser imediatamente explorados.
- Incluir dados nas negociações sobre os capítulos da ZCLCA sobre a concorrência e a propriedade intelectual.
- Acordar em critérios comuns e coerentes para avaliar a adequação dos níveis de proteção dos dados pessoais em todo o continente, a fim de facilitar e permitir a transferência transfronteiriça de dados e normalizar a proteção.

5.5.4 INSTITUIÇÕES E ASSOCIAÇÕES CONTINENTAIS E REGIONAIS

As instituições e associações regionais são um mecanismo central para criar uma voz regional unificada sobre questões de dados. Já existem muitas associações e uma recomendação prioritária é garantir que a aplicação deste quadro se dirija às associações existentes. Os organismos continentais e regionais são particularmente importantes devido à natureza transfronteiriça do fluxo de dados necessário para colher os benefícios dos dados.

Comunidades económicas e de desenvolvimento regionais

A Comunidade Económica dos Estados da África Ocidental (CEDEAO), a Comunidade da África Oriental e a Comunidade de Desenvolvimento da África Austral podem ajudar os Estados-membros a criar capacidade, transpor a política de dados, chegar a consenso sobre a harmonização da política de dados, participar na elaboração de normas, e permitir o fluxo de dados.

Juízes dos direitos humanos

O Tribunal Africano dos Direitos do Homem e dos Povos, o Tribunal de Justiça da África Oriental e o Tribunal de Justiça da Comunidade Económica dos Estados da África Ocidental (CEDEAO) proporcionam fóruns e capacidade qualificada para julgar litígios complexos em matéria de privacidade e igualdade relevantes para a proteção de dados pessoais e a utilização de dados para discriminação injusta.

O Tribunal da SADC, uma vez recapitulado, poderia também oferecer um fórum para disputas de dados, embora dentro de um mandato mais limitado. Os mecanismos de arbitragem continentais e regionais são os mais bem colocados para resolver litígios transfronteiriços em matéria de dados.

Rede Africana de Reguladores de Dados

Capacitar as APD e melhorar o nível de aplicação dos quadros legislativos e regulamentares a nível nacional contribui significativamente para que os indivíduos possam usufruir dos seus direitos digitais. Promover e apoiar as associações existentes, como a Rede Africana de Autoridades de Proteção de Dados, constitui também uma forma de reforçar esta capacidade.

Associações de Autoridades Reguladoras das TIC

Existem associações regionais de reguladores das TIC (ARTAC, WATRA, CRASA e EACO) que constituem importantes mecanismos de aprendizagem entre pares para as associações transfronteiriças. Podem também facilitar a colaboração e a partilha de conhecimentos à medida que são explorados instrumentos e normas transfronteiras.

Associações Sectoriais

As associações sectoriais, como o Fórum Africano da Administração Fiscal, deverão contribuir para a aplicação das recomendações relativas à economia dos dados, em particular. Dada a importância da identidade digital na economia dos dados, a Associação de Conservadores Nacionais é também importante.

Fórum Africano da Concorrência

O Fórum Africano da Concorrência (FAC) descreve-se a si próprio como "uma rede informal de autoridades nacionais e multinacionais africanas da concorrência". O FAC pode criar capacidade para ajudar as autoridades de concorrência a regular as questões de dados.

RECOMENDAÇÕES

- Reforçar a cooperação regulamentar e a partilha de conhecimentos entre países e regiões africanas, através do reforço das capacidades da Rede Africana de Autoridades de Proteção de Dados e à Associação Regional de Reguladores das TIC.
- Os mecanismos de adjudicação continental e regional existentes devem ser explicitamente autorizados a lidar com questões de dados que estejam implicadas em direitos digitais e direitos sobre dados, e disputas transfronteiriças de dados.
- As autoridades fiscais africanas devem colaborar através do Fórum Africano de Administração Fiscal (ATAF) para desenvolver uma posição africana que represente mais eficazmente o interesse comum no processo de reformas fiscais internacionais, tais como o BEPS.
- Criar um Fórum Anual de Inovação de Dados para África para servir de plataforma para discussões entre múltiplos intervenientes, facilitar o intercâmbio entre países e sensibilizar os decisores políticos para o poder dos dados como motor da economia digital atual.

5.6. QUADRO DE IMPLEMENTAÇÃO

5.6.1 FASES DO QUADRO DE IMPLEMENTAÇÃO

Note-se que, embora as áreas de atividade abaixo sejam identificadas como fases, sua realização não é estritamente linear. Particularmente, as fases 2 e 3 são consideradas processos simultâneos, que podem ocorrer juntamente com atividades de transposição. O quadro de implementação deve ser lido em conjunto com o mapeamento das partes interessadas descrito em 5.6.2.

	Actividade	Descrição	Responsabilidade de Liderança
FASE 1: ADOPÇÃO DO QUADRO			
A	Os Estados-membros adoptam um quadro		Membros
B	Concepção de Monitorização para o Quadro	Criação de um quadro de monitorização de alto nível,	CUA
C	Estabelecer ou dar poder a um mecanismo dentro da UA para centralizar os compromissos regionais sobre dados	Actividades para incluir apoio à implementação, coordenação sobre normas de dados, e outras áreas específicas enunciadas nas recomendações que requerem colaboração regional.	CUA

	Actividade	Descrição	Responsabilidade de Liderança
FASE 2: ADESÃO/APROPRIAÇÃO			
A	Avaliar o Quadro Continental	Assegurar o alinhamento com os instrumentos continentais.	CUA, CER, AUDA-NEPAD, Smart Africa
B	Envolver as Estruturas Continentais	Envolver as estruturas associadas em potenciais áreas de colaboração na implementação do quadro.	CUA
C	Avaliar o Quadro Continental	Ênfase nos princípios, explorar o alinhamento com quadros de estruturas internacionais.	CUA
D	Envolver Estruturas Internacionais		CUA, Estados-membros da UA
FASE 3: APOIO CONTINENTAL AOS ESTADOS-MEMBROS PARA SATISFAZEREM AS CONDIÇÕES PRÉVIAS			
A	Desenvolver infra-estruturas de banda larga e quadros regulamentares	Implementação de políti-cas mais amplas iniciada em relação ao ambiente de dados facilitador, a nível interno.	CER, AUDA-NEPAD, ATU, PAPU, SMART AFRICA
FASE 4: TRANSPOSIÇÃO NACIONAL			
A	Envolvimento com várias partes interessadas	Promover o Quadro Político, envolver os intervenientes internos.	Estados-Membros, sector privado, sociedade civil,
B	Iniciar a adesão de múltiplas partes interessadas	Reflexão sobre o mapeamento das partes interessadas na Fase Dois*, garantir o alinhamento das políticas.	Estados-Membros
C	Instrumento aplicado a nível interno	Desenvolver Quadros Jurídicos e Regulamentares estabelecer um regulador de dados e um sistema de governação de dados.	Estados-Membros
D	Quadro orçamental	Alocar recursos para implementação	Estados-Membros

	Actividade	Descrição	Responsabilidade de Liderança
FASE 5: COLABORAÇÃO			
A	Envolver Fóruns Internacionais de Tomada de Decisões	Envolver fóruns de elaboração de regras sobre normas e regras de dados (ver mapeamento das partes interessadas).	Estados-membros da UA
B	Monitorização da implementação dos membros		CUA, CER, AUDA-NEPAD, Smart Africa
C	Sensibilizar para o mecanismo continental centralizador de dados.	Aceitar pedidos directos de assistência	CUA, Instituições Regionais
D	Participar em actividades continentais	Participar nas actividades continentais delineadas na Secção 10.	Estados-Membros

5.6.2 MAPEAMENTO DAS PARTES INTERESSADAS

É fornecido um mapeamento sintético das partes interessadas para facilitar a implementação, particularmente nas fases 2, 4 e 5.

DESCRIÇÃO	SUBTIPOS	FINALIDADE
INTERNACIONAL		
Nações Unidas	União Internacional das Telecomunicações, Departamento de Segurança e Protecção das Nações Unidas	Alinhamento da política de desenvolvimento
Organizações Multilaterais	Organização para a Cooperação e Desenvolvimento Económico, Banco Mundial	Alinhamento da política económica
Estruturas de Governação da Internet	Fórum de Governação da Internet, Grupo de Trabalho de Engenharia da Internet, Corporação para Atribuição de Nomes e Números na Internet	Alinhamento da política digital e da Internet
Normas internacionais	Organização Internacional de Normalização	Alinhamento da padronização dos dados
Organizações multilaterais (sectoriais)	Organização Mundial de Saúde, Organização Mundial do Comércio	Alinhamento das componentes sectoriais de política

REGIONAL		
Comunidades Económicas Regionais	CEDEAO, SADC, CAO, CEEAC, COMESA, IGAD, CEN-SAD, UMA	Alinhamento da política económica e de desenvolvimento
Estruturas de Governação da Internet	AFRINIC, IGF Africano	Alinhamento da política digital e da Internet
Comunidade Regional (regulamentar)	Rede de Autoridades Africanas de Protecção de Dados, Outras Associações Reguladoras, Fórum Africano de Administração Fiscal	Alinhamento das políticas transfronteiras
Comunidade regional (sectorial)	Banco Africano de Desenvolvimento	Alinhamento das componentes sectoriais de política
INTERNO		
Departamentos Nacionais	Telecomunicações, Justiça, Cooperação Internacional, Segurança do Estado	Alinhamento de políticas
DESCRIÇÃO	**SUBTIPOS**	**FINALIDADE**
Agências estatísticas		Capacitação
Autoridades reguladoras	Protecção de dados, Regulamento sobre TIC, Concorrência	Implementação
A nível de empresa	Comités de Governação de Dados	Capacitação, envolvimento de várias partes interessadas

RECOMENDAÇÕES

Na sequência da aprovação do Quadro da Política de Dados da UA pelos órgãos da UA, a Comissão da UA, em colaboração com instituições regionais e partes interessadas relevantes, irá elaborar um Plano de Ação para orientar a implementação do quadro tendo em consideração a soberania digital dos Estados, bem como os diferentes níveis de desenvolvimento, vulnerabilidade das populações e digitalização nos Estados-membros da UA, nomeadamente aspetos relacionados com o défice na infraestrutura das TIC e a falta de políticas e legislações de segurança cibernética (a curto, médio e longo prazo). O plano de ação identificará papéis e responsabilidades e enfatizará as principais prioridades e ações imediatas tanto a nível regional como continental e isto em conformidade com os níveis de maturidade dos dados dos Estados-membros da UA.

BIBLIOGRAFIA

African Development Bank. (2019). Annual Report 2019 | African Development Bank—Building today, a better Africa tomorrow. https://www.afdb.org/en/documents/annual-report-2019

Ahmed, S. (2021). A Gender perspective on the use of Artificial Intelligence in the African Fin- Tech Ecosystem: Case studies from South Africa, Kenya, Nigeria, and Ghana. 23rd ITS Biennial Conference. https://www.econstor.eu/handle/10419/238000?author_page=1

Andreoni, A., & Tregenna, F. (2020). Escaping the middle-income technology trap: A comparative analysis of industrial policies in China, Brazil and South Africa. Structural Change and Economic Dynamics, 54, 324-340. https://doi.org/10.1016/j.strueco.2020.05.008

Arntz, M., Gregory, T., & Zierahn, U. (2016). The Risk of Automation for Jobs in OECD Countries. https://www.oecd-ilibrary.org/content/paper/5jlz9h56dvq7-en

Ballell, T. R. de las H. (2019). Legal challenges of artificial intelligence: Modelling the disruptive features of emerging technologies and assessing their possible legal impact. Uniform Law Review, 24(2), 302–314. https://doi.org/10.1093/ulr/unz018

Carrière-Swallow, Y., & Haksar, V. (2019). The Economics and Implications of Data: An Integrated Perspective (No. 19/16). https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596

Cavoukian, A. (2009). Privacy by design. The 7 foundational principles. Implementation and mapping of fair information practices. Information and Privacy Commissioner.

CNUCED. (2020). Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

CNUCED. (2021). Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow [United Nations publication].

Cory, N. (2017). Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Infor- mation Technology and Innovation Foundation. https://itif.org/publications/2017/05/01/cross- border-data-flows-where-are-barriers-and-what-do-they-cost

Couldry, N., & Mejias, U. (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. SAGE Publications. https://eprints.lse.ac.uk/89511/1/Couldry_Data-colonialism_Accepted.pdf

Deloitte. (2017). Privacy is Paramount | Personal Data Protection in Africa Personal Data Protection in Africa. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf

Gillwald, A., & Mothobi, O. (2019). After Access 2018: A Demand-Side View of Mobile Internet From 10 African Countries (After Access 2018: A Demand-Side View of Mobile Internet from 10 African Countries After Access: Paper No. 7 (2018); Policy Paper Series No. 5). Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf

Global Symposium for Regulators. (2020). the Regulatory Wheel of Change: Regulation for Digital Transformation. ITU. https://www.itu.int:443/en/ITU-D/Conferences/GSR/2020/Pages/default.aspx

Hawthorne, S. (2020). Impact of Internet Connection on Gifted Students' Perceptions of Course Quality at an Online High School. Boise State University Theses and Dissertations. https://doi.org/10.18122/td/1748/boisestate

Information Society. (2018). Personal Data Protection Guidelines for Africa. A joint initiative of the Internet Society and the Commission of the African Union. https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

International Telecommunication Union. (2019). Measuring Digital Development Facts and Figures (978-92-61-29511-0). https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

International Telecommunication Union. (2020). the Regulatory Wheel of Change: Regulation for Digital Transformation. ITU. https://www.itu.int:443/en/ITU-D/Conferences/GSR/2020/Pages/default.aspx

Jones, C., & Tonetti, C. (2020). Nonrivalry and the Economics of Data. The American Economic Review, 110(9), 2819–2858. https://doi.org/10.1257/aer.20191330

Khan, M., & Roy, P. (2019). Digital identities: A political settlements analysis of asymmetric power and information. https://eprints.soas.ac.uk/32531/1/ACE-WorkingPaper015-DigitalIdentities-191004.pdf

Macmillan, R. (2020). Data Governance: Towards a Policy Framework (Policy Brief No. 9). https://www.competition.org.za/ccred-blog-digital-industrial-policy/2020/7/6/data-governance-towards-a-policy-framework

Mazzucato, M., Entsminger, J., & Kattel, R. (2020). Public Value and Platform Governance (SSRN Scholarly Paper ID 3741641). Social Science Research Network. https://doi.org/10.2139/ssrn.3741641

Mitretodis, & Euper. (2019). Interaction Between Privacy and Competition Law in a Digital Economy. Competition Chronicle. https://www.competitionchronicle.com/2019/07/interaction-between-privacy-and-competition-law-in-a-digital-economy/

Nicholas, G., & Weinberg, M. (2019). Data Portability and Platform Competition: Is User Data Exported From Facebook Actually Useful to Competitors? | NYU School of Law. New York University School of Law. https://www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition

OECD. (2019). Data governance in the public sector. 23–57. https://doi.org/10.1787/9cada708-en

Open Data Charter. (2015). Open Data Charter Principles. Open Data Charter. https://opendatacharter.net/principles/

Polatin-Reuben, D., & Wright, J. (2014). An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.902.7318&rep=rep1&type=pdf#:~:text=Weak%20data%20sovereignty%20as%20defined,on%20safeguard%2D%20ing%20national%20security.

Razzano, G., Gillwald, A., Aguera, P., Ahmed, S., Calandro, E., Matanga, C., Rens, A., & van der Spuy, A. (2020). SADC Parliamentary Forum Discussion Paper: The Digital Economy and Society. Research ICT Africa. https://researchictafrica.net/publication/sadc-pf-discussion-paper-the-digital-economy-and-society/

Rinehart, W. (2020, September 14). Is data nonrivalrous? Medium. https://medium.com/cgo-benchmark/is-data-nonrivalrous-f1c8e720820b

Saint, M., & Garba, A. (2016). Technology and Policy for the Internet of Things in Africa (SSRN Scholarly Paper ID 2757220). Social Science Research Network. https://doi.org/10.2139/ssrn.2757220

Savona, M. (2019). The Value of Data: Towards a Framework to Redistribute It (SSRN Scholarly Paper ID 3476668). Social Science Research Network. https://doi.org/10.2139/ssrn.3476668

Schmidt, C. O., Struckmann, S., Enzenbach, C., Reineke, A., Stausberg, J., Damerow, S., Huebner, M., Schmidt, B., Sauerbrei, W., & Richter, A. (2021). Facilitating harmonized data quality assessments. A data quality framework for observational health research data collections with software implementations in R. BMC Medical Research Methodology, 21(1), 63. https://doi.org/10.1186/s12874-021-01252-7

Sen, A. (2001). Development As Freedom. OUP Oxford; eBook Collection (EBSCOhost). http://ezproxy.uct.ac.za/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2089308&site=ehost-live

Stork, C., & Gillwald, A. (2012). South Africa's mobile termination rate debate: What the evidence tells us (Policy Brief No. 2; South Africa). Research ICT Africa. https://researchictafrica.net/publications/Country_Specific_Policy_Briefs/South_Africa_Mobile_Termination_Rate_Debate_-_What_the_Evidence_Tells_Us.pdf

Taylor, L. (2019). Global data justice. Communications of the ACM, 62(6). https://doi.org/10.1145/3325279

Teh, H., Kempa-Liehr, A., & Wang, K. (2020). Sensor data quality: A systematic review. Journal of Big Data, 7. https://doi.org/10.1186/s40537-020-0285-1

United Nations. (2017). Looking to future, UN to consider how artificial intelligence could help achieve economic growth and reduce inequalities—United Nations Sustainable Development. https://www.un.org/sustainabledevelopment/blog/2017/10/looking-to-future-un-to-consid- erhow-artificial-intelligence-could-help-achieve-economic-growth-and-reduce-inequalities/

van der Spuy, A. (2021, February 23). How do we protect children's rights in a digital environment only available to some? African Post. https://researchictafrica.net/2021/02/23/how-do-we-protect-childrens-rights-in-a-digital-environment-only-available-to-some/

Wang, Y., McKee, M., Torbica, A., & Stuckler, D. (2019). Systematic Literature Review on the Spread of Health-related Misinformation on Social Media. Social Science & Medicine, 240, 112552. https://doi.org/10.1016/j.socscimed.2019.112552

Wook, M., Hasbullah, N. A., Zainudin, N. M., Jabar, Z. Z. A., Ramli, S., Razali, N. A. M., & Yusop,

N. M. M. (2021). Exploring big data traits and data quality dimensions for big data analytics application using partial least squares structural equation modelling. Journal of Big Data, 8(1), 49. https://doi.org/10.1186/s40537-021-00439-5

World Bank. (2021). Data for Better Lives. World Bank. Doi : 10.1596/978-1-4648-1600-0

World Bank, & ITU. (2020). The World Bank and International Telecommunication Union launch handbook on digital regulation [Text/HTML]. World Bank. https://www.worldbank.org/en/news/feature/2020/09/08/the-world-bank-and-international-telecommunication-union-launch-handbook-on-digital-regulation

World Economic Forum. (2016). Networked Readiness Index. Global Information Technology Report 2016. http://wef.ch/29cCKbU

Zuboff, S. (2018). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Penguin Publishing Group. https://antipodeonline.org/wp-content/uploads/2019/10/Book-review_Whitehead-on-Zuboff.pdf

ANEXO – DEFINIÇÕES DE TRABALHO

Anonimização: remoção de elementos de identificação pessoal diretos e indiretos dos dados.

Autoridades de Proteção de Dados (APD): autoridades públicas independentes que controlam e supervisionam, através de poderes de investigação e corretivos, a aplicação da lei de proteção de dados. Prestam aconselhamento especializado sobre questões de proteção de dados e tratam queixas que possam ter infringido a lei.

Capacidade digital: competências, literacia, normas sociais e atitudes de que indivíduos e organizações necessitam para prosperar, viver, aprender e trabalhar numa sociedade e economia digital.

Cibercrime: atos ilegais que afetam a confidencialidade, a integridade, a disponibilidade e a sobrevivência dos sistemas de tecnologia da informação e comunicação, os dados que processam e a infraestrutura de rede subjacente (Convenção de Malabo).

Classificação de dados: processo de organização de dados por categorias relevantes para que possam ser utilizados e protegidos de forma mais eficiente.

Comércio eletrónico: transações comerciais que ocorrem através de canais eletrónicos – compra e venda de bens ou serviços via Internet, e transferência de dinheiro e dados para completar as vendas – por métodos especificamente concebidos para efeitos de receção ou colocação de encomendas.

Consentimento da pessoa em causa: qualquer indicação livre, específica, informada e inequívoca da vontade da pessoa em causa pela qual esta, através de uma declaração ou de uma ação afirmativa clara, manifesta a sua concordância com o trata- mento dos dados pessoais que lhe dizem respeito.

Continental: para efeitos do presente quadro, refere-se a África.

Dados abertos: aberto significa que qualquer pessoa pode aceder, utilizar, modificar e partilhar livremente para qualquer fim (sujeito, no máximo, a requisitos que preservem a proveniência e a abertura (*http://opendefini- tion.org*/).

Dados pessoais: qualquer informação relativa a uma pessoa singular identificada ou identificável através da qual essa pessoa possa ser identificada, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a fatores mais específi- cos da sua identidade física, fisiológica, mental, económica, cultural ou social.

Dados sensíveis: todas as informações pessoais relativas às opiniões religiosas, filosóficas e políticas, bem como à vida sexual, raça, saúde e condições sociais da pessoa em causa (Convenção de Malabo).

Ecossistema de dados: para os fins aqui utilizados, não se refere apenas às linguagens de programação, aos pacotes, aos algoritmos, aos serviços de computação em nuvem e à infraestrutura geral que uma organização utiliza para recolher, armazenar, analisar e tirar partido dos dados, mas também à cadeia de valor subjacente associada aos dados como fator de produção, à governação dos sistemas de dados e à proteção das pessoas em causa.

Harmonização: refere-se ao facto de assegurar a uniformidade dos sistemas através da utilização de normas mínimas para facilitar a interoperabilidade e quadros jurídicos e de confiança (por exemplo, para níveis de garantia) para estabelecer regras e criar confiança nos respetivos sistemas.

Identidade digital: conjunto de atributos e/ou credenciais eletronicamente captados e armazenados que identificam de forma única uma pessoa, permitindo a distinção de um indivíduo de outro.

Infraestrutura de dados fundamentais: refere-se a tecnologias avançadas que facilitam o uso intensivo de dados de qualidade. Isto pode incluir redes de banda larga, centros de dados e serviços em nuvem, hardware e software eletrónico, e aplicações digitais que estão disponíveis na Internet.

Interoperacionalidade: capacidade das diferentes unidades funcionais – por exemplo, sistemas, bases de dados, dispositivos ou aplicações – de comunicar, executar programas, ou transferir dados de uma forma que requer que o utilizador tenha pouco ou nen hum conhecimento dessas unidades funcionais (adaptado de ISO/IEC 2382:2015).

Minimização dos dados: princípio dentro dos quadros de proteção de dados, o que reforça a recolha da quantidade mínima de dados pessoais necessários para fornecer um elemento individual de um serviço ou produto.

Nível de garantia (LOA): capacidade de determinar, com algum nível de certeza ou garantia, que uma reivindicação de uma determinada identidade feita por alguma pessoa ou entidade pode ser considerada como sendo de facto a identidade "verdadeira" do requerente (ID4D Cooperação Público-Privada). O nível global de garantia é função do grau de confiança de que a identidade reivindicada pelo requerente é a sua identidade real (o nível de garantia de identidade ou IAL), a força do processo de autenticação (nível de garantia de autenticação ou AAL), e – se utilizar uma identidade federada – o protocolo de afirmação utilizado pela federação para comunicar a autenticação e atribuir informação (nível de garantia de identidade ou FAL) (adaptado de NIST 800-63:2017).

Normas abertas: normas colocadas à disposição do público em geral e são desenvolvidas (ou aprovadas) e mantidas através de um processo de colaboração e de consenso. As normas abertas facilitam a interoperabilidade e o intercâmbio de dados entre diferentes produtos ou serviços e destinam-se a uma adoção generalizada (adotadas pela UIT-T).

Pessoa em causa: entende-se qualquer pessoa singular que seja objeto de processamento de dados pessoais.

Privacidade e segurança através da conceção: significa incorporar proactivamente mecanismos de privacidade e segurança na conceção e operação de produtos e serviços tanto de sistemas não informáticos como de TI, infraestruturas em rede, e práticas comerciais. Isto requer que a governação da privacidade e segurança seja considerada ao longo de todo o processo de engenharia e do ciclo de vida do produto.

Proteção de dados: regula a forma como os dados são utilizados ou processados e por quem, e assegura que os cidadãos têm direitos sobre os seus dados. É particularmente importante para assegurar a dignidade digital, pois pode abordar diretamente o desequilíbrio de poder inerente entre "pessoas em causa" e as instituições ou pessoas que recolheram os dados.

Pseudonimização: processamento de dados de modo a que não possam ser associados a uma pessoa sem informações adicionais.

Publicação de dados: refere-se ao processo através do qual as interações diárias dos seres vivos podem ser transformadas num formato de dados e colocadas em uso social e económico.

Regional: para efeitos do presente quadro, refere-se às cinco regiões de África reconhecidas pela União Africana.

Responsável pelo processamento de dados: qualquer pessoa singular ou coletiva, pública ou privada, qualquer outra organização ou associação que, sozinha ou em conjunto com outras, decida recolher e tratar dados pessoais e determine as finalidades.

Segurança cibernética: a segurança cibernética refere-se ao conjunto de tecnologias, processos e práticas concebidos para proteger redes, dispositivos, programas e dados contra ataques, danos ou acesso não autorizado (*https://digitalguardian.com/blog/what-cyber-security*).

Serviços baseados na nuvem: aplicações de mercado de massas (ou seja, meios de comunicação social e webmail oferecidos através da Internet), em que os dados não se encontram nos dispositivos dos indivíduos, mas são armazenados remotamente num centro de dados. Os exemplos incluem Facebook, YouTube e Gmail.

Serviços em nuvem: serviços utilizados a pedido em qualquer altura, através de qualquer rede de acesso, utilizando quaisquer dispositivos conectados que utilizam tecnologias de computação em nuvem, utilizam software e aplicações que estão localizados na nuvem e não nos próprios dispositivos dos utilizadores.

União Africana

Department of Infrastructure and Energy
African Union Headquaters
P.O. Box 3243, Roosevelt Street
W21K19, Addis Ababa, Ethiopia
Tel: +251 (0) 11 551 77 00
Fax: +251 (0) 11 551 78 44
www.au.int