União Africana

Uma África Integrada,
Próspera e Pacífica

Directrizes para a Integração das Disposições Relativas aos Dados no Protocolo Sobre o Comércio Digital

ÍNDICE

LISTA DE FIGURAS E QUADROS

LISTA DE TABELAS

AGRADECIMENTOS

As *Directrizes para a Integração das Disposições relativas aos Dados no Protocolo* sobre o Comércio Digital foram preparadas sob a orientação geral de S. Exa. Dr.ª Amani Abou-Zeid, Comissária para as Infra-estruturas e Energia, Comissão da UA, por uma equipa composta pelo Dr. Kamugisha Kazaura, Director do Departamento de Infra-estruturas e Energia, Sr. Moses Bayingana Chefe da Divisão Interino da Sociedade da Informação e Sr.ª Souhila Amazouz, Responsável Sénior de Política Digital (Coordenadora do Grupo de Trabalho), bem como as valiosas contribuições e contributos dos membros do Grupo de Trabalho que representam as Comunidades Económicas Regionais, a AUDA-NEPAD, as Instituições Especializadas da UA, as Organizações Regionais e Pan-Africanas, a Rede de Autoridades Africanas de Protecção de Dados (NADPA), bem como as Agências das Nações Unidas e as Organizações Internacionais que operam em África no domínio dos dados e do comércio digital.

O quadro beneficiou do apoio financeiro da GIZ e do apoio técnico do Sr. Paul Baker, Director Executivo da International Economic Consulting Ltd.

Foram também recebidos comentários em várias fases de elaboração do presente documento por peritos africanos dos Estados-membros da UA que participaram no workshop de validação virtual.

Estas Directrizes foram aprovadas na 44.ª Sessão Ordinária do Conselho Executivo, realizada em Fevereiro de 2024, e estão em conformidade com o Quadro de Política de Dados da UA aprovado pela Cimeira da UA em Fevereiro de 2022.

SIGLAS E ACRÓNIMOS

4IR	Quarta Revolução Industrial
ACC	Acordo de Comércio e Cooperação
ACL	Acordo de Comércio Livre
ACR	Acordos Comerciais Regionais
ADR	Resolução Alternativa de Litígios
APEC	Cooperação Económica Ásia-Pacífico
API	Interface de Programação de Aplicações
ASEAN	Associação das Nações do Sudeste Asiático
B2B	Empresa a empresa
BATNA	Melhor Alternativa a um Acordo Negociado
CBPR	Regras de Privacidade Transfronteiriças
CCPA	Lei da Privacidade do Consumidor da Califórnia
CEDEAO	Comunidade Económica dos Estados da África Ocidental
CER	Comunidades Económicas Regionais
CPTPP	Acordo Global e Progressivo para a Parceria Trans-Pacífico
DEA	Parceria para a Economia Digital
DEPA	Acordo de Parceria para a Economia Digital
DFFT	Fluxo Livre de Dados com Confiança
DSM	Mercado Único Digital
E-Commerce	Comércio Electrónico
ETD	Estratégia de Transformação Digital
EUA	Estados Unidos da América
FEM	Fórum Económico Mundial
G20	Grupo dos Vinte
GATS	Acordo Geral sobre o Comércio de Serviços
GBP	Libra Esterlina
GDPR	Regulamento Geral sobre a Protecção de Dados
GMV	Volume Bruto de Mercadoria
IA	Inteligência Artificial
IFCSFI	Sociedade Financeira Internacional
IoT	Internet das Coisas
ISP	Fornecedores de Serviços de Internet
JSI	Iniciativa da Declaração Conjunta
MCC	Modelo de Cláusulas Contratuais
MRL	Mecanismo de Resolução de Litígios
OCDE	Organização para a Cooperação e Desenvolvimento Económico
ODS	Objectivo de Desenvolvimento Sustentável
OMC	Organização Mundial do Comércio
ONU	Nações Unidas

PIB	Produto Interno Bruto
POPIA	Lei de Protecção de Informações Pessoais
PTP	Parceria Trans-Pacífico
QGD	Quadro de Gestão de Dados
RCEP	Parceria Económica Regional Abrangente
SADC	Comunidade para o Desenvolvimento da África Austral
TAPED	Disposições dos Acordos Comerciais sobre Comércio Electrónico e Dados
TCAC	Taxa de Crescimento Anual Composta
TIC	Tecnologias de Informação e Comunicação
TiSA	Acordo sobre Comércio de Serviços
UA	União Africana
UE	União Europeia
UK	Reino Unido
UNCTAD	Conferência das Nações Unidas sobre Comércio e Desenvolvimento
UNDG	Grupo de Desenvolvimento das Nações Unidas
US$	Dólar dos Estados Unidos da América
USMCA	Acordo EUA-México-Canadá
ZCLCA	Acordo sobre o Comércio Livre Continental Africano
ZOPA	Zona de Possível Acordo

1. INTRODUÇÃO

1.1. TENDÊNCIA MUNDIAL DE DESENVOLVIMENTO DA ECONOMIA DIGITAL

A digitalização tornou-se uma das principais fontes de crescimento socioeconómico. A economia digital foi avaliada em 11,5 biliões de USD a nível mundial, o equivalente a 15,5% do PIB mundial em 2016, e cresceu duas vezes e meia mais rápido do que o PIB mundial desde 2000 (Huawei & Oxford Economics, 2017). Os progressos na expansão da conectividade trouxeram enormes oportunidades para o desenvolvimento socioeconómico. Actualmente, 95% da população mundial está coberta por uma rede de banda larga móvel e 63% da população mundial utilizava a Internet em 2021 (GSMA, 2022; ITU, 2021). De acordo com a GSMA (2023), em 2023, as tecnologias e serviços móveis geraram 5,2 biliões de USD de valor económico acrescentado ou 5% do PIB. A conectividade digital também demonstrou o seu papel na promoção da resiliência social durante a crise da COVID-19, permitindo que as pessoas continuassem as suas actividades económicas e sociais habituais durante os confinamentos mundiais de 2020-2021 (ICC, 2022).

O comércio digital também tem vindo a expandir-se a um ritmo impressionante. Em termos de comércio de mercadorias de comércio electrónico, a UNCTAD estima que as vendas globais de comércio electrónico ascenderam a 26,7 biliões de USD em 2019, com o comércio electrónico B2B a representar 82% de todo o comércio electrónico (UNCTAD, 2021). A pandemia da COVID-19 alterou, sem dúvida, o comportamento de aquisições, que passou de offline para online (UNCTAD, 2021). O comércio de serviços prestados por via digital também tem vindo a aumentar ao longo dos anos, crescendo cerca de 7% ao ano entre o período de 2005-2021. Em 2021, as exportações de serviços prestados por via digital ascenderam a 3,8 biliões de USD, representando aproximadamente 63% do comércio mundial de serviços, de acordo com o UNCTADStat.

Os dados estão integrados em todas as tecnologias de ponta que estão a impulsionar a economia digital.[1] Os dados não servem apenas como um contributo para a produção de bens e serviços, mas possuem também características únicas (ver Quadro 1) que lhes permitiram tornar-se um factor de competitividade das empresas (Hagiu & Wright, 2020). Tal como referido por Giddlings et al. (2021), "a digitalização económica e financeira em curso está a fazer dos dados individuais um contributo fundamental e uma fonte de valor para as empresas de todos os sectores, desde as grandes tecnologias e os produtos farmacêuticos até aos fabricantes e prestadores de serviços financeiros. Os dados sobre o comportamento e as escolhas humanas - os nossos "gostos", padrões de compra, localização, actividades sociais, biometria e escolhas de financiamento - estão a ser gerados, recolhidos, armazenados e processados a uma escala sem precedentes."

1 ADBC - inteligência artificial, blockchain, nuvem e dados - são considerados o alfabeto do futuro. Ver (GovTech Singapore, 2018; CloudSufi, 2021)

Quadro 1. As características únicas dos dados

O valor acrescentado dos dados provém do processamento, transmissão, armazenamento e combinação de dados. Os dados são intangíveis e não rivais, o que significa que muitas pessoas podem utilizar os mesmos dados simultaneamente ou ao longo do tempo, sem os esgotar. Ao mesmo tempo, o acesso aos dados pode ser limitado por meios técnicos ou legais, o que resulta em vários graus de exclusão. Por exemplo, os dados recolhidos pelas principais plataformas globais não estão facilmente disponíveis para utilização por terceiros, o que confere aos proprietários das plataformas uma posição monopolista para beneficiarem dos dados. Além disso, os valores agregados podem muitas vezes ser superiores à soma dos valores individuais, especialmente se combinados com outros dados complementares. [...]

Além disso, os dados são de natureza multidimensional. De uma perspectiva económica, podem proporcionar não só valor privado para aqueles que recolhem e controlam os dados, mas também valor social para toda a economia. O valor social não pode ser assegurado apenas pelos mercados. Além disso, a distribuição dos ganhos de rendimento privado provenientes dos dados é altamente desigual. Consequentemente, é necessário que a definição de políticas apoie os objectivos de eficiência e equidade. No entanto, há também dimensões não económicas a considerar, uma vez que os dados estão estreitamente relacionados com a privacidade e outros direitos humanos, bem como com questões de segurança nacional, que devem ser abordadas. Do ponto de vista dos benefícios socioeconómicos, os dados podem servir como condições fundamentais ou facilitadores que permitem aos governos prestar serviços públicos mais eficazes, oferecer uma gestão ambiental efectiva e melhorar a transparência e a governação das acções governamentais.

Devido a estes benefícios, foi sublinhada a necessidade de dados abertos, normas de interoperabilidade 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 utilização indevida dos dados; criar e manter um sistema nacional integrado de dados que permita o fluxo de dados entre um vasto leque de utilizadores de uma forma que facilite a utilização e reutilização seguras dos dados.

Fonte: (UNCTAD, 2021; African Union, 2022)

1.2. O POTENCIAL DA ECONOMIA DIGITAL EM ÁFRICA

A economia digital de África está pronta para se tornar uma fonte de crescimento enorme e resistente. O continente registou um crescimento substancial do número de telemóveis, com 61% e 40% da população a ter agora acesso a telemóveis e à Internet, respectivamente. O crescimento dos serviços de banda larga é impressionante, liderado pela banda larga móvel, que atingiu 42% da população em 2022 (ITU, 2022). De acordo com um relatório elaborado conjuntamente pela SFI e pela Google (2020), a economia digital africana tem potencial para acrescentar até 180 mil milhões de USD ao Produto Interno Bruto (PIB) de África até 2025. Actualmente, dezanove dos vinte países com o crescimento mais rápido do mundo encontram-se em África. O continente tem também a mão de obra mais jovem, de crescimento mais rápido e cada vez mais urbanizada do mundo (Google & SFI, 2020). Espera-se que estes dados demográficos, associados a uma maior longevidade e níveis de educação, a grandes investimentos em infra-estruturas de TIC e a uma maior concorrência entre os fornecedores de serviços Internet (FSI), impulsionem tanto a procura como a capacidade de oferta de bens e serviços digitais, contribuindo para o crescimento económico digital do continente.

Embora ainda enfrente vários desafios em termos de infra-estruturas e de governação, a economia digital africana é impulsionada por empresários digitais jovens e dinâmicos. As empresas emergentes estão a resolver alguns dos problemas mais difíceis de África, como o acesso a cuidados de saúde para populações em zonas periféricas, oportunidades de emprego para mulheres e a capacidade de enviar e receber dinheiro de forma segura. Muitos consumidores africanos passaram directamente do dinheiro para os pagamentos móveis sem nunca terem tido um cartão bancário - uma história admirada e seguida por muitos países a nível mundial (Smart Africa Alliance, 2021). A história de sucesso do cenário de pagamentos móveis em África reforçou a credibilidade da criação de uma solução africana. Os novos modelos de negócio em África estão agora a aproveitar as tecnologias avançadas - adaptadas a abordagens orientadas por dados, escaláveis e pan-africanas (Google & SFI, 2020).

Os mercados de dados em África estão em vias de duplicar a cada cinco ou seis anos. Estima-se que o valor dos mercados de dados em África atinja mais de 3 mil milhões de USD até 2025, crescendo mais de 12% entre 2019 e 2025 (Koigi, 2020). O sector recebeu investimentos de 2,6 mil milhões de USD em 2021 (Research and Markets, 2022). A indústria africana de centros de dados tem testemunhado um interesse constante dos principais fornecedores mundiais de serviços de nuvem, como a AWS e a Microsoft, juntamente com a Huawei, nos últimos cinco anos (Koigi, 2020).

1.3. O PAPEL FUNDAMENTAL DOS DADOS NA TRANSIÇÃO AFRICANA PARA A ECONOMIA DIGITAL

Os dados têm vindo a contribuir cada vez mais para as transformações digitais e tecnológicas, alimentando novos modelos de negócio. De facto, os dados têm sido referidos como o novo petróleo (Rotella, 2012), porque, embora tanto os dados como o petróleo tenham um valor intrínseco, ambos têm de ser "refinados" ou transformados de outra forma para realizarem todo o seu potencial (World Bank, 2021). Actualmente, os dados são considerados um activo e uma fonte potencial de crescimento e inovação. O volume crescente de dados pessoais, não pessoais, industriais e públicos, combinado com tecnologias emergentes como a Inteligência Artificial (IA), a Internet das Coisas (IoT) e a computação em nuvem, teve um impacto dramático na forma como os dados são recolhidos, armazenados, processados e transmitidos em todo o mundo. A importância dos dados para as sociedades modernas exige uma perspectiva política estratégica e de alto nível que possa equilibrar múltiplos objectivos políticos - desde a libertação do potencial económico e social dos dados até à atenuação dos riscos associados à recolha e ao tratamento em massa de dados pessoais.

Para África, a transformação digital pode criar oportunidades significativas num futuro próximo. A produção e a utilização cada vez maiores de dados têm a possibilidade de apoiar o desenvolvimento de uma economia e de uma sociedade sustentáveis e inclusivas, baseadas em dados, em conformidade com as aspirações da Agenda 2063. Para permitir que os países tirem proveito da quantidade substancial de dados pessoais, não pessoais, industriais e públicos gerados pelos seus cidadãos e indústrias e também para facilitar o fluxo fácil de dados entre sectores e além-fronteiras, é necessário promover o estabelecimento de um espaço comum de dados e a criação de um ambiente político favorável e de apoio para impulsionar a inovação e a introdução de novos modelos de negócio.

Os líderes do continente indicam um forte apoio à definição de prioridades e à aceleração da digitalização. A Estratégia de Transformação Digital da União Africana (UA), adoptada pela

Cimeira da UA em Fevereiro de 2020, apela, entre outras recomendações, ao desenvolvimento de abordagens e políticas continentais sobre questões transversais como a protecção de dados, a identificação digital, a segurança cibernética e as tecnologias emergentes. O Quadro de Política de Dados para a União Africana, desenvolvido em 2021 por um Grupo de Trabalho Pan-Africano e aprovado pela Cimeira da União Africana em Fevereiro de 2022, estabelece uma visão comum, princípios, prioridades estratégicas e recomendações fundamentais para orientar os Estados-membros da UA no desenvolvimento dos seus sistemas e capacidades nacionais de dados para retirar valor efectivo dos dados que estão a ser gerados pelos cidadãos, entidades governamentais e indústrias. Além disso, o Quadro visa optimizar os fluxos de dados transfronteiriços, reforçar e harmonizar os quadros de governação de dados em África e, assim, criar um espaço de dados partilhado e normas que regulem a intensificação da produção e utilização de dados em todo o continente.

O Acordo de Comércio Livre Continental Africana (ZCLCA) constitui uma oportunidade de cooperação em aspectos importantes da transformação digital e da política de dados. A adopção mais generalizada dos fundamentos digitais das iniciativas continentais, como o ZCLCA, será essencial para concretizar os benefícios de uma maior cooperação económica. Tal pode ser facilitado por regras que exijam uma melhor interoperabilidade transfronteiriça dos dados, criando assim uma abordagem continental harmonizada da economia digital baseada em dados. Esta abordagem deve encontrar um equilíbrio entre, por um lado, a promoção dos benefícios socioeconómicos do comércio digital e do comércio electrónico e, por outro, a garantia de que as informações sensíveis permaneçam seguras e protegidas e de que os regulamentos pertinentes sobre a protecção de dados pessoais sejam respeitados. As negociações em curso do Protocolo do ZCLCA sobre o Comércio Digital proporcionam uma oportunidade única para os Estados-membros da UA harmonizarem os regulamentos da economia digital, incluindo os regulamentos relativos aos dados, para apoiar o crescimento económico colectivo de uma perspectiva comercial.

Neste contexto, este resumo de políticas tem como objectivo fornecer um mapa fundamental de princípios e directrizes (incluindo recomendações) para promover a utilização responsável, segura e equitativa de dados em acordos comerciais no contexto das negociações em curso do protocolo do ZCLCA sobre o comércio digital, bem como as negociações prospectivas do ZCLCA sobre serviços e bens digitais (a segunda fase). Mais significativamente, o protocolo sobre o comércio digital lançará as bases para um mercado digital único continental.

2. PANORAMA DA POLÍTICA GLOBAL DE DADOS

2.1 TENDÊNCIAS NA GOVERNAÇÃO DOS FLUXOS DE DADOS

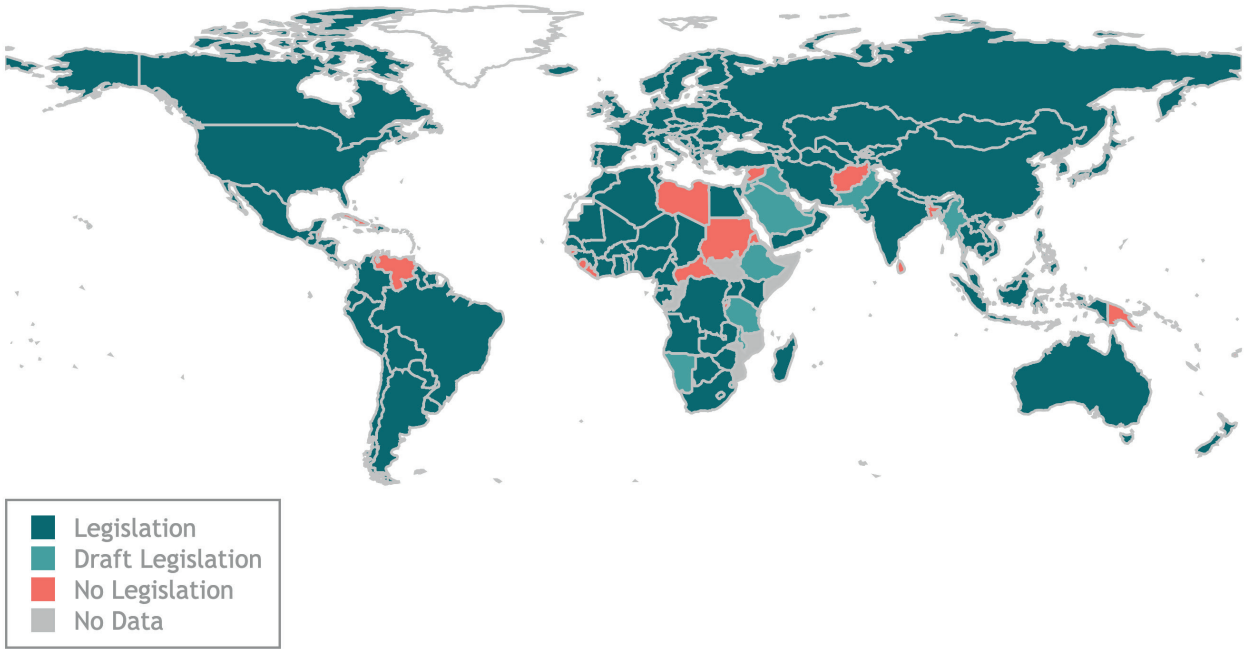
2.1.1. PANORAMA GLOBAL E REGIONAL DA GOVERNAÇÃO DE DADOS

Como os dados são cada vez mais parte integrante da sociedade contemporânea e a sua importância continua a crescer na era digital, o papel de uma governação de dados eficaz não pode ser subestimado. A governação dos fluxos de dados tornou-se uma questão crucial, uma vez que os dados têm um valor económico considerável e merecem uma utilização adequada e a protecção de informações sensíveis. Como tal, tem havido várias tendências na governação dos fluxos de dados, cada uma delas procurando responder aos desafios colocados durante a recolha, o tratamento, a utilização e a monetarização dos dados.

Os quadros de governação dos dados têm sido impulsionados pela necessidade de equilibrar a importância crescente dos dados como um activo e a necessidade de proteger os direitos de privacidade das pessoas. Este facto dá origem a diversos focos de diferentes jurisdições na regulação de questões relacionadas com os dados, dependendo das opiniões dos Estados sobre quem deve "controlar" os dados. Por exemplo, existem actualmente três focos principais dos três reinos digitais. Os Estados Unidos centram-se no controlo dos dados pelo sector privado, a China dá ênfase ao controlo dos dados pelo Governo, enquanto a União Europeia (UE) favorece o controlo dos dados pelos indivíduos com base em direitos e valores fundamentais (UNCTAD, 2021).

Uma das tendências mais proeminentes na governação dos fluxos de dados é a adopção de leis de protecção de dados (UNCTAD, 2016). As leis de protecção de dados procuram regular a recolha, o tratamento e o armazenamento de dados pessoais (Crocetti, Peterson, & Hefner, n.d.). Em Dezembro de 2021, cerca de 71% dos países a nível mundial tinham implementado leis sobre protecção de dados e privacidade, enquanto 9% tinham projectos de legislação (Figura 1) (UNCTAD, 2021). A nível mundial, a legislação e a regulamentação em matéria de protecção de dados variam consoante os países e, no caso dos EUA, por exemplo, variam consoante os Estados. Entre toda a legislação existente sobre protecção de dados, o Regulamento Geral sobre a Protecção de Dados (RGPD) da UE é considerado o conjunto mais rigoroso de regras de privacidade, o que deu origem a várias leis de privacidade de dados semelhantes ao RGPD (Satariano, 2018; Simmons, 2022) (Satariano, 2018; Simmons, 2022).

Figura 1. Legislação sobre Protecção de Dados e Privacidade no Mundo, 2021



Fonte: UNCTAD (2021)

Além disso, tem-se verificado uma convergência crescente no sentido de uma maior transparência na governação dos fluxos de dados. Existem maiores expectativas, tanto por parte das entidades reguladoras como dos consumidores, no sentido de uma maior transparência relativamente às práticas relativas aos dados (Harvard Business Review, 2021). Espera-se que as organizações forneçam aos indivíduos informações claras sobre a forma como os seus dados são recolhidos, processados e armazenados.

Muitos países estão também a introduzir cada vez mais regulamentos sobre a localização de dados. Considerando que os dados podem ser sensíveis para a segurança nacional, existe uma preocupação crescente quanto à necessidade de os dados serem armazenados e tratados dentro das fronteiras de um país (Yayboke & Ramos, 2021). Por conseguinte, alguns países estão a introduzir leis que exigem que os dados sejam armazenados na jurisdição onde foram recolhidos. Entre 2017 e 2021, o número de jurisdições com leis de protecção de dados aumentou significativamente, passando de 35 para 62. Esses 62 países implementaram um total de 144 restrições relativas à localização de dados, em contraste com 2017, quando apenas 67 dessas medidas estavam em vigor (Cory & Dascoli, 2021).

Embora sejam considerados necessários por razões de segurança, os requisitos de localização de dados podem criar obstáculos às operações comerciais transfronteiriças e ao comércio internacional (Hinrich Foundation, 2019). As políticas de localização de dados também aumentam o custo do negócio para as empresas estrangeiras, diminuindo assim a sua competitividade global. Num estudo realizado pela Fundação para a Tecnologia da Informação e Inovação, verificou-se que o aumento da restritividade dos dados em 1% pode levar a um declínio de 7% na produção comercial bruta de um país, a um declínio de 2,9% na produtividade, bem como a uma queda de 1,5% nos preços a jusante (Cory & Dascoli, How

Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, 2021).

A localização de dados está estreitamente associada à soberania dos dados. O conceito de soberania dos dados defende que os dados devem estar sujeitos às leis e regulamentos do país em que são gerados. A procura de soberania dos dados é motivada por preocupações sobre o controlo e a propriedade dos dados, particularmente no contexto da computação em nuvem e dos fluxos de dados transfronteiriços (Gao, 2022). Esta preocupação surgiu predominantemente no contexto das empresas multinacionais que podem armazenar dados em vários locais. Certos países, , adoptaram uma posição sobre a soberania dos dados, implementando regulamentos que exigem que as empresas armazenem os dados localmente e permitam ao governo um maior acesso a esses dados (Kuo, 2022).

No outro extremo do espectro, houve iniciativas para apoiar o livre fluxo de dados. Embora os dois conceitos não sejam necessariamente contraditórios, apresentam perspectivas diferentes sobre as abordagens de governação de dados. Já em 2000, a Declaração Conjunta sobre Comércio Electrónico do ACL entre a Jordânia e os EUA salientava a "necessidade de continuar o livre fluxo de informação". Desde então, um número crescente de acordos comerciais regionais (ACR) incorporou aspirações e compromissos semelhantes. Em 2019, a iniciativa Fluxo Livre de Dados com Confiança (DFFT) foi proposta pelo Japão e aprovada pelos membros do grupo de nações do G20

(Kudo & Soble, 2022), enquanto a UE adoptou uma abordagem mais cautelosa para promover o "fluxo livre de dados não pessoais" (European Commission, 2023).

Além disso, os dados abertos, especialmente os dados governamentais abertos, têm-se centrado na transparência e nos aspectos dos dados que permitem a inovação. Um número crescente de países e instituições reconhece que os dados são um recurso valioso que pode ser utilizado para impulsionar a inovação e criar oportunidades (World Bank, n.d.). Como tal, defendem que os dados não sensíveis e não pessoais devem ser de acesso livre e utilizáveis. Muitos governos em todo o mundo estão a abrir cada vez mais os seus dados ao público, disponibilizando-os para utilização por diferentes partes interessadas (OCDE, 2020). Por exemplo, o Governo do Reino Unido lançou o data.gov.uk, um portal em linha com dados publicados pelo governo central, autoridades locais e organismos públicos do Reino Unido sobre uma série de sectores e temas, incluindo a economia, a saúde, os transportes e a educação, entre outros (data.gov.uk, n.d.).

Dada a diversidade de abordagens à governação dos dados, as empresas que se dedicam ao comércio internacional podem, assim, enfrentar dificuldades e custos crescentes de conformidade em várias jurisdições. Para atenuar os desafios colocados por regulamentações variadas, é importante que os países se empenhem no desenvolvimento e na adopção de normas internacionais relativas à governação de dados que possam ajudar a racionalizar e harmonizar as regulamentações. Numerosos quadros internacionais, na sua maioria voluntários, foram concebidos a este respeito para fornecer directrizes sobre as melhores práticas de governação de dados. Apresentam-se a seguir alguns dos quadros mais importantes adoptados a nível mundial. No Anexo 2 é apresentada uma análise mais exaustiva das melhores práticas.

A Organização das Nações Unidas (ONU) desenvolveu um conjunto de princípios relativos à privacidade dos dados que visam promover a utilização responsável dos dados para o desenvolvimento sustentável salvaguardando simultaneamente a privacidade e protegendo os direitos humanos (UN Global Pulse, n.d.). Estes incluem os Princípios das Nações Unidas

sobre Protecção de Dados Pessoais e Privacidade 2018 (os "Princípios") e a Nota de Orientação das Nações Unidas sobre Grandes Dados para a Realização da Agenda 2030: Privacidade, Ética e Protecção de Dados (a "Orientação"). Estes princípios têm por objectivo (i) harmonizar as normas para a protecção de dados pessoais em todo o Sistema das Nações Unidas; (ii) facilitar o tratamento responsável de dados pessoais; e (iii) assegurar o respeito pelos direitos humanos e liberdades fundamentais dos indivíduos, em particular o direito à privacidade. Estes princípios podem também ser utilizados como referência para o tratamento de dados não pessoais (Nações Unidas, 2018).

As Directrizes de Privacidade da Organização para a Cooperação e Desenvolvimento Económico (OCDE) constituem também um importante quadro internacional para a protecção de dados. As Directrizes de Privacidade da OCDE foram adoptadas pela primeira vez em 1980 para orientar o tratamento responsável dos dados pessoais e, desde então, têm sido actualizadas e revistas para se adaptarem à rápida evolução do panorama da privacidade dos dados (OCDE, n.d.). As Directrizes sobre Privacidade da OCDE baseiam-se em determinados princípios fundamentais centrados na importância da qualidade dos dados, da especificação da finalidade, da responsabilidade e dos direitos individuais (OCDE, 2013). Uma das principais características das Directrizes sobre Privacidade da OCDE é a sua ênfase nos fluxos de dados transfronteiriços. As Directrizes da OCDE em matéria de privacidade sublinham a importância de adoptar leis abrangentes de protecção de dados que incluam disposições relativas às transferências transfronteiriças de dados, sendo necessário manter salvaguardas adequadas nessas transferências. Além disso, as Directrizes referem que quaisquer limitações impostas ao fluxo transfronteiriço de dados devem ser proporcionais aos riscos (OCDE, 2013).

O Quadro de Privacidade da APEC estabelece princípios para a recolha, detenção, processamento, utilização, transferência ou divulgação de informações pessoais aplicados a pessoas ou organizações dos sectores público e privado que controlam cada um dos processos acima referidos. Este quadro promove uma abordagem flexível da protecção da privacidade da informação nas economias membros da APEC, evitando ao mesmo tempo a criação de barreiras desnecessárias aos fluxos de informação (APEC, 2005). Ao implementar o Quadro de Privacidade da APEC, o Sistema de Regras de Privacidade Transfronteiriça da APEC (CBPR) fornece uma certificação de privacidade de dados apoiada pelo governo à qual as empresas podem aderir para demonstrar a conformidade com protecções de privacidade de dados reconhecidas internacionalmente (APEC, 2019). O sistema CBPR exige que as empresas participantes criem e apliquem políticas de privacidade de dados coerentes com o Quadro de Privacidade da APEC.

Uma iniciativa mais recente, o Fluxo Livre de Dados com Confiança (DFTT) do Fórum Económico Mundial (FEM), visa facilitar o livre fluxo de dados, garantindo simultaneamente a confiança na privacidade e segurança dos dados. A iniciativa DFFT baseia-se na premissa de que o livre fluxo de dados é crucial para o crescimento económico e a inovação e que a protecção dos dados e a privacidade são fundamentais para manter a confiança na economia digital (WEF, 2020). Assim, a iniciativa procura encontrar um equilíbrio entre a promoção do livre fluxo de dados e a protecção das informações pessoais. Em 2021, foi adoptado um roteiro para a cooperação, centrado em quatro áreas de cooperação, nomeadamente a localização de dados; a cooperação regulamentar; o acesso dos governos aos dados; e a partilha de dados para sectores prioritários (Arasasingham & Goodman, 2023). Em 2022, foi elaborado um plano de acção. Dado o seu âmbito internacional e o enfoque no sector privado, a iniciativa poderia ajudar a reduzir a fragmentação regulamentar a nível mundial, o que facilitaria o acesso das empresas e a utilização de dados além-fronteiras.

O RGPD da UE tem regulamentos abrangentes e sólidos sobre a protecção de dados pessoais. Dada a sua profundidade e o seu vasto âmbito de aplicação, o RGPD serviu de inspiração para o desenvolvimento de legislação em todo o mundo. O RGPD da UE é aplicado fora do território da eu. Exige o consentimento para o tratamento, a recolha ou a utilização de informações sobre os cidadãos da UE, reconhece os direitos de privacidade dos titulares dos dados e prevê sanções em caso de incumprimento. O RGPD da UE também impõe restrições ao fluxo transfronteiriço de dados pessoais. De acordo com as disposições do RGPD, os dados pessoais só podem ser transferidos para territórios onde esteja garantido um nível de protecção adequado ao abrigo da legislação nacional. A Comissão Europeia é responsável por determinar a adequação do nível de protecção de dados em países não pertencentes à UE. Apenas alguns países são reconhecidos como tendo leis adequadas (European Commission, n.d.).[2] Quando não existe adequação, as organizações recorrem a outros mecanismos legais para transferir dados pessoais para fora da UE. Estes podem incluir cláusulas contratuais-tipo, regras empresariais vinculativas, códigos de conduta e mecanismos de certificação (Comissão Europeia, n.d.).

O desenvolvimento sólido da legislação sobre protecção de dados reflecte o papel crucial dos dados e do fluxo de dados na economia. Na sociedade moderna, os dados têm sido a força motriz da "inovação baseada em dados" disruptiva e de modelos de negócio rentáveis, como as empresas de plataformas ou os agregadores de dados (Thirani & Gupta, 2017; Redman, 2015). Para além dos seus benefícios económicos, o papel dos dados ultrapassa a perspectiva relativamente estreita dos modelos de negócio de uma empresa para tocar nas múltiplas facetas da sociedade, como a privacidade e a segurança pessoais. Neste contexto, é necessária uma abordagem equilibrada para garantir que os benefícios económicos da inovação baseada em dados sejam captados, enquanto a segurança social e a privacidade pessoal permanecem devidamente protegidas. A próxima secção abordará vários esforços a nível multilateral, regional e nacional para alcançar este ponto de equilíbrio.

2.1.2. ACORDOS COMERCIAIS MULTILATERAIS E REGIONAIS QUE INCLUEM DISPOSIÇÕES SOBRE DADOS

(I) DISCIPLINAS DA OMC SOBRE DADOS

Embora sejam consideradas como "legislação anterior à Internet", as regras multilaterais da OMC em vigor continuam a ter alguma aplicabilidade às medidas de governação dos dados. O princípio da neutralidade tecnológica constitui uma base importante para a aplicação das regras existentes do GATS ao comércio electrónico (Mattoo & Schuknecht, 1999). Basicamente, este princípio procura garantir que não haja distinções políticas entre produtos com base no meio de entrega, permitindo assim a longevidade de uma regra e a aplicação uniforme em diferentes tecnologias (Greenberg, 2016). Um relatório do Conselho da OMC para o Comércio de Serviços (1999) estabelece que "os membros acordaram que o GATS era aplicável a todos os serviços, independentemente dos meios tecnológicos utilizados para a sua prestação. ... Foi observado que o princípio da neutralidade tecnológica também era aplicável aos compromissos calendarizados, excepto se a calendarização especificasse o contrário: era, por conseguinte, possível que os membros calendarizassem os compromissos de uma forma não tecnologicamente neutra" (OMC, 1999). O relatório de progresso da OMC sobre o programa de

2 Os países que foram reconhecidos como tendo legislação adequada sobre protecção de dados pela Comissão da UE incluem Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, República da Coreia, Suíça, Reino Unido e Uruguai.

trabalho relativo ao comércio electrónico confirma igualmente a neutralidade tecnológica do GATS "no sentido em que não contém quaisquer disposições que estabeleçam uma distinção entre os diferentes meios tecnológicos através dos quais um serviço pode ser prestado" (OMC, 1999). Isto proporciona uma base importante para a leitura das listas de compromissos dos membros da OMC: restringir ou proibir os fluxos de dados transfronteiriços, obstruindo assim a prestação transfronteiriça de serviços em sectores em que os membros assumiram compromissos explícitos no GATS, poderia violar a obrigação de acesso ao mercado (Mitchell & Hepburn, 2017).

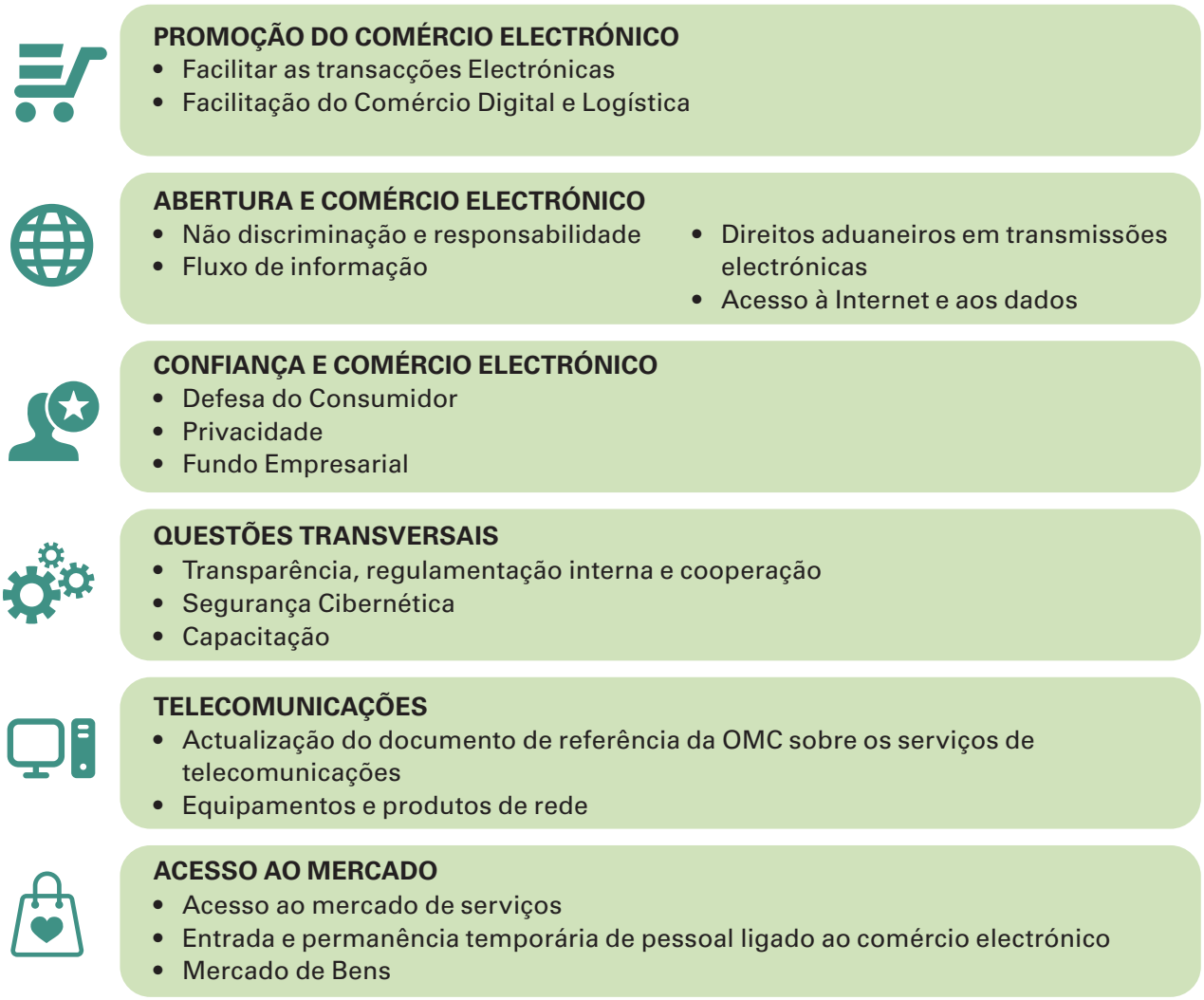
O Acordo Geral sobre o Comércio de Serviços (GATS) da OMC proporciona uma base importante para a imposição de medidas legítimas de protecção dos dados pessoais e da privacidade. Especificamente, a alínea c), subalínea i), do artigo XIV reconhece a importância da protecção da vida privada e, por conseguinte, permite derrogações às obrigações existentes dos membros sempre que seja necessário proteger a vida privada das pessoas relativamente ao tratamento e à divulgação de dados pessoais.[3] A excepção relativa à "moral pública" prevista na alínea a) do artigo XIV do GATS pode também ser interpretada como abrangendo a privacidade. Além disso, o Anexo sobre Telecomunicações do GATS também permite a adopção de medidas "necessárias para garantir a segurança e o sigilo das mensagens."[4] Como regra geral para todas as excepções do GATS, estas medidas não devem ser adoptadas numa base discriminatória ou para fins proteccionistas. No entanto, é também de salientar que o GATS não aborda especificamente a protecção de dados e informações pessoais, o que resulta em lacunas cruciais neste regime de comércio internacional na era digital.

Na ausência de regras explícitas para o comércio digital nos acordos da OMC, a Iniciativa de Declaração Conjunta (JSI) sobre o comércio electrónico representa um passo no sentido da disciplina da governação dos dados. Em 2017, no 11.º Conselho Ministerial, 76 membros da OMC concordaram em iniciar os trabalhos para futuras negociações sobre questões relacionadas com o comércio electrónico, incluindo a governação de dados. O projecto de texto de negociação consolidado da iniciativa conjunta está centrado em seis áreas principais, conforme apresentado na Figura 2. No final de Março de 2023, os participantes envolvidos na iniciativa reuniram-se para discutir várias propostas relacionadas com o comércio electrónico, incluindo o fluxo de dados (OMC, 2023). Numa declaração anterior, foi comunicado que os membros tinham alcançado um bom consenso em áreas como a protecção dos consumidores por via electrónica; mensagens electrónicas comerciais não solicitadas; dados governamentais abertos; e acesso aberto à Internet (WTO, 2021). Entretanto, os membros continuam a encontrar convergência em temas como a protecção de dados e a privacidade, os fluxos de dados transfronteiriços, o código-fonte e a criptografia (OMC, 2023). O mesmo braço de ferro sobre questões de governação de dados está também presente nas negociações do Acordo sobre Comércio de Serviços (TiSA). Por um lado, os EUA defendem a transferência transfronteiriça de informações, incluindo dados pessoais, no âmbito da actividade do prestador de serviços (Berka, 2017). A UE, por outro lado, opõe-se a essa proposta com o argumento de que "o direito à privacidade deve ser reconhecido como um direito fundamental e não como uma barreira comercial" e promove o sistema de adequação (European Parliament, 2016).

3 Artigo XIV (c) (i) do GATS: "Nenhuma disposição do presente Acordo poderá ser interpretada de forma a impedir a adopção ou a aplicação, por qualquer Membro, de medidas: (c) necessárias para garantir o cumprimento de leis ou regulamentos que não sejam incompatíveis com as disposições do presente Acordo, incluindo as relativas a: (i) a protecção da privacidade das pessoas relativamente ao tratamento e divulgação de dados pessoais e a protecção do sigilo dos registos e contas individuais."

4 A alínea d) do n.º 5 do anexo do GATS relativo às telecomunicações estabelece o seguinte "[Um] Membro pode adoptar as medidas necessárias para garantir a segurança e o sigilo das mensagens, sob reserva de que tais medidas não sejam aplicadas de forma a constituir um meio de discriminação arbitrária ou injustificável ou uma restrição dissimulada ao comércio de serviços".

Figura 2. Áreas principais das negociações da JSI sobre Comércio Electrónico da OMC



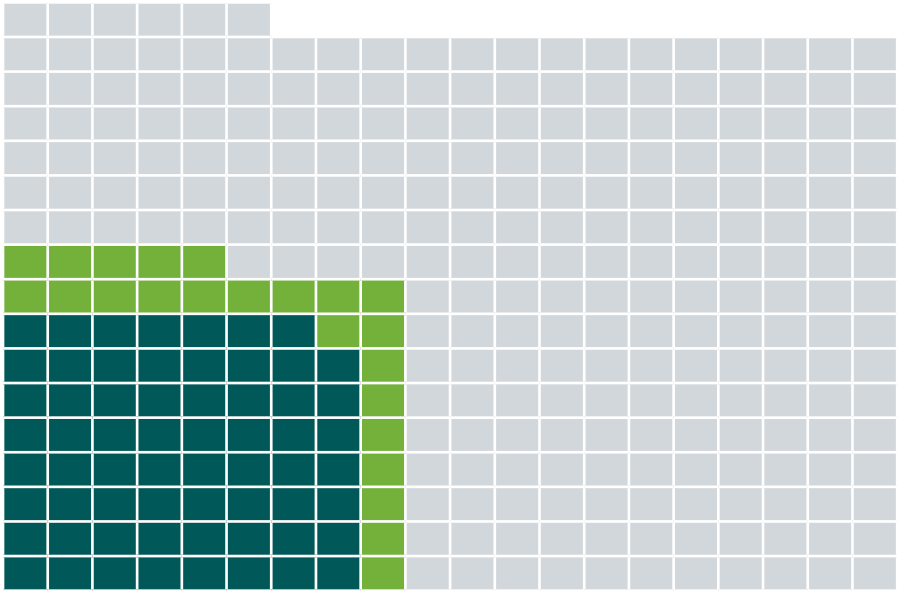
Fonte: (OMC Plurilaterals, n.d.)

(II) DISPOSIÇÕES RELATIVAS AOS DADOS ESSENCIAIS NOS ACR

Um número crescente de ACR inclui disposições relativas ao comércio digital e, subsequentemente, incorpora também certas disposições relativas aos dados. Num estudo recente, Burri (2021) conclui que, dos 347 ACR celebrados entre 2000 e 2019, 184 continham disposições sobre comércio digital, o que corresponde a mais de metade dos ACR assinados durante esse período (Burri, Big Data and Global Trade Law, 2021). A incorporação de tais disposições registou um maior aumento a partir de 2010, com 68% de todos os ACR celebrados entre 2010 e 2019, incluindo algum tipo de disposição sobre comércio digital. Da mesma forma, ao longo dos anos, o número de disposições incluídas nesses capítulos aumentou. Por exemplo, em 2000, o número médio de artigos relativos ao comércio digital era de um. Em 2019, o número médio de artigos relacionados com o comércio digital aumentou para treze (Burri, Big Data and Global Trade Law, 2021). No entanto, é de notar que as disposições contidas nestes capítulos são altamente diversificadas e abordam uma série de temas diferentes, desde o comércio electrónico e o comércio sem papel até à protecção de dados. Além disso, verificou-se igualmente que o nível de aplicação destas disposições varia consoante os acordos.

As disposições relativas aos dados são um fenómeno relativamente novo nos ACR. Os Estados Unidos da América desempenharam um papel proeminente na incorporação de disposições relativas a dados nos seus ACR, insistindo em regras liberais à luz da sua "Agenda Digital" (Burri, Big Data and Global Trade Law, 2021). Os acordos celebrados com a Austrália, Bahrein, Chile, Marrocos, Omã, Peru, Singapura, Panamá, Colômbia e Coreia do Sul continham disposições relativas ao comércio digital, pelo que os EUA foram além dos compromissos da OMC nesta matéria. No entanto, outros países, nomeadamente Singapura, Austrália, Japão e Colômbia, desempenharam igualmente um papel importante na difusão de tais disposições nos ACR (Burri, Big Data and Global Trade Law, 2021). Até 2020, de acordo com a base de dados DESTA, sessenta e três dos 346 ACR assinados desde 2000 (ou 18 % do total) incluem disposições relativas a dados (Figura 3). Ao longo dos anos, o número de ACL, incluindo disposições sobre comércio electrónico, continua a ser superior ao dos que contêm dados, o que indica a ainda relutância dos países em incorporar regras sobre a governação dos dados nos acordos comerciais.

Figura 3. Dados e cobertura do comércio electrónico de todos os ACL assinados desde 2000



25%
(**86** de 346) do ACL abrange as disposições sobre o comércio eletrónico

18%
(**63** de 346) do ACL abrange o fornecimento de dados. Também cobrem disposições de comércio eletrónico.

ALC que inclui apenas disposições sobre o comércio eletrónico.

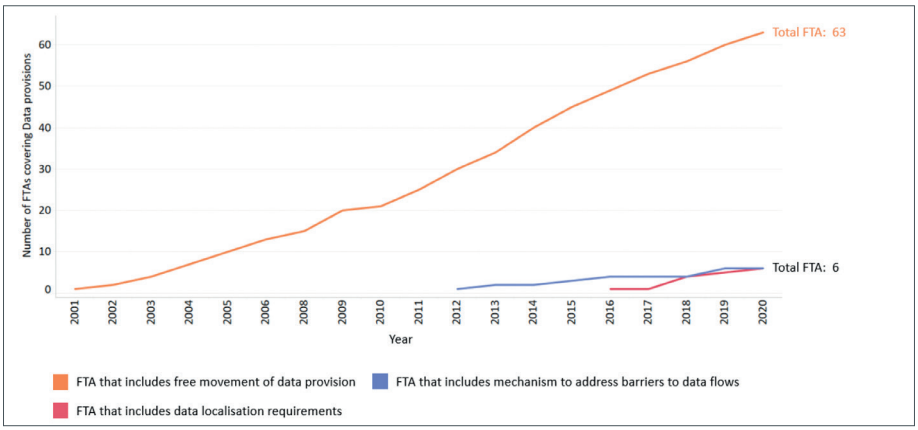
ALC que inclui disposições sobre dados e comércio eletrónico.

ALC que não inclui dados e disposições sobre o comércio eletrónico.

Fonte: Cálculos do autor baseados em (Dür, Baccini, & Elsig, 2022)

Embora a disposição relativa à livre circulação de dados tenha sido incluída desde 2001, as disposições relativas aos mecanismos destinados a eliminar os obstáculos aos fluxos de dados só começaram em 2012. A primeira inclusão foi no acordo da Aliança do Pacífico. No final de 2020, seis acordos deste tipo em todo o mundo incluíam disposições destinadas a eliminar os obstáculos aos fluxos de dados. Trata-se dos acordos da Aliança do Pacífico, da UE-Colômbia e do Peru, do México-Panamá, do Japão-Mongólia, da Argentina-Chile e da UE-Japão. A partir de 2016, os requisitos de localização de dados começaram a ser incluídos nos ACL. O primeiro foi o acordo Japão-Mongólia, que entrou em vigor em 2016. No final de 2020, seis acordos incluíam requisitos de localização de dados (Figura 4).

Figura 4. ACL com disposições relativas a dados aplicadas desde 2000, por tipo de cobertura



Fonte: Cálculos do autor baseados em (Dür, Baccini, & Elsig, 2022)

(III) UMA ANÁLISE EXAUSTIVA DAS DISPOSIÇÕES RELATIVAS AOS DADOS EM ACR SELECCIONADOS

Esta secção avalia alguns dos acordos mais recentes e abrangentes que incluem disposições sobre a governação dos dados. No total, foram avaliados 6 ACR relativamente a 14 tipos diferentes de disposições. A Tabela 1 destaca a cobertura das diferentes disposições relativas a dados contidas nos ACR seleccionados.

Tabela 1. Cobertura das diferentes disposições relativas aos dados nos ACR

Agreements	Cross Border Data Flows	Data Localisation	Data Protection	Digital Identities	Open Government Data	Data Innovation	Digital Inclusion	Cooperation	Cybersecurity	Cryptography	Source Code	Online Safety & Security	Spam
CPTPP	Y	Y	Y	N	N	N	N	Y	Y	N	Y	Y	Y
DEPA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
EU-UK TCA	Y	N	Y	N	Y	N	N	Y	Y	N	Y	Y	Y
UK-Singapore DEA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
USMCA	Y	Y	Y	N	Y	N	N	Y	Y	N	Y	Y	Y
RCEP	Y	Y	Y	N	N	N	N	Y	Y	N	N	Y	Y

N	The Agreement does not include a specific provision on the subject
Y	The Agreement includes a specific provision on the subject
	Data governance provisions
	Provisions related to responsible, secure and equitable use of data

*Spam or also Unsolicited Commercial Electronic Messages

Fonte: Compilação do autor

Em termos de cobertura, verifica-se que todos os seis ACR seleccionados incluem disposições sobre a governação dos dados. A Parceria para a Economia Digital (DEA) entre o Reino Unido e Singapura é o acordo mais ambicioso estudado no contexto do presente relatório, abrangendo os 14 tipos diferentes de disposições avaliadas. Segue-se o Acordo de Parceria para a Economia Digital (DEPA), que contém 13 dos 14 tipos de disposições relativas aos dados. O único domínio não abrangido pelo DEPA, neste caso, diz respeito às disposições relativas ao código-fonte. Em contrapartida, os acordos com menos disposições sobre dados são o Acordo de Comércio e Cooperação UE-Reino Unido (ACC) e a Parceria Económica Regional Abrangente (RCEP), com apenas oito áreas diferentes abrangidas em cada um deles.

Em todos os ACR, o livre fluxo de informação é incluído como uma disposição importante. A primeira menção ao livre fluxo de informações em qualquer ACL remonta ao ACL entre a Jordânia e os EUA de 2000, em que a Declaração Conjunta sobre Comércio Electrónico expressava a "necessidade de continuar o livre fluxo de informações" (Burri, Big Data and Global Trade Law, 2021). Os acordos comerciais recentes incluem disposições mais substanciais sobre o livre fluxo de informações. De acordo com o artigo 8.61F do DEA Reino Unido-Singapura, nenhuma das Partes "deve proibir ou restringir a transferência transfronteiriça de informações por meios electrónicos, incluindo informações pessoais, se esta actividade se destinar à realização de negócios de uma pessoa abrangida." O CPTPP, por sua vez, afirma que "cada Parte deve permitir a transferência transfronteiriça de informações por meios electrónicos, incluindo informações pessoais, quando esta actividade se destinar à realização de negócios de uma pessoa abrangida." A redacção dos outros quatro acordos é semelhante a este respeito e, por conseguinte, existe uma maior convergência no sentido de adoptar disposições vinculativas a este respeito.

Com a excepção do TCA entre a UE e o Reino Unido, todos os acordos avaliados incluem disposições que limitam a aplicação dos requisitos de localização de dados. Nos cinco acordos, é proibido impor restrições à localização de dados. O artigo 4.4.2 do DEPA afirma que "nenhuma Parte pode exigir que uma pessoa abrangida utilize ou localize instalações informáticas no território dessa Parte como condição para efectuar negócios nesse território", e a linguagem contida nos outros acordos é muito semelhante. De facto, a maioria dos ACR que incluem disposições sobre a localização de dados incluem uma linguagem forte e compromissos vinculativos. O primeiro acordo com compromissos vinculativos sobre a localização de dados foi o ACL entre o Japão e a Mongólia, em 2015. As negociações do TPP influenciaram grandemente essas disposições em acordos posteriores, incluindo o CPTPP e o USMCA, entre outros (Burri, Big Data and Global Trade Law, 2021).

No que diz respeito à protecção dos dados pessoais, cinco dos seis acordos implicam compromissos vinculativos. Para além do TCA entre a UE e o Reino Unido, as disposições relativas à protecção de dados pessoais são coerentes em todos os ACR. Por exemplo, de acordo com o artigo 19.8.2 do USMCA, "cada Parte deve adoptar ou manter um quadro jurídico que preveja a protecção de dados pessoais dos utilizadores do comércio digital..." A maioria dos acordos também estabelece que qualquer quadro jurídico adoptado deve estar em conformidade com as normas e os princípios internacionais. Para este efeito, o USMCA remete para o Quadro de Privacidade da APEC e para a Recomendação do Conselho da OCDE relativa às Directrizes que regem a Protecção da Privacidade e os Fluxos Transfronteiriços de Dados Pessoais (2013). Além disso, os acordos também incluem disposições vinculativas que exigem a adopção de práticas não discriminatórias na protecção dos utilizadores do comércio digital contra violações da protecção das informações pessoais e a publicação das protecções das informações pessoais que proporcionam aos utilizadores do comércio digital.

Para além destas três áreas fundamentais da governação dos dados, um número crescente de ACR procura também incorporar disposições destinadas a garantir a utilização responsável, segura e equitativa dos dados. Para esta avaliação, foram identificados e avaliados 11 domínios diferentes, de acordo com a Tabela 1. A este respeito, as disposições contêm uma combinação de compromissos vinculativos e não vinculativos. Por exemplo, no que diz respeito à transferência e ao acesso aos códigos-fonte, os quatro acordos em que o assunto é abordado incluem compromissos vinculativos. A este respeito, o CPTPP afirma que "nenhuma Parte exigirá a transferência ou o acesso ao código-fonte de software detido por uma pessoa de outra Parte, como condição para a importação, distribuição, venda ou utilização do referido software, ou de produtos que contenham esse software, no seu território". No outro extremo

do espectro, as disposições sobre inovação digital, contidas apenas no DEPA e no DEA entre o Reino Unido e Singapura, por exemplo, são disposições de melhor esforço e, por conseguinte, não são vinculativas.

2.2 POLÍTICA AFRICANA E QUADRO REGULAMENTAR SOBRE O FLUXO DE DADOS

O continente africano tem vindo a embarcar proactivamente na jornada da transformação digital. Em 2020, a Cimeira da UA adoptou a **Estratégia de Transformação Digital da UA (ETD)** para África 2020-2030, que visa orientar uma resposta africana comum e coordenada aos desafios e oportunidades da Quarta Revolução Industrial (4IR), uma vez que estabelece os objectivos de alcançar o acesso universal às redes digitais e estabelecer um Mercado Único Digital (DSM) até 2030.

De acordo com a estratégia da UA para a a criação de um ambiente político e regulamentar favorável ao mercado único digital em África, o mercado único de dados é identificado como um dos três pilares fundamentais que apoiam a realização do DSM africano.[5] Para concretizar os potenciais benefícios de um mercado comum de dados, são necessários quadros jurídicos favoráveis em todos os países africanos para permitir e facilitar o livre fluxo de dados. Os quadros jurídicos favoráveis são fundamentais para o desenvolvimento de um mercado comum de dados em África porque fornecem as regras e regulamentos necessários para o livre fluxo de dados através das fronteiras. Esses quadros são necessários para garantir que os dados possam ser recolhidos, partilhados e analisados sem interferir nos direitos individuais, nas preocupações de segurança nacional ou nas leis de propriedade intelectual. Ao fornecer um conjunto claro e consistente de regras e regulamentos para a recolha, partilha e análise de dados, estes quadros podem ajudar a desbloquear o potencial do desenvolvimento baseado em dados em África. As secções seguintes, subcapítulos 2.2.1 e 2.2.2, destacam alguns dos principais avanços alcançados a este respeito a nível regional e nacional, respectivamente.

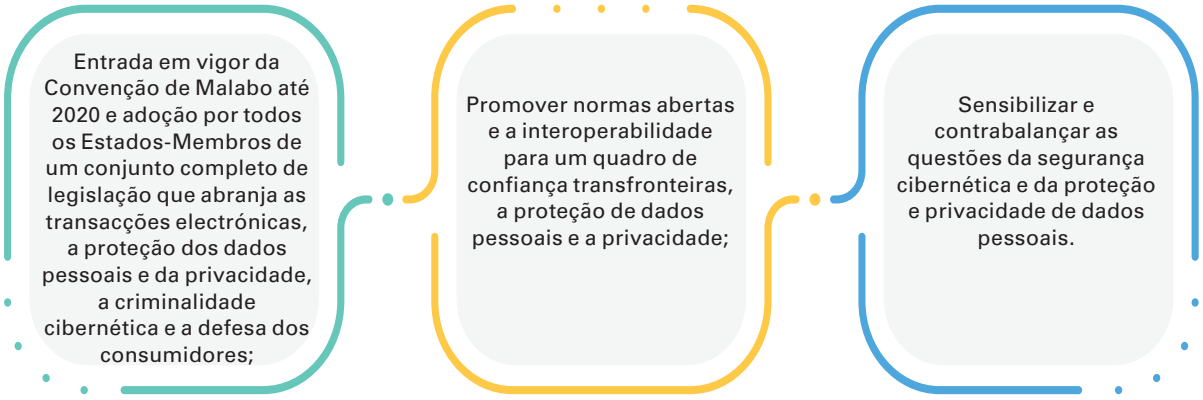
2.2.1 QUADROS CONTINENTAIS E REGIONAIS

(I) ESTRATÉGIA DE TRANSFORMAÇÃO DIGITAL PARA ÁFRICA

A Estratégia de Transformação Digital para África (ETD) para o período 2020-2030 é o principal instrumento que orienta o percurso digital do continente. A ETD, aprovada na 36.ª Sessão Ordinária do Conselho Executivo da União Africana, visa aproveitar as tecnologias digitais e a inovação para transformar as sociedades e economias africanas, entre outros aspectos, para o desenvolvimento socioeconómico do continente e garantir a apropriação por África de ferramentas modernas de gestão digital (African Union, 2020). A ETD estabelece a agenda para uma maior coerência entre as políticas e estratégias digitais existentes e futuras, a fim de posicionar África como um parceiro estratégico na economia digital global. Reconhecendo que os dados são um motor essencial para a transformação digital, a integração, a inovação e o empreendedorismo, o comércio e os serviços financeiros, a ETD assinalou os desafios em torno do desenvolvimento e da utilização de dados de qualidade e propôs várias recomendações políticas e acções para melhorar o acesso e a utilização dos dados. Alguns dos objectivos específicos da ETD relacionados com a governação de dados são apresentados a seguir.

5 Os três pilares são: Mercado Único da Conectividade; Mercado Único dos Dados; e Mercado Único Electrónico. Ver (União Africana,, Fevereiro 2024).

Figura 5. Os objectivos específicos da ETD relativos à governação dos dados



Fonte: (African Union, 2020)

A ETD apresenta um roteiro ambicioso em matéria de governação e protecção de dados. Uma das recomendações propostas no âmbito da ETD é garantir que a Convenção de Malabo seja coerente com as normas internacionais, a fim de assegurar a competitividade das empresas africanas nos mercados globais. O instrumento fixou o objectivo de estabelecer regulamentos em 10 das 14 áreas relacionadas com os dados (conforme identificado na secção 2.1.2). As únicas áreas em que a ETD não especificou pormenores sobre a transferência e o acesso ao código fonte em fluxos transfronteiriços, mensagens comerciais não solicitadas, produtos que utilizam criptografia e inovação de dados. Assim, se devidamente implementados e aplicados, os objectivos da ETD resultariam num panorama regulamentar bastante robusto para os países africanos. Neste sentido, o âmbito e a cobertura ambiciosos da ETD podem servir como uma orientação importante para os negociadores no contexto da negociação das disposições relativas aos dados no âmbito do Protocolo sobre o Comércio Digital do ZCLCA.

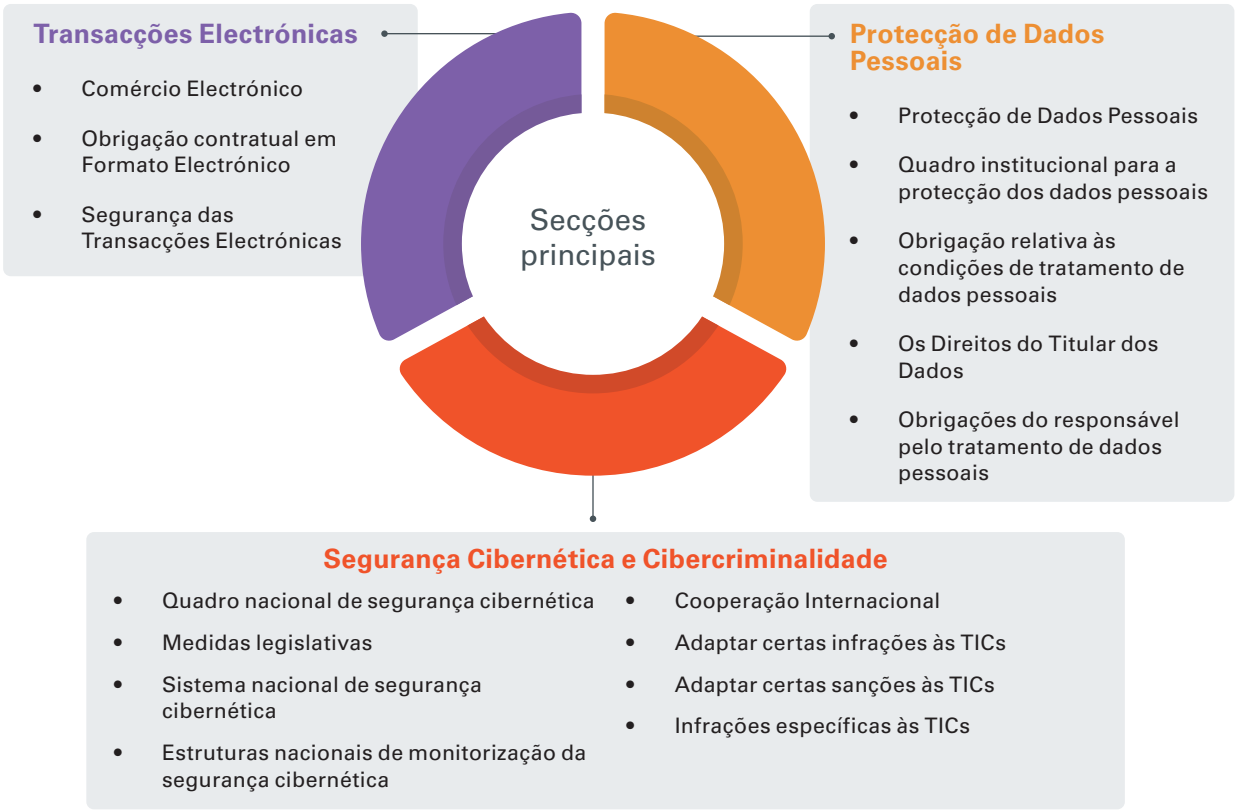
(II) CONVENÇÃO DE MALABO

Na última década, África assistiu ao desenvolvimento de vários instrumentos de governação destinados a abordar e facilitar a criação e o reforço dos ecossistemas digitais africanos. Em Junho de 2014, a União Africana adoptou a Convenção da UA sobre Segurança Cibernética e Protecção de Dados Pessoais (Convenção de Malabo) para estabelecer um quadro credível para a segurança cibernética e a protecção de dados em África. A Convenção de Malabo foi desenvolvida tendo em conta a importância crescente dos dados e das tecnologias digitais em África e a necessidade de quadros jurídicos abrangentes para reger a sua utilização. A Convenção de Malabo visa estabelecer "*as regras essenciais para a criação de um ambiente digital credível (espaço cibernético) e colmatar as lacunas que afectam a regulamentação e o reconhecimento jurídico das comunicações electrónicas e da assinatura electrónica, bem como a ausência de regras jurídicas específicas que protejam os consumidores, os direitos de propriedade intelectual, os dados pessoais e os sistemas de informação e a privacidade em linha*" (African Union Commission, 2018).

A Convenção centra-se em três áreas fundamentais, nomeadamente as transacções electrónicas, a protecção de dados pessoais e a segurança cibernética e a criminalidade cibernética. A Convenção será fundamental para o desenvolvimento de normas comuns que promovam e regulem a utilização de dados no continente. A Convenção fornece aos países um quadro jurídico comum e visa estabelecer um ecossistema propício à transmissão e partilha de dados entre fronteiras. As várias secções da Convenção são resumidas a seguir. Além disso,

a Convenção também reconhece a importância dos fluxos de dados transfronteiriços para o desenvolvimento económico em África. Permite o livre fluxo de dados através das fronteiras, sujeito a salvaguardas adequadas para a protecção de dados e a segurança cibernética. A convenção exige igualmente que os países estabeleçam mecanismos para o reconhecimento mútuo das normas de protecção de dados e para a resolução de litígios relacionados com os fluxos de dados transfronteiriços.

Figura 6: Secções principais da Convenção de Malabo



Fonte: (African Union Commission, 2018)

A ratificação da Convenção de Malabo tem sido lenta devido a vários factores. Em Maio de 2023, 19 dos 55 Estados-membros africanos assinaram a Convenção, dos quais 15 procederam à ratificação (African Union, 2023). A última ratificação foi efectuada pela Mauritânia em 9 de Maio de 2023, o que desencadeou a entrada em vigor da Convenção em 8 de Junho de 2023 (Ayalew, 2023).[6] Uma das principais razões para os atrasos em torno da ratificação e implementação da Convenção pode ser atribuída à falta de dinamismo e vontade política entre os países africanos, muitos dos quais já estabeleceram regulamentos e normas nacionais em matéria de governação de dados (Okwara, 2022). Além disso, tem havido também uma falta de sensibilização para a Convenção entre os países africanos, com marketing insuficiente e dinâmica gerada em torno dela após a sua adopção em 2014. Com a elaboração do Protocolo sobre o Comércio Digital do ZCLCA, existe a oportunidade de promover a ratificação da Convenção de Malabo, uma vez que esta tem o potencial de proporcionar orientação e direcção para as preocupações e desafios decorrentes do comércio digital.

6 Os países que ratificaram a Convenção são Angola, Cabo Verde, Costa do Marfim, Congo, Gana, Guiné, Moçambique, Mauritânia, Maurícias, Namíbia, Níger, Ruanda, Senegal,Togo e Zâmbia.

(III) O QUADRO DA POLÍTICA DE DADOS DA UNIÃO AFRICANA

Outro desenvolvimento importante no que diz respeito à governação de dados no continente africano é o Quadro de Política de Dados da União Africana. O Quadro de Política de Dados da UA foi desenvolvido em reconhecimento das oportunidades apresentadas pela ETD e pelo ZCLCA para abordar e aproveitar o crescimento de dados que será possibilitado pela economia digital de África (African Union, 2022). O Quadro de Políticas representa um passo significativo para a criação de um ambiente consolidado e harmonizado de governação de dados e de dados para permitir o fluxo livre e seguro de dados em todo o continente, salvaguardando simultaneamente os direitos humanos, defendendo a segurança e garantindo o acesso equitativo e a partilha de benefícios.

O quadro estabelece uma visão comum, princípios, prioridades estratégicas e recomendações fundamentais para orientar os países africanos no desenvolvimento dos seus sistemas de dados nacionais e das suas capacidades para utilizarem eficazmente os dados e explorarem o seu valor. Reconhece que os dados são um pré-requisito para a criação de valor, o empreendedorismo e a inovação em África (African Union, 2022). Para desenvolver e aproveitar os dados em África, o Quadro propõe que a geração e o desenvolvimento de dados em todo o continente devem estar em conformidade com os princípios de cooperação; integração; equidade e inclusão; confiança, segurança e responsabilização; abrangência e visão de futuro; e integridade e justiça. Como tal, quando implementado, o Quadro irá:

1. capacitar os cidadãos africanos para o exercício dos seus direitos através da promoção de sistemas de dados fiáveis, seguros e protegidos, integrados com base em normas e práticas comuns;
2. criar, coordenar e capacitar instituições de governação para regular, se necessário, o panorama dos dados em constante mutação e aumentar a utilização produtiva e inovadora dos dados para fornecer soluções e criar oportunidades, atenuando simultaneamente os riscos; e
3. garantir que os dados possam circular tão livremente quanto possível através das fronteiras, assegurando ao mesmo tempo uma distribuição equitativa dos benefícios e abordando os riscos relacionados com os direitos humanos e a segurança nacional (African Union, 2022).

O quadro propõe igualmente que os modelos de dados e a segurança sejam transversais, com ênfase específica no armazenamento em nuvem e no processamento de dados sensíveis/proprietários, na gestão de API e no apoio a economias de dados equitativas (African Union, 2022). O Quadro apresenta um conjunto de recomendações pormenorizadas e acções decorrentes para orientar os Estados-membros através da formulação de políticas no seu contexto nacional, bem como recomendações para reforçar a cooperação entre países e promover os fluxos de dados intra-africanos.

(IV) QUADRO DE INTEROPERABILIDADE DA IDENTIDADE DIGITAL

Um quadro conexo que também foi avançado pela União Africana é o Quadro de Interoperabilidade da Identidade Digital. Os BI digitais têm inúmeras vantagens para uma sociedade em que os governos e as empresas, por exemplo, podem utilizar os BI digitais para racionalizar, expandir e inovar as suas operações e melhorar a prestação de serviços através da digitalização e da automatização, especialmente quando concebidos como uma "pilha digital" com partilha de dados fiáveis e plataformas de pagamento digital. O quadro prevê uma norma comum a nível continental para representar, digitalmente, as provas de identidade

emitidas por fontes fiáveis dos Estados-membros da UA e para assegurar a interoperabilidade em todo o continente. O quadro será fundamental para facilitar o comércio digital, permitindo a utilização de identidades digitais fiáveis e autenticadas, e permitirá a geração de conjuntos de dados que podem apoiar o desenvolvimento de outros serviços em África.

(V) INICIATIVAS REGIONAIS DE LEI-MODELO

A nível regional, várias comunidades económicas regionais africanas (CER) também desenvolveram instrumentos destinados a regulamentar a utilização e o armazenamento de dados nos seus Estados-membros. Entre estas contam-se o quadro jurídico da Comunidade da África Oriental (CAO) para as leis cibernéticas de 2008; a lei complementar da Comunidade Económica dos Estados da África Ocidental (CEDEAO) sobre a protecção dos dados pessoais; as leis-modelo sobre telecomunicações/TIC e segurança cibernética, que incluem disposições sobre protecção de dados, crimes cibernéticos e transacções electrónicas da região da Comunidade Económica dos Estados da África Central (CEEAC); e as leis-modelo da Comunidade para o Desenvolvimento da África Austral (SADC) sobre comércio electrónico/ transacções, protecção de dados, crimes cibernéticos, etc.

O quadro jurídico da CAO para as leis cibernéticas de 2008 foi uma das primeiras iniciativas em África a adoptar um quadro regional harmonizado moderno e eficaz para as leis cibernéticas. O quadro foi concebido para satisfazer as necessidades da região, a fim de apoiar o processo de integração regional no que diz respeito à administração pública electrónica e ao comércio electrónico (UNCTAD, 2012). O quadro inclui dois conjuntos de documentos: O Quadro I abrange as transacções electrónicas, incluindo as assinaturas electrónicas; o crime cibernético; a protecção de dados e a privacidade; a protecção dos consumidores. O Quadro II abrange a propriedade intelectual; concorrência; tributação electrónica; e segurança da informação. No entanto, a transposição destes quadros e regras exigirá mais trabalho para garantir o alinhamento e a aplicação a nível nacional. Entre os seis Estados parceiros da CAO, apenas o Ruanda assinou e ratificou a Convenção da UA sobre Segurança Cibernética e Protecção de Dados Pessoais.

A **Lei Complementar da CEDEAO sobre a Protecção de Dados Pessoais**, assinada a 16 de Fevereiro de 2010, visa estabelecer um quadro jurídico harmonizado para o tratamento de dados pessoais nos seus Estados-membros. A lei é juridicamente vinculativa e os Estados-membros são obrigados a aplicá-la no prazo de dois anos a contar da sua adopção. Assim, cada Estado-Membro é obrigado a estabelecer um quadro jurídico para a protecção dos dados pessoais no que diz respeito à recolha, tratamento, transmissão, armazenamento e utilização de dados pessoais. Além disso, cada Estado-membro deve criar uma autoridade independente de protecção de dados (APD), que é responsável por garantir que os dados pessoais são tratados em conformidade com as disposições da lei. Estão igualmente previstas sanções administrativas e financeiras para combater as violações das disposições da lei por parte dos responsáveis pelo tratamento de dados ou dos subcontratantes (OneTrust, 2022).

Concebida em 2013, a **Lei-Modelo de Protecção de Dados da SADC** serve de quadro geral para os Estados da SADC desenvolverem as suas próprias leis nacionais sobre protecção de dados. Abrange um vasto leque de áreas diferentes, incluindo a criação de uma autoridade de protecção de dados, directrizes sobre a qualidade dos dados, regras gerais sobre o tratamento de dados pessoais, deveres do responsável pelo tratamento de dados e do subcontratante, direitos da pessoa em causa, recurso à autoridade judicial, sanções e fluxos transfronteiriços de informação (ITU, 2013). Baseada em princípios internacionais e compatível com a Convenção

de Malabo, a Lei-Modelo constitui uma base sólida para proteger os dados pessoais e facilitar os fluxos globais de informação, a fim de assegurar a coerência das práticas de protecção de dados nos Estados-membros. No entanto, dado que a Lei-Modelo foi elaborada há mais de uma década, contém numerosas lacunas, pelo que deve ser modernizada e actualizada (SADC, 2021).

2.2.2 QUADROS REGULAMENTARES A NÍVEL NACIONAL

Dada a importância crescente da protecção de dados, vários países africanos começaram a desenvolver políticas e estratégias para promover o desenvolvimento e a utilização de dados. Antes de 2016, apenas 16 países africanos tinham leis relativas à protecção de dados. Em 2021, 33 países, o equivalente a 60% do continente, tinham adoptado essas leis.[7] No entanto, em cerca de metade destas jurisdições, as leis sobre protecção de dados ainda não entraram em vigor ou não estão totalmente implementadas (Greenleaf & Cottier, International and regional commitments in African data privacy laws: A comparative analysis, 2022).

De um modo geral, a legislação e os regulamentos que foram desenvolvidos em todo o continente incluem elementos comuns, tais como os princípios do tratamento de dados e os direitos das pessoas em causa. No entanto, existem igualmente divergências entre as legislações de vários países. Por exemplo, no que diz respeito ao âmbito de aplicação, alguns países podem aplicar as leis de protecção de dados apenas ao sector privado ou ao sector público. Podem também existir divergências no que respeita à definição de dados pessoais ou ao tratamento dos fluxos transfronteiriços de informação e ao que constituiria equivalência.

De acordo com uma análise continental sobre o panorama da protecção e localização de dados em África realizada pela CUA no âmbito do Projecto da Iniciativa de Política e Regulamentação para a África Digital (PRIDA), para avaliar os países quanto ao nível de alinhamento e convergência das suas políticas, regulamentos e legislações nacionais em relação a 10 indicadores/princípios de harmonização, nomeadamente:

1. Direito à privacidade e quadro jurídico,
2. Direitos Individuais de Protecção de Dados,
3. Fluxos Transfronteiriços de Dados Pessoais,
4. Disposições favoráveis à Economia Digital,
5. Aplicação adequada da legislação relativa à protecção de dados,
6. Salvaguardas de Segurança Adequadas,
7. Limitações Específicas à Privacidade da Informação,
8. Cooperação com a sociedade civil,
9. Compromissos Multilaterais e Bilaterais,
10. Formação e Desenvolvimento de Competências.

A análise comparativa segue-se à identificação dos princípios/indicadores através da análise de conteúdo dos dados relativos aos quadros regionais e continentais e à criação de um índice de harmonização utilizando os princípios de harmonização. A análise comparativa

7 Entre estes contam-se Cabo Verde (2001, alterado em 2013), Seychelles (2003), Burkina Faso (2004, revisto em 2021), Maurícias (2004, revisto em 2017), Tunísia (2004, em revisão), Senegal (2008, em revisão), Benim (2009, revisto em 2017), Marrocos (2009, em revisão), Angola (2011), Gabão (2011), Lesoto (2011), Gana (2012), Costa do Marfim (2013), Mali (2013), África do Sul (2013), Madagáscar (2014), Chade (2015), Malawi (2016), Guiné Equatorial (2016), São Tomé e Príncipe (2016), Guiné (Conacri) (2016), Mauritânia (2017), Níger (2017), Argélia (2018), Botswana (2018), Nigéria (2019), Uganda (2019), Quénia (2019), República do Congo (2019), Togo (2019), Egipto (2020), Ruanda (2021) e Zimbabwe (2002).

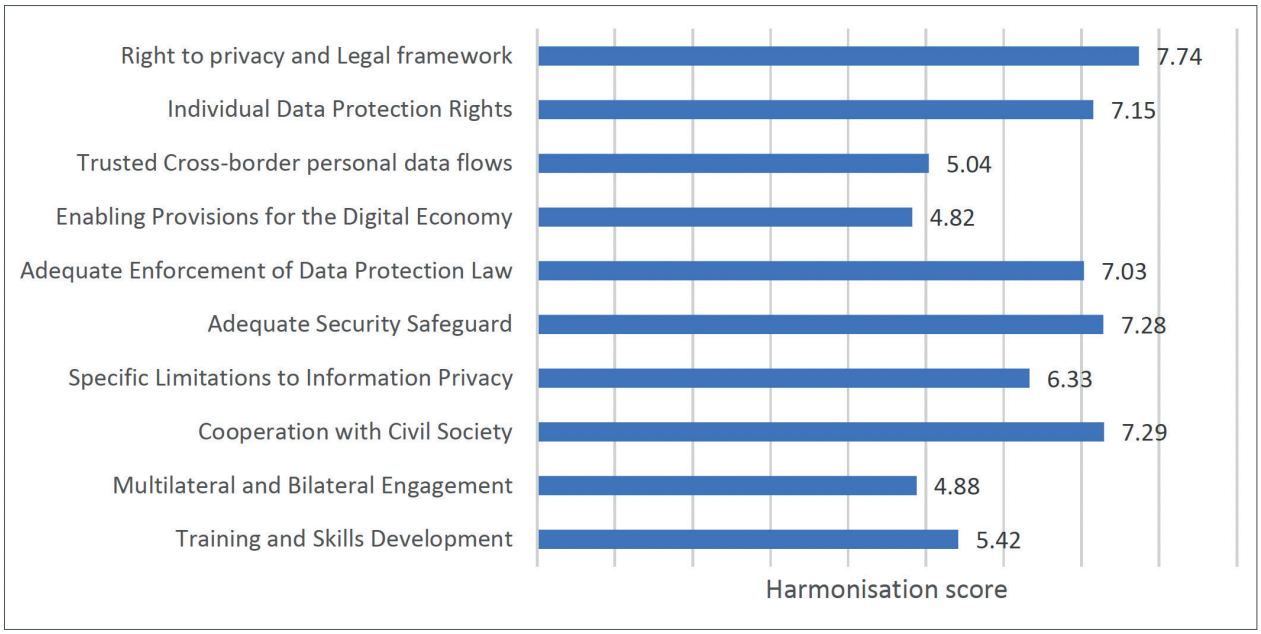
compara os princípios/indicadores identificados com as práticas jurídicas do país. Esta fase investiga se os indicadores/princípios são implementados no país específico. Assim, ao efectuar a análise, apenas os documentos oficiais legais e regulamentares são visitados/utilizados para efeitos de comparação. A análise inclui sete etapas, a saber: (i) Pesquisa e pré-qualificação do documento jurídico, (ii) Identificação das secções relevantes, (iii) Pesquisa de palavras-chave (palavras-chave pré-determinadas a partir dos princípios identificados), (iv) Destaque das disposições com palavras-chave relevantes, (v) Comparação da disposição do documento jurídico com o princípio/indicador, (vi) Análise e registo do grau de harmonização com o princípio/indicador como base da pontuação, (vii) Repetição para o princípio/indicador seguinte.

A pontuação é utilizada como uma técnica para estabelecer valores numa determinada variável, dependendo do facto de o país em questão ter ou não harmonizado um determinado aspecto de um princípio, sendo que o indicador tem uma escala entre zero (0) e dez (10), em que 0 indica um vazio legal/regulamentar, 5 indica um cumprimento parcial e 10 significa um cumprimento total.

Embora tenha sido realizada uma avaliação e análise a nível nacional, em que os relatórios individuais dos países, que reflectem o grau de harmonização de cada país, demonstram diferentes níveis na adopção e implementação de leis e regulamentos sobre protecção e localização de dados, foi fornecida uma visão geral do estado da política, legislação e regulamentos de protecção de dados nos 33 países participantes em África. Como mostra a Figura 7 abaixo, a nível agregado, foi feito muito trabalho no que respeita ao direito à privacidade e aos quadros jurídicos, aos direitos individuais de protecção de dados, às salvaguardas de segurança adequadas e à cooperação com a sociedade civil, uma vez que muitos países criaram plataformas para a partilha de informações e para sensibilizar as pessoas para a privacidade e a protecção de dados. No entanto, mesmo com estes bons desempenhos, existem algumas lacunas que afectam os processos de harmonização a nível continental. Por outro lado, os indicadores com desempenhos mais fracos, que exigem muito mais intervenções tanto a nível nacional como continental, incluem:

a. Fluxos de dados transfronteiriços fiáveis;
b. Disposições favoráveis à economia digital;
c. Limitações específicas à informação Privacidade;
d. Compromissos Multilaterais e Bilaterais; e
e. Formação e Desenvolvimento de Competências.

Figura 7. Nível de harmonização das políticas e regulamentações nacionais africanas sobre proteção e localização de dados



Fonte: CUA (2023)

De um modo geral, a harmonização das leis continua a ser um desafio, apesar dos progressos significativos no desenvolvimento de políticas, leis e regulamentos em todo o continente nos últimos anos. Isto deve-se à falta de um quadro comum que forneça uma base para a implementação, juntamente com a falta de profissionais de dados com competências adequadas para garantir uma governação eficaz dos dados e a criação de valor. Embora a Convenção de Malabo seja um bom ponto de partida, a sua adopção tem sido lenta, o que afecta o seu arranque e a sua aplicação. Dos países que têm leis de protecção de dados, muito poucos as aplicaram na íntegra. A fim de facilitar a harmonização que permite os fluxos de dados dentro e entre países em apoio ao comércio digital de África e à economia baseada em dados, as leis e as autoridades dos Estados-Membros devem ser reforçadas, e as formações e os programas de desenvolvimento de competências a nível continental são fundamentais para permitir que os países façam a autogestão dos seus dados e facilitem transferências de dados transfronteiriças seguras e fiáveis.

Em suma, embora a elaboração de leis de protecção de dados em muitas jurisdições seja um grande avanço, é evidente que estas estão a ser desenvolvidas unilateralmente. Sem uma abordagem harmonizada e coordenada, o continente herdará provavelmente políticas e estratégias que são fragmentadas e diversas. Estas terão impactos prejudiciais na implementação efectiva do ZCLCA. À medida que o Protocolo do ZCLCA sobre o Comércio Digital é redigido, é essencial ter em conta as especificidades da legislação nas diferentes jurisdições e garantir que os Estados-membros estão dispostos a fazer a transição para um conjunto comum de normas e práticas, a fim de assegurar a consistência e a coerência. Além disso, tal como evidenciado na secção anterior, foram realizados numerosos desenvolvimentos a nível continental e regional. Estes constituiriam passos importantes para orientar a elaboração das disposições relativas aos dados no Protocolo.

Leitura complementar

- African Union. (2020). The Digital Transformation Strategy for Africa (2020-2030).
- African Union. (2022). AU Data Policy Framework.
- WTO. (n.d.). Joint Initiative on E-commerce. From World Trade Organisation: *https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm*
- OECD. (2013). Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. From *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188*
- UNCTAD (2021). Digital Economy Report 2021: Cross-border data flows and development: For whom the data flow. United Nations Conference on Trade and Development.
- UNDG (2017). United Nations Sustainable Development Goals Guidance Note on Big Data for Achievement of the 2030 Agenda: Data Privacy, Ethics and Protection. United Nations Development Group.
- WEF (2020). Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows. World Economic Forum.
- Burri, M. (2021). Big Data and Global Trade Law. Cambridge: Cambridge University Press.
- Gao, H. (2022, January 18). Data sovereignty and trade agreements: Three digital kingdoms. Hinrich Foundation.

3. GUIA DE REFERÊNCIA PARA INTEGRAR AS DISPOSIÇÕES RELATIVAS AOS DADOS NO PROTOCOLO DO ZCLCA SOBRE O COMÉRCIO DIGITAL

3.1 OBJECTIVOS E ÂMBITO

Estas Directrizes para a Integração das Disposições Relativas aos Dados no Protocolo sobre Comércio Digital estão em conformidade com o quadro de Política de Dados da UA, aprovado pela União Africana em Fevereiro de 2022, estabelece a visão para orientar os Estados-membros da União Africana no desenvolvimento dos seus sistemas de dados nacionais (African Union, 2022). Este quadro pode servir de base para os princípios gerais que orientam a governação e a utilização dos dados. Especificamente no que respeita ao papel dos dados no comércio digital e na economia digital, o objectivo e a finalidade podem ser múltiplos: promover a inovação e o crescimento económico; proporcionar um ambiente seguro e protegido para reforçar a confiança; preservar o espaço político para os Estados protegerem interesses públicos legítimos, como a segurança nacional e os direitos humanos; ou equilibrar os benefícios e as responsabilidades das partes envolvidas na economia digital.

Importa sublinhar que as disposições dos ACR, incluindo as disposições relativas aos dados, são vinculativas para os Estados-Membros dos acordos e, por conseguinte, apenas fornecem os compromissos mínimos das Partes. Isto corresponde ao princípio do "direito de regulamentar", segundo o qual as disposições dos ACR servem apenas como regras mínimas gerais, enquanto os Estados têm o poder de conceber a especificidade dos seus respectivos regulamentos internos para a aplicação dessas regras.

Embora os preâmbulos não sejam geralmente considerados como tendo qualquer significado jurídico imediato (Schenker, 2015) ma vez que não especificam as obrigações das Partes como a maioria das cláusulas substantivas, as declarações fornecidas na secção do preâmbulo serão utilizadas para a interpretação das disposições de acordo com o artigo 31.º da Convenção de Viena sobre o Direito dos Tratados de 1969[8]. O preâmbulo de um tratado define, em termos gerais, os objectivos, considerações ou motivações que levaram as partes a concluir um tratado (Mbengue, 2006). Por outras palavras, os preâmbulos estão frequentemente associados ao objecto e à finalidade de um tratado. Sendo parte integrante de um tratado, o texto preambular tem sido cada vez mais associado a um peso jurídico e interpretativo substancial, particularmente nos contextos recentes da OMC e do litígio sobre investimento internacional (Hulme, 2016). Este facto constitui um forte motivo para os negociadores considerarem cuidadosamente as implicações que os preâmbulos podem ter na elaboração dos textos de abertura dos tratados.

8 O artigo 31 (Regra geral de interpretação) da Convenção de Viena de 1969 estipula que: 1. Um tratado deve ser interpretado de boa-fé, de acordo com o sentido comum que deve ser dado aos termos do tratado no seu contexto e à luz do seu objecto e finalidade. 2. Para efeitos da interpretação de um tratado, o contexto compreende, para além do texto, incluindo o preâmbulo e os anexos: a) Qualquer acordo relativo ao tratado que tenha sido celebrado entre todas as partes no âmbito da conclusão do tratado; b) Qualquer instrumento que tenha sido celebrado por uma ou mais partes no âmbito da conclusão do tratado e aceite pelas outras partes como um instrumento relativo ao tratado.[...]

Figura 8. Algumas considerações fundamentais sobre as disposições relativas aos dados nos ACL

Com base na redacção da visão do Quadro de Política de Dados da UA, o texto seguinte seria um exemplo para as declarações preambulares relacionadas com os dados do Protocolo do ZCLCA sobre Comércio Digital para apoiar a utilização responsável, segura e equitativa dos dados:

[As Partes no presente Acordo, decidindo:][9]

- Reconhecer o potencial transformador dos dados para capacitar os países africanos, melhorar a vida das pessoas, salvaguardar os interesses colectivos, proteger os direitos digitais e impulsionar um desenvolvimento socioeconómico equitativo;
- Reconhecer a necessidade de sistemas de dados **fiáveis, seguros e protegidos**, integrados com base em normas e práticas comuns;
- Reconhecer a necessidade de um ambiente propício que estimule a **inovação** e o empreendedorismo para promover o desenvolvimento de economias baseadas no valor dos dados;
- Reconhecer a necessidade de **dados abertos,** normas de interoperabilidade e iniciativas de partilha de dados para aproveitar o potencial dos dados a fim de impulsionar o desenvolvimento e garantir uma melhor distribuição dos benefícios da economia baseada em dados;
- Reconhecer a necessidade de garantir a soberania dos Estados-Membros e a sua capacidade de estabelecer prioridades legislativas e regulamentares para **regular** o panorama dos dados em constante mutação e aumentar a utilização produtiva e inovadora dos dados para fornecer soluções e criar oportunidades, atenuando simultaneamente os riscos na economia digital;
- Reconhecer a necessidade de uma **abordagem equilibrada** para facilitar o livre fluxo de dados através das fronteiras, assegurando ao mesmo tempo uma distribuição equitativa dos benefícios e abordando os riscos relacionados com o bem-estar público, os direitos humanos, a segurança nacional e outros objectivos legítimos de política pública;

9 Esta lista de exemplos de texto preambular não é exaustiva e não abrange as declarações de objectivos mais gerais do capítulo sobre comércio digital.

- Reafirmar a importância de promover a responsabilidade social das empresas, a identidade e a diversidade culturais, a protecção e a conservação do ambiente, a igualdade de género, os direitos dos povos indígenas, os direitos laborais, o comércio inclusivo, o desenvolvimento sustentável e os conhecimentos tradicionais, bem como a importância de preservar o direito de regulamentação dos Estados em questões de interesse público;
- Reconhecer a necessidade de facilitar os fluxos transfronteiriços de dados e aumentar as oportunidades de negócio, assegurando simultaneamente um nível adequado de protecção dos **dados pessoais e da privacidade;**
- Reconhecer a necessidade de os Estados-membros **cooperarem** em questões de governação de dados para alcançar objectivos comuns relacionados com o desenvolvimento sustentável das suas economias e sociedades.

Estas declarações apresentam a visão e os objectivos do Protocolo sobre o Comércio Digital. Normalmente, não são especificamente vinculativas nem prevêem quaisquer compromissos em termos de restrição ou facilitação dos fluxos de dados. O preâmbulo é uma declaração de intenções sobre a forma como as partes pretendem regular e facilitar aspectos do mercado de dados e destaca o alinhamento das partes em relação a alguns princípios fundamentais.

3.2 CONSIDERAÇÕES RELATIVAS ÀS DISPOSIÇÕES FUNDAMENTAIS

A presente secção tece considerações sobre as disposições fundamentais, incluindo, se for o caso, a necessidade de dispor de tais disposições no contexto africano; as implicações para a regulamentação, a competitividade e o acesso ao mercado; os eventuais desafios de implementação e as opções para negociações de diferentes tipos (em termos de áreas de questões).

Esta secção centra-se em nove disposições que estão estreitamente ligadas à governação dos dados ou que têm um impacto na utilização responsável, segura e equitativa dos dados (tal como enumerado abaixo). As regras relacionadas com o quadro da política de dados podem também ser encontradas nos protocolos da concorrência e da propriedade intelectual, mas estes estão fora do âmbito deste guia de políticas e, por conseguinte, não estão incluídos.

Como abordagem geral, com base na taxonomia e na análise do texto de diferentes acordos, esta secção sugere uma série de opções para diferentes disposições relativas aos dados. Para facilitar a navegação pelas opções, são indicados diferentes níveis de compromissos através das combinações de verbos e verbos modais entre parênteses rectos ([...]): desde meramente de aspiração (como indicado através da utilização de "as Partes reconhecem", "esforçar-se-ão por", "empenhar-se-ão em", etc.) até compromissos mais fortemente vinculativos (através da utilização de "devem", "adoptarão", "não deixarão de", etc.) (Baker, 2021). São igualmente fornecidas terminologias alternativas entre parênteses rectos ([...]) para indicar opções possíveis. O número da opção é indicado em cada uma das possíveis opções mutuamente exclusivas para facilitar a leitura dos negociadores. Algumas disposições, como as relativas à cooperação ou à inovação no domínio dos dados, são geralmente semelhantes na maior parte dos acordos, uma vez que não impõem obrigações rígidas às Partes. Por conseguinte, para cada um destes tipos de disposições, é apresentada apenas uma opção (com escolhas de palavras potencialmente diferentes).

3.2.1. PROTECÇÃO DOS DADOS PESSOAIS/ PRIVACIDADE DOS DADOS

A inclusão de medidas de protecção de dados pessoais nos acordos comerciais tem sido motivada por preocupações com a privacidade dos indivíduos ou com a segurança nacional (Banga, Macleod, & Mendez-Parra, 2021). Embora persista a resistência à inclusão da protecção de dados por receio de derrogar a privacidade (Greenleaf, 2018), as disposições sobre questões de dados recentemente aprovadas nas negociações comerciais preferenciais podem proporcionar oportunidades para equilibrar os objectivos conflituosos da protecção de dados versus proteccionismo de dados (Burri, 2017), bem como para construir uma abordagem harmonizada da protecção de dados em geral. Isto é ainda mais importante no contexto de África e das negociações do Protocolo do ZCLCA sobre o comércio digital, uma vez que apenas 33 países africanos (ou 61% de todos os Estados-membros da UA) têm legislação em vigor em matéria de protecção de dados e privacidade.

De acordo com a base de dados das TAPED, oitenta e um dos 370 ACR celebrados durante o período 2000-2022 incluem disposições sobre "protecção de dados" com níveis variados de compromissos vinculativos (Burri, Callo-Müller, & Kugler, 2022). Embora as disposições dos ACR sobre protecção de dados não determinem os direitos específicos dos titulares dos dados (como as leis nacionais), exigem frequentemente que os países criem um quadro jurídico ou uma medida para garantir a protecção das informações pessoais (ver pormenores abaixo).

Para além das disposições mais comuns que obrigam as Partes a ter ou a manter um quadro jurídico nacional sobre protecção de dados, muitos ACR também pedem que, no desenvolvimento de normas de protecção de dados pessoais digitais, cada Parte tenha em conta as normas internacionais existentes ou as directrizes de organizações internacionais relevantes - como o Quadro de Privacidade da APEC ou as Directrizes da OCDE sobre Fluxos Transfronteiriços de Dados Pessoais (2013). Alguns acordos especificam mesmo princípios sobre a protecção dos dados pessoais, incluindo os princípios da limitação da finalidade, da qualidade e proporcionalidade dos dados, da transparência, da segurança, do direito de acesso, rectificação e oposição, das restrições às transferências ulteriores e da protecção dos dados sensíveis, bem como disposições sobre os mecanismos de aplicação, a coerência com os compromissos internacionais e a cooperação entre as partes, a fim de assegurar um nível adequado de protecção dos dados pessoais.[10]

Muitos ACR com disposições relativas à protecção de dados reconhecem também as diferentes abordagens jurídicas das Partes em relação à protecção de informações pessoais e, portanto, incentivam as Partes a desenvolver mecanismos para promover a compatibilidade entre esses diferentes regimes. Estes mecanismos podem incluir o reconhecimento de resultados regulamentares, quer sejam concedidos de forma autónoma (como a decisão de adequação da UE), por acordo mútuo (como o Escudo de Protecção da Privacidade entre a UE e os EUA, que foi declarado inválido pelo Tribunal de Justiça Europeu em 16 de Julho de 2020), ou ao abrigo de quadros internacionais mais amplos (como as Directrizes de Privacidade da OCDE ou as Regras de Privacidade Transfronteiriça da APEC).

Como os países podem estar em diferentes fases de desenvolvimento de quadros jurídicos nacionais para a protecção de dados, foram também incorporadas actividades de cooperação nos ACR para melhorar o nível de protecção da privacidade nas comunicações electrónicas, evitando simultaneamente obstáculos ao comércio. Estas disposições podem incluir a partilha

10 Artigo 199-200, APE entre CARIFORUM-CE

de informações e experiências sobre regulamentos, leis e programas de protecção de dados; actividades de investigação e formação; a criação de programas e projectos conjuntos; a manutenção de um diálogo; a realização de consultas sobre questões de protecção de dados, etc. (Burri, 2021). É igualmente importante que as partes no acordo trabalhem no sentido de reconhecer a adequação das regulamentações entre si, algo que é promovido no CPTPP (Baker & Le, 202 (Baker & Le, 202 (Baker & Le, 2022).

Com base nestas considerações, são sugeridas as seguintes opções para as disposições relativas à protecção dos dados pessoais. No contexto africano, a Convenção de Malabo representa um passo importante para a harmonização do quadro regulamentar do continente relativo à segurança cibernética e à protecção de dados pessoais. Por conseguinte, é acrescentado um exemplo de disposição para incentivar os Estados-membros da UA a acelerarem o processo de ratificação.

(I) OBJECTIVOS

Reafirmação das vantagens da protecção de dados pessoais: Os Estados Partes[11] reconhecem os benefícios económicos e sociais da protecção das [*informações/dados*] pessoais dos participantes na [*economia digital/comércio digital/comércio electrónico*] e a importância dessa protecção para o reforço da confiança na [*economia digital/comércio digital/comércio electrónico*][12]

Reconhecer os direitos de privacidade: Os Estados Partes reconhecem que a protecção das [*informações/dados*] pessoais e da privacidade é um direito fundamental e que normas elevadas nesta matéria contribuem para a confiança na economia digital e para o desenvolvimento do comércio.

Sublinhar a proporcionalidade das medidas de protecção de dados: Os Estados Partes reconhecem a importância de garantir o cumprimento das medidas de protecção de dados pessoais e de assegurar que quaisquer restrições aos fluxos transfronteiriços de dados pessoais sejam necessárias e proporcionais aos riscos existentes.[13]

(II) REGULAMENTOS INTERNOS

[Opção 1] Legislação nacional para promover o comércio electrónico e o comércio electrónico digital: Cada Estado Parte [*pode/deve*] adoptar [*e/ou*] manter [*um quadro jurídico/medidas*] que preveja a protecção das [*informações/dados*] pessoais dos utilizadores do comércio electrónico e do comércio digital.[14]

[Opção 2] Legislação nacional para garantir a protecção da privacidade: Os Estados Partes [*podem/devem*] adoptar [*e/ou*] manter [*um quadro jurídico/medidas*] que assegurem a protecção de [*informações/dados*] pessoais, incluindo a transferência e o tratamento transfronteiriço de [*informações/dados*] pessoais e as condições e requisitos a eles relativos, a fim de promover os valores fundamentais do respeito pela vida privada e da protecção de [*informações/dados*] pessoais.[15]

11 A maioria dos ACR utiliza Partes ou Membros para indicar os signatários. A ZCLCA utiliza o termo "Estado Parte" para se referir a um Estado-Membro da União Africana que ratificou ou aderiu ao Acordo e para o qual o Acordo está em vigor. Por conseguinte, o presente guia utiliza igualmente o termo "Estado Parte" (ou "Estados Partes" no plural) por uma questão de coerência.

12 Com base no Artigo 14.8.1, CPTPP; Artigo 4.2.1, DEPA.

13 Parágrafo 3, Secção C.2.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.

14 Com base na primeira frase, Artigo 14.8.2, CPTPP; Artigo 12.8, RCEP; primeira frase, Artigo 4.2, DEPA.

15 Parágrafo 4, Secção C.2.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.

(III) CONSIDERAÇÕES ESPECIAIS PARA OS ESTADOS PARTES[16] NUMA FASE INICIAL DE DESENVOLVIMENTO DOS SISTEMAS DE DADOS NACIONAIS

[Opção 1] Permitir que o Estado Parte desenvolva o quadro nacional ao seu próprio ritmo: [*Nome do Estado Parte*] não é obrigado aplicar o presente artigo antes da data em que esse Estado Parte implementar o seu quadro jurídico que prevê a protecção dos dados pessoais dos utilizadores do comércio electrónico. Para maior certeza, um Estado Parte pode cumprir a obrigação prevista no presente artigo adoptando ou mantendo medidas como leis abrangentes de protecção da privacidade, das informações pessoais ou dos dados pessoais, leis sectoriais específicas que abranjam a privacidade ou leis que prevejam a aplicação de compromissos voluntários das empresas em matéria de privacidade.[17]

[Opção 2] Prever um período de transição específico a pedido do Estado Parte: [*Nome do Estado Parte*] deverá aplicar o presente artigo o mais tardar em [*citar o número de anos de transição*] após a data de entrada em vigor do presente Acordo para essa Parte. Não obstante [*referência à cláusula específica*], o [*nome do Estado Parte*] pode solicitar uma prorrogação de [*citar o número de anos de transição adicionais*] para cumprir integralmente os compromissos previstos em [*referência à cláusula específica*], apresentando um pedido por escrito ao [*indicar o comité específico*], o mais tardar seis meses antes do termo do período de [*citar o número de anos de transição iniciais*] previsto no presente número.

(IV) ADOPÇÃO DE DIRECTRIZES INTERNACIONAIS

[Opção 1] Incentivo genérico: [*No desenvolvimento do seu [quadro jurídico/medidas] para a protecção de [informações/dados]* pessoais, cada Estado Parte terá em conta os princípios e directrizes dos organismos internacionais relevantes.[18]

[Opção 2] Citando as Directrizes Internacionais específicas: No desenvolvimento do seu [*quadro jurídico/medidas*] para a protecção de [*informações/dados*] pessoais, cada Estado Parte [*deve/pode/deverá*] ter em conta as normas internacionais, os princípios, as directrizes e os critérios das organizações ou organismos internacionais pertinentes, como a Recomendação do Conselho da OCDE relativa às directrizes que regem a protecção da privacidade e os fluxos transfronteiriços de dados pessoais (2013).[19]

(V) PRINCÍPIOS FUNDAMENTAIS

Sublinhar o princípio do consentimento dos utilizadores: Os Estados Partes garantirão a obtenção do consentimento individual directamente expresso para a transferência e o tratamento transfronteiriço dos seus dados pessoais. [20]

Enumeração dos princípios fundamentais do quadro jurídico nacional: Os Estados Partes reconhecem que os princípios subjacentes a um quadro jurídico sólido para a protecção de dados pessoais devem incluir a limitação da recolha; a escolha; a qualidade dos dados;

16 Estes exemplos de cláusulas são fornecidos no âmbito da disposição relativa à protecção de dados pessoais, mas os Estados Partes podem também considerar a possibilidade de incluir uma linguagem semelhante noutras disposições, com base nas necessidades e no acordo entre os Estados Partes.
17 Com base na Nota de Rodapé 5 e na Nota de Rodapé 6 do CPTPP.
18 Com base na segunda frase do Artigo 14.8.2 do CPTPP; segunda frase do Artigo 4.2, DEPA.
19 Com base no Parágrafo 5, Secção C.2.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.
20 Parágrafo 8, Secção C.2.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.

a especificação da finalidade; a limitação da utilização; as garantias de segurança; a transparência; a participação individual; e a responsabilidade.[21]

(VI) COMPROMISSO DE RATIFICAÇÃO DA CONVENÇÃO DE MALABO

Os Estados Partes envidarão esforços contínuos e sustentados para ratificar a Convenção da União Africana sobre Segurança Cibernética e Protecção de Dados Pessoais de 2014 (Convenção de Malabo). Os Estados Partes [comprometem-se/devem esforçar-se] por respeitar, promover e realizar, nas suas leis e práticas, os princípios enunciados na Convenção de Malabo.

(VII) NÃO-DISCRIMINAÇÃO

Regra geral de não-discriminação relativa aos dados pessoais dos utilizadores do comércio electrónico: Cada Estado Parte [*deve esforçar-se por*] adoptar práticas não discriminatórias para proteger os utilizadores do comércio electrónico contra violações da protecção de dados pessoais que ocorram na sua jurisdição.[22]

Não-discriminação, com ênfase na informação dos consumidores e dos pacientes médicos: Estado Parte [*deve esforçar-se por*] adoptar práticas não-discriminatórias para proteger os cidadãos, os consumidores e os pacientes médicos contra violações da protecção de dados pessoais que ocorram na sua jurisdição.[23]

(VIII) PUBLICAÇÃO DE INFORMAÇÃO

Cada Estado Parte [*deve/deverá*] publicar informações sobre as protecções de dados pessoais que oferece aos utilizadores do comércio electrónico, incluindo a forma como: (a) os indivíduos podem recorrer a soluções; (b) as empresas podem cumprir quaisquer requisitos legais.[24]

(IX) PROMOÇÃO DA COMPATIBILIDADE DOS REGIMES

Mecanismos de promoção da compatibilidade e/ou do reconhecimento mútuo: Reconhecendo que os Estados Partes podem adoptar abordagens jurídicas diferentes para a protecção de dados pessoais, cada Estado Parte deve [*prosseguir/incentivar*] o desenvolvimento de mecanismos para promover a compatibilidade [*e/ou*] interoperabilidade entre os seus diferentes regimes de protecção de dados pessoais.[25]

Estes mecanismos podem incluir: (a) o reconhecimento de resultados regulamentares, concedidos de forma autónoma ou por acordo mútuo; (b) quadros internacionais mais amplos;[26](c) (c) sempre que possível, o reconhecimento adequado de uma protecção comparável proporcionada pelos quadros nacionais de certificação ou de marcas de confiança dos respectivos quadros jurídicos; ou (d) outras vias de transferência de dados pessoais entre os Estados Partes.[27]

---

21 Com base no Artigo 19.8.3, USMCA; Artigo 4.2.3, DEPA.
22 Com base no Artigo 4.4, DEPA; Artigo 14.8.3, CPTPP; Artigo 19.8.4, USMCA; Parágrafo 7, Secção C.2.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.
23 Parágrafo 7, Secção C.2.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.
24 Com base no Artigo 4.5, DEPA; Artigo 14.8.4, CPTPP; Artigo 19.8.5, USMCA; Artigo 12.8.3, RECP; Parágrafo 9 Secção C.2.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.
25 Com base na primeira frase, Artigo 19.8.6, USMCA.
26 Com base na primeira e segunda frases do Artigo 14.8.5, CPTPP.
27 Com base no Artigo 4.6, DEPA; Parágrafos 10 e 11, Secção C.2.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.

Intercâmbio de informações: Os Estados Partes [*esforçar-se-ão por*] trocar informações sobre os mecanismos aplicados nas suas jurisdições e explorar formas de os alargar ou outras disposições adequadas para promover a compatibilidade entre eles.[28]

3.2.2. FLUXOS DE DADOS TRANSFRONTEIRIÇOS

A importância crescente dos dados na economia deu origem a debates sobre as regras que regem os fluxos transfronteiriços de dados. As restrições à transferência transfronteiras de dados são determinadas pela abordagem de soberania dos dados adoptada por um país. As limitações à transferência transfronteiras de dados podem resultar na perda de oportunidades de negócio e reduzir a capacidade de uma organização para efectuar trocas comerciais a nível internacional. A abordagem geral da transferência de dados exige um nível adequado de protecção no país receptor. Por exemplo, a Convenção de Malabo, ao mesmo tempo que garante o livre fluxo de informação, exige que "O responsável pelo tratamento de dados não transfira dados pessoais para um Estado não membro da União Africana, a menos que esse Estado garanta um nível adequado de protecção da privacidade, das liberdades e dos direitos fundamentais das pessoas cujos dados estão a ser ou são susceptíveis de ser tratados."[29] Neste contexto, é essencial estabelecer o princípio básico para a protecção de dados que fornece uma sincronia ou similar com os regulamentos de outras jurisdições para estabelecer uma base para uma troca de dados confiável, incluindo dados pessoais.

O Quadro de Política de Dados da UA incentiva os Estados-Membros a tirarem partido das economias de escala das infra-estruturas digitais oferecidas pelos serviços de computação em nuvem e outras novas tecnologias para a criação de valor dos dados, tanto para o sector público como para o sector privado (African Union, 2022). Isto implicaria a necessidade de permitir fluxos de dados transfronteiriços livres dentro e fora do continente, sujeitos a condições e normas para garantir a segurança dos dados. Além disso, os fluxos livres de dados intercontinentais serão um elemento essencial para a criação do mercado comum africano e, em especial, para concretizar a visão de um mercado único digital africano, tal como previsto na Estratégia de Transformação Digital para África (2020-2030) (African Union, 2020).

As referências ao fluxo de dados surgiram nos ACR já na década de 2000. No âmbito do ACL entre a Jordânia e os EUA, a Declaração Conjunta sobre Comércio Electrónico salientava a "necessidade de continuar o livre fluxo de informações" (Burri, 2021). Desde então, um número crescente de ACR incorporou disposições mais vinculativas para facilitar os fluxos de dados transfronteiriços. No entanto, os actuais quadros jurídicos relativos aos fluxos de dados transfronteiriços apresentam um elevado nível de diversidade (UNCTAD, 2023). Consequentemente, o âmbito do fluxo transfronteiriço de dados tem sido menos sólido do que o da protecção de dados, o que torna necessário conciliar as abordagens diferenciadas da transferência transfronteiriça de informações, incluindo os dados pessoais.

De um modo geral, os ACR em vigor contêm três tipos de disposições relativas ao fluxo de dados transfronteiras, incluindo os de âmbito mais alargado, como o DEPA ou o DEA entre o Reino Unido e Singapura. Estas incluem disposições que citam o direito de regulamentar, os compromissos de permitir a transferência transfronteiras de informações por meios

28 Com base no Artigo 4.7, DEPA; segunda frase, Artigo 19.8.6, USMCA.
29 Artigo 14.6(a), Convenção de Malabo.

electrónicos e o tratamento não-discriminatório.[30] The specific conditions for cross-border transfer, however, are left to be regulated at the domestic level. No entanto, as condições específicas para a transferência transfronteiras são deixadas para serem regulamentadas a nível nacional. Isto corresponde provavelmente à ênfase no direito de regulamentar das Partes, mas também exige um trabalho de colaboração a nível bilateral e regional, especialmente no contexto de África, para garantir tanto o livre fluxo de dados como a segurança dos dados.

Com base na análise das práticas actuais, apresentam-se a seguir as diferentes opções para estes tipos de disposições relativas ao fluxo de dados transfronteiras do Protocolo do ZCLCA sobre o comércio digital.

(I) OBJECTIVOS

Equilíbrio de direitos: Os Estados Partes reconhecem a importância do livre fluxo de informação na Internet, embora concordem que tal não deve prejudicar os direitos de outras pessoas, entidades ou empresas, incluindo os direitos de propriedade intelectual.

(II) RECONHECIMENTO DOS DIREITOS DE REGULAÇÃO

Direito genérico de regulamentar: Os Estados Partes reconhecem que cada Estado Parte pode ter os seus próprios requisitos regulamentares relativos à transferência de informações por meios electrónicos.[31]

Direito de regulamentar em função de interesses essenciais de segurança: Nenhuma disposição do presente artigo impedirá um Estado Parte de adoptar ou manter qualquer medida que considere necessária para a protecção dos seus interesses essenciais de segurança.[32]

Direito de regulamentar sem discriminação ou inibição do comércio: Nenhuma disposição do presente artigo impedirá um Estado Parte de adoptar ou manter uma medida incompatível com [*exigência de permitir a transferência transfronteiriça de informações por meios electrónicos*] que considere necessária para atingir um objectivo legítimo de política pública, desde que a medida (a) não seja aplicada de forma a constituir um meio de discriminação arbitrária ou injustificável ou uma restrição dissimulada ao comércio;[33] e (b) não imponha restrições às transferências de informações superiores às necessárias para atingir o objectivo.[34]

(III) GOVERNAÇÃO DO FLUXO DE DADOS TRANSFRONTEIRAS

[Opção 1] Melhores esforços: Os Estados Partes esforçar-se-ão por apoiar os fluxos transfronteiriços de dados com confiança através de contratos-modelo de protecção de dados e da utilização de tecnologias emergentes. Ambas as partes explorarão igualmente colaborações sobre a utilização de tecnologias que reforcem a privacidade.[35]

30 A regra da não-discriminação também enfatiza o poder de uma Parte de regulamentar para servir objectivos de política pública e, por isso, neste guia, incluímos este tipo de disposição no mesmo conceito de "direito de regulamentar".
31 Com base no Artigo 4.3.1, DEPA; Artigo 14.11.1, CPTPP; Artigo 12.15.1, RCEP; Parágrafo 4, Secção B.2.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.
32 Com base no Artigo 12.15.3(b), RCEP; Parágrafo 6, Secção B.2.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.
33 Com base no Artigo 12.15.3(a), RCEP.
34 Com base no Artigo 4.3.3, DEPA; Artigo 19.11.2, USMCA; Artigo 14.11.3, CPTPP; Parágrafo 6, Secção B.2.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.
35 Com base no parágrafo 26, Secção 4, Parceria digital entre a UE e a Singapura.

[Opção 2] Livre circulação sem condições: Nenhum Estado Parte poderá [*proibir/restringir/prevenir*] a transferência transfronteiriça de informações [*nulas/incluindo dados pessoais*] por meios electrónicos quando essa actividade se destinar ao exercício da actividade comercial de uma pessoa abrangida.[36]

[Opção 3] Livre circulação sem requisitos de localização: Os Estados Partes estão empenhados em assegurar o fluxo transfronteiriço de dados para facilitar o comércio na economia digital. Para o efeito, os fluxos transfronteiriços de dados não devem ser restringidos por: [37]

a. Exigir a utilização de meios informáticos ou de elementos de rede no território do Estado Parte para o processamento, nomeadamente impondo a utilização de meios informáticos ou de elementos de rede certificados ou aprovados no território do Estado Parte;
b. exigir a localização dos dados no território do Estado Parte para efeitos de armazenamento ou tratamento;
c. proibir a armazenagem ou a transformação no território de outros Estados Partes;
d. condicionar a transferência transfronteiras de dados à utilização de meios informáticos ou de elementos de rede no território do Estado Parte ou a requisitos de localização no território do Estado Parte.

3.2.3. LOCALIZAÇÃO DOS DADOS

À semelhança da transferência transfronteiriça de informações, a localização de dados, muitas vezes designada por requisitos de "localização de instalações informáticas", é frequentemente debatida em ligação com a soberania dos dados. A localização de dados envolve as barreiras legislativas aos fluxos de dados, nomeadamente através de requisitos obrigatórios de armazenamento local de dados (Cory, 2017). A localização de dados é motivada não só pela necessidade de proteger os titulares dos dados, mas também para apoiar as políticas públicas e a regulamentação nacional, especialmente em sectores críticos como a fiscalidade, a contabilidade, as finanças ou as telecomunicações.

De um modo geral, as regras de localização de dados impõem a conservação dos dados ou de uma cópia dos mesmos no território de um país. As regras estritas de localização de dados exigem o armazenamento de todos os dados localmente, e não apenas de uma cópia. As regras de localização de dados destinam-se frequentemente a evitar crimes cibernéticos (como a usurpação de identidade), a promover as economias locais (através da criação de emprego) e a responder às crescentes preocupações com a privacidade (McKinsey, 2022). No entanto, quando as infra-estruturas de dados locais não são suficientemente seguras, podem tornar-se susceptíveis a ameaças à segurança, como ataques cibernéticos e vigilância estrangeira. Além disso, os requisitos de cópias duplicadas de dados podem impor obrigações financeiras indevidas às empresas. Alguns países africanos enfrentam graves limitações de capacidade tecnológica, pelo que os requisitos de localização de dados podem, de facto, sobrecarregar a capacidade interna da actual infra-estrutura digital (como os centros de dados nacionais)

36 Com base no Artigo 19.11.1, USMCA; Artigo 12.15.2, RCEP; Parágrafo 5, Secção B.2.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico. Artigo 4.3.2, DEPA e Artigo 14.11.2, o CPTPP exprime a mesma noção num pacto afirmativo, em vez de negativo: "Cada Parte deve permitir a transferência transfronteiriça de informações por meios electrónicos, incluindo dados pessoais, quando esta actividade se destinar ao exercício da actividade comercial de uma pessoa abrangida."

37 Parágrafo 5, Secção B.2.1, Projecto deTexto de Negociação das Negociações da OMC sobre o Comércio Electrónico; Artigo 201, TCA entre a UE e o REINO UNIDO.

(African Union, 2022). É por isso essencial que os Estados-Membros da UA avaliem a aplicação da localização de dados numa base de custo-benefício, com a incorporação do valor público, para garantir a facilitação da inovação tecnológica sem sobrecarregar a capacidade da infra-estrutura nacional.

A primeira regra de localização de dados foi incluída no ACL entre o Japão e a Mongólia em 2015. Desde então, um número crescente de acordos comerciais incorporou esta regra no seu capítulo sobre comércio electrónico. No entanto, à semelhança das regras relativas à transferência transfronteiriça de dados, o actual âmbito de aplicação das regras de localização de dados no âmbito dos ACR também se tem limitado à protecção de dados, o que torna necessário conciliar as abordagens diferenciadas e a ênfase na soberania dos dados dos países.

Em geral, os ACR existentes, incluindo os de âmbito mais alargado, como o DEPA ou o DEA entre o Reino Unido e a Singapura, contêm três tipos de disposições sobre a localização de dados. Estas incluem disposições que citam o direito de regulamentar, a proibição de utilizar os requisitos de localização de dados como condição para efectuar negócios no território de um país e o tratamento não discriminatório. À semelhança da regra relativa à transferência transfronteiriça de informações, as condições específicas para a localização obrigatória das instalações informáticas devem ser regulamentadas a nível nacional. Os serviços financeiros têm um requisito de transferência de dados distinto, segundo o qual pode-se aplicar certas restrições aos fluxos de dados para proteger a privacidade ou o sigilo dos registos individuais, ou por razões prudenciais. Por conseguinte, as opções para este tipo de disposição também são apresentadas a seguir.

(I) RECONHECIMENTO DOS DIREITOS DE REGULAÇÃO

Direito genérico de regulamentar: Os Estados Partes reconhecem que cada Estado Parte pode ter os seus próprios [*requisitos/medidas regulamentares*] relativos à utilização ou localização de meios informáticos, incluindo [*requisitos/medidas regulamentares*] que procurem garantir a segurança e a confidencialidade das comunicações.[38]

Direito de regulamentar em função de interesses essenciais de segurança: Nenhuma disposição do presente artigo impedirá um Estado Parte de adoptar ou manter qualquer medida que considere necessária para a protecção dos seus interesses essenciais de segurança.[39]

Direito de regulamentar sem discriminar ou inibir o comércio: Nenhuma disposição do presente artigo impedirá um Estado Parte de adoptar ou manter medidas incompatíveis com [*a proibição da localização de dados no território de um Estado Parte*] que considere necessárias para atingir um objectivo legítimo de política pública, desde que a medida: (a) não seja aplicada de forma a constituir um meio de discriminação arbitrária ou injustificável ou uma restrição dissimulada ao comércio;[40] e (b) não imponha restrições à utilização ou localização de recursos informáticos superiores às [necessárias/requeridas] para atingir o objectivo.[41]

38 Com base no Artigo 4.4.1, DEPA; Artigo 12.14.1, RCEP; Artigo 14.13.1, CPTPP; Parágrafo 4, Secção B.2.2, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.
39 Com base no Artigo 12.14.3(b), RCEP; Parágrafo 7, Secção B.2.2, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.
40 Com base no Artigo 12.14.3(a), RCEP
41 Com base no Artigo 4.4.3, DEPA; Artigo 14.13.3, CPTPP; Parágrafo 6, Secção B.2.2, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.

(II) PROIBIÇÃO DA LOCALIZAÇÃO DE DADOS

Nenhum Estado Parte exigirá que uma pessoa abrangida utilize ou localize instalações informáticas no território desse Estado Parte como condição para exercer actividades comerciais no território desse Estado Parte.[42]

(III) LOCALIZAÇÃO DAS INSTALAÇÕES DE COMPUTAÇÃO FINANCEIRA DO PRESTADOR DE SERVIÇOS FINANCEIROS ABRANGIDO

[Opção 1] Reconhecer a necessidade de acesso à informação para efeitos de regulamentação e supervisão financeira: Os Estados Partes reconhecem que o acesso imediato, directo, completo e permanente das autoridades reguladoras financeiras de um Estado Parte às informações dos prestadores de serviços financeiros abrangidos, incluindo as informações subjacentes às transacções e operações dessas pessoas, é fundamental para a regulamentação e supervisão financeiras e reconhecem a necessidade de eliminar quaisquer potenciais limitações a esse acesso.[43]

[[Opção 2] Não é exigida a localização de dados, sob reserva de determinadas condições: Nenhum Estado Parte exigirá que um prestador de serviços financeiros abrangido utilize ou localize instalações informáticas de serviços financeiros no território do Estado Parte como condição para exercer actividades nesse território, desde que as autoridades reguladoras financeiras do Estado Parte, para fins de regulamentação e supervisão, tenham acesso imediato, directo, completo e permanente às informações processadas ou armazenadas em instalações informáticas de serviços financeiros que o prestador de serviços financeiros abrangido utilize ou localize fora do território do Estado Parte.[44]

3.2.4. IDENTIDADES DIGITAIS

A identidade digital não só está intimamente ligada à questão dos dados pessoais, como também pode ter um grande impacto distributivo. Garantir que todos tenham acesso à identificação é uma das metas do Objectivo de Desenvolvimento Sustentável (ODS), Meta 16.9 – "fornecer identidade legal para todos, incluindo o registo de nascimento" até 2030. Além disso, a identificação permitiu o acesso a oportunidades financeiras e económicas, protecção social, cuidados de saúde, educação, etc. (World Bank, 2023). Os sistemas de identidade digital podem apoiar o actual sistema de identidade baseado em papel, que está atrasado. Este aspecto é ainda mais importante no contexto da África Subsariana, que conta com cerca de 500 milhões de pessoas, ou seja, quase metade da população mundial não registada (World Bank, 2023).

A criação de um sistema de identidade digital é uma tarefa difícil, pois exige que se enfrentem os riscos potenciais de privacidade, inclusão e sustentabilidade do sistema de identificação tradicional (World Bank, 2023), bem como o risco de segurança cibernética de um sistema digital (Kanwar, Reddy, Kedia, & Manish, 2022). Por conseguinte, as nuances da concepção e do funcionamento do sistema devem ser da competência do governo (daí o direito de regulamentar

42 Com base no Artigo 4.4.2, DEPA; Artigo 19.12, USMCA; Artigo 14.13.2, CPTPP; Artigo 12.14.2, RCEP; Parágrafo 5, Secção B.2.2, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.
43 Parágrafo 10, Secção B.2.3, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.
44 Parágrafo 10, Secção B.2.3, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.

no contexto do acordo regional). No entanto, para garantir os amplos benefícios do sistema de identidade digital, deve ser realçado o reconhecimento mútuo das identidades digitais, uma vez que tal pode permitir a integração e a cooperação económicas regionais. Isto é ainda mais crucial para a realização dos objectivos da Comunidade Económica Africana com a livre circulação de pessoas, bens, serviços e capitais.[45] O quadro de interoperabilidade da UA para a identificação digital e o quadro de política de dados da UA reconhecem isso e visam alcançar um elevado nível de interoperabilidade e coerência dos sistemas de identificação digital e de dados em todo o continente. Embora vários países africanos tenham introduzido sistemas de identificação digital, os sistemas de identificação digital generalizados e interoperáveis continuam a ser um grande desafio social e económico no continente. Para apoiar o reconhecimento mútuo, o Quadro de Interoperabilidade da Identidade Digital será fundamental para facilitar a criação de conjuntos de dados que possam apoiar o desenvolvimento de serviços públicos e privados em África.

Esta consideração reflecte-se nas regras existentes relativas às identidades digitais no âmbito dos ACR. As disposições relativas à identidade digital afirmam, em geral, o direito do Estado Parte de regulamentar a implementação nacional de sistemas de identidade digital, promovendo simultaneamente mecanismos de apoio à interoperabilidade e ao reconhecimento mútuo entre as Partes. As seguintes opções de disposições são, por conseguinte, fornecidas para as disposições relativas à identidade digital do Protocolo do ZCLCA sobre o comércio digital.

(I) ASPIRAÇÃO DE PROMOVER A INTEROPERABILIDADE DOS REGIMES DE IDENTIDADE DIGITAL

Reconhecendo que a cooperação dos Estados Partes no domínio das identidades digitais, individuais ou colectivas, aumentará a conectividade regional e global, e reconhecendo que cada Estado Parte pode ter diferentes implementações e abordagens jurídicas das identidades digitais, cada Estado Parte esforçar-se-á por promover a interoperabilidade entre os respectivos regimes de identidades digitais.[46]

(II) MEDIDAS PARA PROMOVER A INTEROPERABILIDADE DA IDENTIDADE DIGITAL

Os Estados Partes esforçar-se-ão por facilitar as iniciativas destinadas a promover essa compatibilidade e interoperabilidade [*entre regimes de identidade digital*], que podem incluir:

a. a criação ou manutenção de quadros adequados para promover a interoperabilidade técnica ou normas comuns entre a implementação de identidades digitais de cada Estado Parte;
b. a protecção comparável das identidades digitais proporcionada pelos respectivos quadros jurídicos de cada Estado Parte, ou o reconhecimento dos seus efeitos jurídicos e regulamentares, quer autonomamente quer por acordo mútuo;
c. a criação ou manutenção de quadros continentais e internacionais mais alargados [*sobre regimes de identidade digital*];
d. identificar e implementar casos de utilização para o reconhecimento mútuo de identidades digitais e
e. o intercâmbio de conhecimentos e competências sobre as melhores práticas relacionadas com as políticas e a regulamentação no domínio da identidade digital, a aplicação técnica e as normas de segurança, bem como a promoção da utilização de identidades digitais.[47]

45 Artigo 4.2.1, *Tratado de Abuja*
46 Com base no Artigo 7.1, DEPA; Artigo 8.61-S (1), DEA entre o Reino Unido e a Singapura.
47 Com base no Artigo 7.1, DEPA; Artigo 8.61-S (2), DEA entre o Reino Unido e a Singapura.

(III) EXTINÇÃO PARA OBJECTIVOS DE POLÍTICA PÚBLICA

Para maior certeza, nada no presente artigo impedirá um Estado Parte de adoptar ou manter medidas incompatíveis com [medidas que promovam a interoperabilidade entre regimes de identidades digitais] para atingir um objectivo legítimo de política pública.[48]

3.2.5. DADOS GOVERNAMENTAIS ABERTOS

Os grandes volumes de dados e os dados abertos são os dois principais desenvolvimentos que moldam a trajectória da economia baseada em dados. Os grandes volumes de dados são mais úteis e têm maior valor económico e social quando são também dados abertos (Gurin, 2014). Os dados governamentais abertos, quer se trate de grandes volumes de dados ou não, podem contribuir para a construção de uma sociedade transparente, criando confiança e permitindo uma utilização mais inteligente dos dados, permitindo que indivíduos, organizações e até os próprios governos inovem e colaborem de novas formas (World Bank, 2019; HM Government, 2013). Por exemplo, os dados governamentais podem ser utilizados no desenvolvimento de aplicações para melhorar o acesso e a utilização de serviços locais, como os transportes públicos (Gurin, 2014). McKinsey (2013) estima que os dados abertos podem ajudar a desbloquear até 5 biliões de USD em valor económico anualmente em sete sectores (educação, transportes, produtos de consumo, electricidade, petróleo e gás, cuidados de saúde e financiamento do consumo).

O Quadro de Política de Dados da UA incentiva o estabelecimento de iniciativas de dados governamentais abertos por parte das agências governamentais em apoio à criação de sistemas de dados nacionais integrados e interoperáveis. O Quadro de Política de Dados da UA sublinha que "as normas de dados abertos devem ser prioritárias na criação e manutenção de dados públicos. A criação de dados segundo estas normas não exclui mecanismos sobrepostos de controlo ou limitação do acesso em categorias de dados definidas para fins imperativos." De facto, foram levadas a cabo em África várias inovações bem-sucedidas baseadas em dados abertos para melhorar o desempenho nas áreas da produção agrícola, social e governação, e acesso a medicamentos.

Os dados abertos implicariam mudanças substanciais nos aspectos jurídicos, sociais e técnicos (como a mudança de mentalidade, a abordagem de governação e o quadro jurídico) (Open Data Handbook, 2023). Além disso, não se deve presumir que a prática dos dados abertos se enraizará automaticamente em toda a administração pública. É provável que haja resistência à mudança e, neste caso, a defesa e a sensibilização para os dados abertos por parte de todos os actores institucionais serão benéficas (Schalkwyk, Willmers, & Schonwetter, 2015).

Consequentemente, a nível bilateral, a maioria das disposições relativas aos dados governamentais abertos nos ACR existentes são pouco vinculativas. No entanto, representam um passo "verdadeiramente inovador e muito relevante" no domínio dos regimes nacionais de governação de dados (Burri, 2021). Normalmente, as disposições relativas aos dados governamentais abertos abrangem o reconhecimento dos benefícios conferidos pelo acesso público e pela utilização de dados governamentais, possíveis critérios para os dados governamentais abertos para apoiar o acesso e a utilização, incentivando a cooperação bilateral/regional e os domínios de cooperação. Entre estes, os critérios para os dados governamentais abertos podem apoiar a criação de sistemas de dados nacionais integrados

48 Com base no Artigo 7.2, DEPA.

e interoperáveis para promover uma forte economia de dados, tal como previsto no Quadro de Política de Dados da UA. Com base na consideração das práticas actuais, apresentam-se a seguir algumas opções para estes tipos de disposições relativas aos dados governamentais abertos do Protocolo do ZCLCA sobre o comércio digital.

(I) INCENTIVAR O ACESSO DO PÚBLICO AOS DADOS GOVERNAMENTAIS E A SUA UTILIZAÇÃO

Os Estados Partes reconhecem que facilitar o acesso público e a utilização de dados governamentais promove o desenvolvimento económico e social, a competitividade e a inovação.[49] Para o efeito, os Estados Partes [*são encorajados a/se esforçarão por/deverão*] por alargar a cobertura desses dados, nomeadamente através do envolvimento e consulta das partes interessadas.[50]

(II) CRITÉRIOS PARA DADOS GOVERNAMENTAIS ABERTOS

Na medida em que um Estado Parte opte por disponibilizar digitalmente os dados governamentais para acesso e utilização públicos, o Estado Parte [esforçar-se-á/esforçar-se-á], na medida do possível, por assegurar que esses dados:

a. (seja disponibilizado num formato aberto e legível por máquina;

b. pode ser pesquisado, recuperado, utilizado, reutilizado e redistribuído;

c. seja actualizado, se for caso disso, de forma atempada;

d. seja acompanhada de meta-dados que, na medida do possível, se baseiem em formatos de uso comum que permitam ao utilizador compreender e utilizar os dados;

e. é disponibilizado num formato espacialmente habilitado com interfaces de programação de aplicações fiáveis, fáceis de utilizar e disponíveis gratuitamente (“APIs”)

f. esteja geralmente disponível sem custos ou a um custo razoável para o utilizador.

g. pode ser utilizado para fins comerciais e não comerciais, incluindo no processo de produção de um novo produto ou serviço. [51]

(III) INCENTIVAR A COOPERAÇÃO PARA FACILITAR A UTILIZAÇÃO DE DADOS GOVERNAMENTAIS

Os Estados Partes [*devem esforçar-se por*] cooperar em questões que facilitem e alarguem o acesso do público aos dados governamentais e a sua utilização, incluindo o intercâmbio de informações e experiências sobre práticas e políticas, com vista a incentivar o desenvolvimento do comércio electrónico e a criar oportunidades de negócio, especialmente para as pequenas e médias empresas.[52]

---

49 Com base no Artigo 19.18.1, USMCA; Artigo 9.5.1, DEPA; Artigo 8.61-H (1), DEA entre o Reino Unido e a Singapura.

50 Parágrafo 2, Secção B.4.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.

51 Consolidado a partir de vários textos do artigo 8.61-H (2), DEA entre o Reino Unido e Singapura; parágrafos 3 e 4, secção B.4.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.

52 Com base no artigo 8.61-H (3), DEA entre o Reino Unido e Singapura; artigo 9.5.3, DEPA; artigo 19.18.3, USMCA; parágrafo 5, secção B.4.1, Projecto de Texto de Negociação das Negociações da OMC sobre o Comércio Electrónico.

(IV) DOMÍNIOS DE COOPERAÇÃO

A cooperação ao abrigo do presente artigo pode incluir actividades como:

a. identificar conjuntamente os sectores em que os conjuntos de dados abertos, em especial os que têm valor global, podem ser utilizados para facilitar a transferência de tecnologia, a formação de talentos e a inovação, entre outros aspectos;

b. incentivar o desenvolvimento de novos produtos e serviços baseados em conjuntos de dados abertos; e

c. promover a utilização e o desenvolvimento de modelos de licenciamento de dados abertos sob a forma de licenças públicas normalizadas disponíveis em linha, que permitirão que os dados abertos sejam livremente acedidos, utilizados, modificados e partilhados por qualquer pessoa para qualquer fim permitido pelas respectivas leis e regulamentos dos Estados Partes, e que se baseiam em formatos de dados abertos.[53]

3.2.6. INOVAÇÃO BASEADA EM DADOS

O avanço tecnológico incorporado na sociedade moderna deu origem a mais e melhores conjuntos de dados para utilização e análise, que, por sua vez, apoiam uma melhor tomada de decisões nos sectores público e privado. Além disso, os dados também podem ser utilizados para apoiar mais inovações, como a aprendizagem automática, a automatização e a inteligência artificial (IA) (Borne, 2021). Para além das oportunidades proporcionadas pela aplicação da IA a dados em grande escala, têm surgido preocupações crescentes sobre os seus impactos socioeconómicos. Estas preocupações vão desde possíveis perdas de emprego, expansão do monopólio com acesso exclusivo à tecnologia, direitos humanos fundamentais e impactos na estabilidade política até preocupações éticas relacionadas com erros e enviesamentos dos algoritmos (Mittelstadt, 2021; Bossmann, 2016; Smart Africa Alliance, 2021; Adams, 2022).[54] Provavelmente devido a estas preocupações, bem como ao facto de os países se encontrarem em diferentes fases de desenvolvimento da inovação baseada em dados, as disposições relativas à inovação baseada em dados nos quadros regionais e bilaterais existentes são, na sua maioria, enquadradas como "melhores esforços" e cooperação, sem serem juridicamente vinculativas (como se refere mais adiante). Em África, o Quadro de Política de Dados da UA também destaca a importância política da regulamentação económica necessária para corrigir a distribuição desigual das oportunidades relacionadas com a criação de valor e a inovação dos dados (African Union, 2022).

Embora se espere que o sector privado, por ser o sector mais ágil e activo, conduza grande parte do progresso, os governos têm um papel importante no apoio à inovação baseada em dados para o crescimento económico e a melhoria da qualidade de vida. Em particular, os governos têm um papel importante na recolha e divulgação de dados, criando os quadros jurídicos adequados para promover a partilha de dados e sensibilizando o público para a importância da partilha de dados (Castro & Korte, 2013). O Quadro de Política de Dados da UA recomenda a criação de "um Fórum Anual de Inovação de Dados para África que sirva de plataforma para debates entre várias partes interessadas, facilite os intercâmbios entre países e sensibilize os decisores políticos para o poder dos dados como motor da economia digital

53 Artigo 9.5, DEPA.

54 Este tema está fora do âmbito do presente guia e não será aqui explorado, uma vez que foi tratado noutras iniciativas pan-africanas, como a Estratégia Continental da União Africana para a Inteligência Artificial (AU-AI) para África, que está a ser desenvolvida (AUDA-NEPAD, 2023), ou o modelo de Inteligência Artificial para África, desenvolvido conjuntamente pela Aliança Inteligente de África e pelo governo sul-africano (Smart Africa Alliance, 2021).

actual". Isto apela a acções de cooperação entre todas as partes interessadas, tanto governos como empresas, para fazer avançar a economia inovadora baseada em dados.

A mesma noção reflecte-se na estrutura das disposições relativas à inovação baseada em dados nos ACR. De um modo geral, as disposições relativas à inovação baseada em dados reconhecem o papel dos dados e da inovação baseada em dados na economia e apelam a actividades de cooperação para apoiar a inovação de dados. Note-se que, nesta fase, tal como noutras áreas relacionadas com os dados, dadas as diferentes abordagens à governação dos dados, os compromissos em matéria de inovação de dados são sobretudo de melhor esforço. Com base na análise das práticas actuais, apresentam-se a seguir algumas opções para as disposições relativas à inovação de dados do Protocolo do ZCLCA sobre o comércio digital.

(I) RECONHECER O PAPEL DOS DADOS NA ECONOMIA:

[Opção 1] Os Estados Partes reconhecem que a digitalização e a utilização de dados promovem o crescimento económico.[55]

[Option 2] Os Estados Partes reconhecem que os fluxos de dados transfronteiras e a partilha de dados permitem a inovação baseada em dados.

(II) RECONHECER A NECESSIDADE DE UM AMBIENTE PROPÍCIO E DE MECANISMOS PARA A INOVAÇÃO DOS DADOS

[Option 1] Para apoiar a transferência transfronteiriça de informações por meios electrónicos e promover a inovação baseada em dados, os Estados Partes reconhecem a necessidade de criar um ambiente que permita, apoie e conduza à experimentação e à inovação, nomeadamente através da utilização de ambientes de teste regulamentares, quando aplicável.[56]

[Option 2] Os Estados Partes reconhecem que a inovação pode ser reforçada no contexto de "caixas de areia" regulamentares onde os dados, incluindo informações pessoais, são partilhados entre empresas em conformidade com as respectivas leis e regulamentos dos Estados Partes.[57]

[Option 3] Os Estados Partes reconhecem que os mecanismos de partilha de dados, como os quadros de partilha de dados de confiança e os acordos de licenciamento aberto, facilitam a partilha de dados e promovem a sua utilização no ambiente digital para (a) promover a inovação e a criatividade; (b) facilitar a difusão da informação, do conhecimento, da tecnologia, da cultura e das artes; e (c) fomentar a concorrência e mercados abertos e eficientes.[58]

(III) COLABORAÇÃO NA INOVAÇÃO DE DADOS

Os Estados Partes esforçar-se-ão por apoiar a inovação dos dados através de:[59]

55 Artigo 8.61-I(1), DEA entre o Reino Unido e a Singapura.
56 Artigo 8.61-I (2), DEA entre o Reino Unido e a Singapura.
57 Com base no Artigo 9.4.1, DEPA.
58 Com base no Artigo 9.4.2, DEPA.
59 Artigo 8.61-I (3), UK-Singapore DEA.

a. colaborar em projectos de partilha de dados, incluindo projectos que envolvam investigadores, académicos e a indústria, utilizando os ambientes de teste regulamentares necessários para demonstrar os benefícios da transferência transfronteiriça de informações por meios electrónicos;[60]
b. cooperar no desenvolvimento de políticas e normas para a mobilidade dos dados, incluindo a portabilidade dos dados dos consumidores; e
c. partilhar abordagens políticas e práticas da indústria relacionadas com a partilha de dados, como os fundos fiduciários de dados.[61]

3.2.7. INCLUSÃO DIGITAL

A inclusão digital é definida como "o acesso equitativo, significativo e seguro à utilização, liderança e concepção de tecnologias digitais, serviços e oportunidades associadas para todos, em todo o lado" (United Nations, 2023). É indiscutivelmente apropriado discutir a inclusão digital no contexto de questões relacionadas com os dados, uma vez que a inclusão digital representa tanto um desafio como um resultado esperado da economia baseada em dados. A ONU salienta os factores de acesso, acessibilidade e participação como factores que contribuem para a inclusão digital (United Nations, 2023). Estes factores estão inter-relacionados, uma vez que o acesso e a acessibilidade dos preços proporcionarão os meios para que as pessoas possam fazer ouvir a sua voz e participar.

No contexto de África, assegurar a inclusão digital é ainda mais crítico para garantir que o continente possa colher os benefícios da economia baseada em dados. A IFC e a Google estimam que a economia da Internet em África tem potencial para atingir 180 mil milhões de USD até 2025 e 712 mil milhões de USD até 2050 (Google & SFI, 2020). De facto, a Estratégia de Transformação Digital para África (2020-2030) e o Quadro de Política de Dados da UA salientam a inclusão equitativa como uma condição importante para a economia dos dados. No entanto, para concretizar esse potencial, o continente precisa de ultrapassar vários desafios relacionados com as infra-estruturas, os recursos humanos e o quadro regulamentar.

As disposições em matéria de inclusão digital nos ACR visam dar resposta a alguns dos desafios no acesso e na participação na economia digital e baseada em dados através de uma abordagem essencialmente cooperativa. Isto inclui, entre outros, a partilha de experiências e de boas práticas, a eliminação dos obstáculos ao acesso e o desenvolvimento de competências digitais. Além disso, para um melhor acompanhamento e orientação das políticas de inclusão digital, o papel da recolha de dados em formas desagregadas é também sublinhado para fornecer uma base probatória na formulação de políticas de apoio à inclusão digital.

Com base na análise das práticas actuais, apresentam-se a seguir algumas opções para as disposições relativas à inovação de dados do Protocolo do ZCLCA sobre o comércio digital.

60 Uma disposição semelhante consta do artigo 9.4.3, DEPA.
61 Pode definir-se um fundo de dados como um mecanismo de administração que gere os dados de alguém em seu nome. Ver (Artyushina, 2021).

(I) RECONHECER A IMPORTÂNCIA DA INCLUSÃO DIGITAL

Os Estados Partes reconhecem a importância da inclusão digital para garantir que todas as pessoas e empresas tenham o que precisam para participar, contribuir e beneficiar da economia digital.[62]

Os Estados Partes reconhecem a importância de expandir e facilitar as oportunidades na economia digital, eliminando os obstáculos à participação na economia digital, e que tal pode exigir abordagens adaptadas, desenvolvidas em consulta com pessoas colectivas, indivíduos e outros grupos que enfrentam desproporcionadamente esses obstáculos, nomeadamente entre os povos indígenas, as mulheres, as populações rurais e os grupos socioeconómicos desfavorecidos. [63]

(II) ÁREAS DE COOPERAÇÃO PARA APOIAR A INCLUSÃO

Para o efeito, os Estados Partes cooperarão em questões relacionadas com a inclusão digital, incluindo a participação das mulheres, das populações rurais, dos grupos socioeconómicos desfavorecidos e dos povos indígenas na economia digital. A cooperação pode incluir:

a. partilha de experiências e melhores práticas, incluindo o intercâmbio de peritos, no que respeita à inclusão digital;

b. promover um crescimento económico inclusivo e sustentável para ajudar a garantir que os benefícios da economia digital sejam mais amplamente partilhados;

c. identificar e eliminar os obstáculos ao acesso às oportunidades da economia digital;

d. desenvolver programas para promover a participação de todos os grupos na economia digital;

e. melhorar as competências digitais e o acesso a ferramentas empresariais em linha;

f. promover a protecção laboral dos trabalhadores envolvidos ou que apoiam o comércio digital;

g. partilhar métodos e procedimentos para a recolha de dados desagregados, a utilização de indicadores e a análise de estatísticas relacionadas com a participação na economia digital;

h. partilhar as melhores práticas, colaborar em iniciativas de reforço de capacidades, empenhar-se activamente em fóruns internacionais e promover a participação e a contribuição dos países para o desenvolvimento global de regras sobre o comércio digital; e

i. outros domínios acordados conjuntamente pelos Estados Partes.[64]

(III) MECANISMO DE COOPERAÇÃO

As actividades de cooperação relacionadas com a inclusão digital podem ser realizadas através da coordenação, conforme adequado, das respectivas agências, empresas, sindicatos, sociedade civil, instituições académicas e organizações não governamentais dos Estados Partes, entre outros.[65]

62 Com base no Artigo 11.1.1, DEPA.
63 Consolidado com base no Artigo 11.1.2, DEPA; Artigo 8.61-P (1), DEA entre o Reino Unido e a Singapura.
64 Com base no Artigo 11.1.3, DEPA; Artigo 8.61-P (2) & (4), DEA entre o Reino Unido e a Singapura.
65 Com base no Artigo 11.1.4, DEPA; Artigo 8.61-P (3), DEA entre o Reino Unido e a Singapura.

3.2.8. COOPERAÇÃO

Embora as acções de cooperação tenham sido abrangidas por algumas das disposições acima referidas, existe a opção de ter uma disposição separada que abranja todas as áreas que apoiam os objectivos mais amplos de desenvolvimento do comércio digital, incluindo as questões relativas aos dados. Tal como referido, a governação dos dados continua a ser um domínio político sensível, especialmente no que respeita aos dados pessoais, pelo que exige uma abordagem sensata para conciliar os benefícios das várias partes interessadas. Além disso, a segurança dos dados e a criação de confiança são elementos importantes para persuadir as empresas e os indivíduos a participarem na economia digital. Enquanto as soluções tecnológicas dão resposta à segurança dos dados, a criação de confiança exige uma abordagem gradual baseada na cooperação e na sensibilização.

As disposições sobre cooperação são geralmente apresentadas sob a forma de compromissos de "melhor esforço" em todos os ACR, tal como indicado na utilização da expressão "As Partes esforçar-se-ão por [...]". Isto indica as fracas características vinculativas deste tipo de disposições e a dependência das Partes para realizarem as actividades previstas nas disposições. As variáveis entre os diferentes ACR neste tipo de disposição são os domínios de cooperação identificados no acordo e o mecanismo de cooperação. Segue-se a consolidação das áreas de cooperação encontradas no acordo comercial mais abrangente com capítulo/provisões sobre comércio digital para consideração no âmbito do Protocolo sobre Comércio Digital do ZCLCA. Os Estados Partes podem acrescentar ou retirar os domínios que considerem adequados às suas aspirações.

(I) ÁREAS DE COOPERAÇÃO

Os Estados Partes esforçar-se-ão por:

a. trocar informações e partilhar experiências sobre a regulamentação, as políticas, a aplicação e o cumprimento da legislação relativa à protecção das informações pessoais, com vista a reforçar os mecanismos internacionais de cooperação existentes para a aplicação da legislação de protecção da privacidade;

b. cooperar e manter um diálogo sobre a promoção e o desenvolvimento de mecanismos que promovam a interoperabilidade continental dos regimes de protecção da vida privada;

c. promover, através de iniciativas de cooperação transfronteiriça internacional, o desenvolvimento de mecanismos para ajudar os utilizadores a apresentarem queixas transfronteiriças relativas à protecção de informações pessoais.[66]

d. identificar conjuntamente os sectores em que os conjuntos de dados abertos, em especial os que têm valor global, podem ser utilizados para facilitar a transferência de tecnologia, a formação de talentos e a inovação, entre outros aspectos;

e. incentivar o desenvolvimento de novos produtos e serviços baseados em conjuntos de dados abertos; e

f. promover a utilização e desenvolver modelos de licenciamento de dados abertos sob a forma de licenças públicas normalizadas disponíveis em linha, que permitam que os dados abertos sejam livremente acedidos, utilizados, modificados e partilhados por qualquer pessoa para qualquer fim permitido pelas respectivas leis e regulamentos dos Estados Partes, e que se baseiem em formatos de dados abertos.[67]

66 Com base no Artigo 19.14, USMCA (parcialmente).
67 Com base no Artigo 9.5.4, DEPA.

(II) MECANISMO DE COOPERAÇÃO

Os Estados Partes devem [*considerar a possibilidade de criar/estabelecer*] um [*fórum/grupo de trabalho técnico/subcomité no âmbito do comité do comércio digital/outras opções de mecanismo de cooperação*] para abordar qualquer uma das questões acima enumeradas ou qualquer outra questão relacionada com o funcionamento do presente capítulo.[68]

3.2.9. EXCEPÇÕES GERAIS

Para além da criação de um ambiente propício ao desenvolvimento da inovação e da tecnologia digital, outras tarefas fundamentais dos governos abrangem a promoção e protecção da saúde pública, a segurança dos consumidores, a moral pública, a ordem pública, a segurança nacional, etc. A fim de proteger e promover estes valores e interesses sociais, os governos mantêm normalmente o poder de adoptar legislação ou tomar outras medidas que não sejam compatíveis com os compromissos acima referidos. Estas medidas são frequentemente previstas na cláusula "Excepções gerais" dos acordos comerciais, que são aplicáveis a todo o acordo ou a um capítulo específico.

[**Opção 1] Incorporação da excepção geral do GATT e do GATS:** Para efeitos do presente Acordo, são aplicáveis, na medida do necessário, o artigo XX do GATT de 1994 e a sua nota interpretativa, bem como o artigo XIV do Acordo Geral sobre o Comércio de Serviços constante do Anexo 1B do Acordo da OMC. Para o efeito, as disposições acima referidas são incorporadas no presente Acordo e dele fazem parte integrante, mutatis mutandis. Os Estados Partes acordam ainda que, tendo em conta os desafios colocados pela natureza global da Internet, o presente Acordo não impede os Membros de adoptarem ou manterem quaisquer medidas para garantir a segurança cibernética, salvaguardar a soberania do espaço cibernético, proteger os direitos e interesses legítimos dos seus cidadãos, pessoas colectivas e outras organizações e alcançar outros objectivos legítimos de política pública, desde que essas medidas não sejam aplicadas de forma a constituírem um meio de discriminação arbitrária ou injustificável ou uma restrição dissimulada ao comércio, e não sejam mais do que o necessário para alcançar os objectivos.[69]

[Opção 2] Especificar as excepções: Sem prejuízo da exigência de que tais medidas não sejam aplicadas de forma a constituírem um meio de discriminação arbitrária ou injustificável entre países em que prevaleçam condições similares, ou uma restrição dissimulada ao comércio e à transferência transfronteiriça de informações por via electrónica, nenhuma disposição do presente Acordo será interpretada de modo a impedir a adopção ou a aplicação, por qualquer Estado Parte, de medidas (a) Necessárias para proteger a moral pública ou para manter a ordem pública; b) Necessárias para assegurar a imposição ou a cobrança equitativa ou efectiva de impostos directos no que respeita ao comércio por via electrónica; c) Necessárias para garantir o cumprimento de disposições legislativas ou regulamentares que não sejam incompatíveis com as disposições do presente Acordo, incluindo as relativas a: (i) à prevenção de práticas enganosas e fraudulentas; (ii) à protecção da privacidade dos indivíduos em relação ao processamento e divulgação de dados pessoais e à protecção do sigilo dos registos e contas individuais; e (iii) à segurança.[70]

68 Com base no Artigo 19.14, USMCA.
69 Com base no Artigo 6, Anexo 1: Âmbito e disposições gerais, Projecto deTexto de Negociação das Negociações da OMC sobre o Comércio Electrónico.
70 Com base no Artigo 6, Anexo 1: Âmbito e Disposições Gerais, Projecto deTexto de Negociação das Negociações da OMC sobre o Comércio Electrónico.

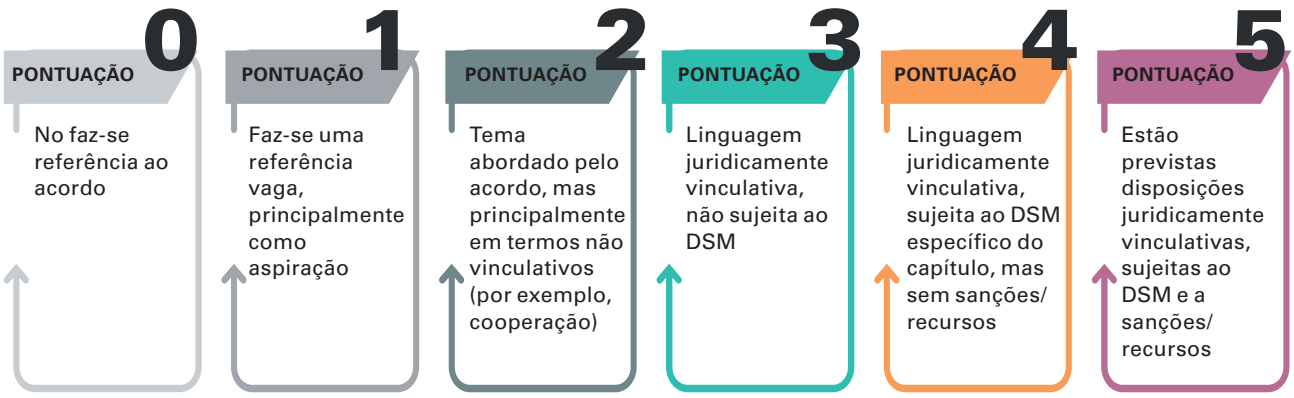
3.2.10. PREVENÇÃO E RESOLUÇÃO DE LITÍGIOS

Os Estados Partes podem optar por aplicar ou não um Mecanismo de Resolução de Litígios às disposições relativas aos dados, bem como a todo o Protocolo sobre o Comércio Digital. A aplicabilidade das disposições relativas aos dados será diferente consoante a forma como as disposições relativas aos dados são estruturadas em combinação com a aplicabilidade do Mecanismo de Resolução de Litígios. A Figura 9 abaixo ilustra os diferentes níveis de aplicabilidade das disposições do ACR por ordem crescente. Por exemplo, uma disposição com uma linguagem de aspiração (por exemplo, os Estados Partes "devem", "esforçar-se-ão por", "esforçar-se-ão por", etc.) será menos vinculativa para os Estados Partes do que uma disposição com uma linguagem mais fortemente vinculativa (por exemplo, os Estados Partes "deverão", "comprometer-se-ão a", "não deixarão de o fazer", etc.). Uma disposição sujeita ao mecanismo de gestão de riscos é mais fortemente aplicável do que uma disposição que não está [sujeita ao Mecanismo de Resolução de Litígios]. Para tal, é necessário ler as disposições no seu contexto e em ligação com outras disposições/capítulos do acordo.

Os actuais ACR têm abordagens diferentes em relação ao Mecanismo de Resolução de Litígios no que respeita às disposições relativas aos dados. A RCEP, por exemplo, exclui actualmente da resolução de litígios todas as questões decorrentes do seu capítulo sobre comércio electrónico. O CPTPP, por outro lado, prevê um período de transição para determinados membros, a fim de lhes dar tempo para "respirar" e ajustar as regulamentações nacionais. O DEPA prevê um quadro completo para a prevenção e resolução de litígios no âmbito do capítulo do comércio digital, incluindo todas as etapas processuais para a realização de mediação e arbitragem. No entanto, o DEPA exclui explicitamente a sua aplicação a algumas das disposições "sensíveis", incluindo a transferência transfronteiriça de informações por meios electrónicos e a localização de instalações informáticas.

Nos casos em que o Mecanismo de Resolução de Litígios é aplicado, as suas disposições permitem muitas vezes a aplicação de um mecanismo de resolução de litígios a vários níveis, através do qual as Partes avançam passo a passo por um processo de resolução de litígios escalonado. O processo começa normalmente com consultas bilaterais, seguidas de outros métodos alternativos de resolução de litígios (ADR), e termina com uma arbitragem/painel com uma decisão vinculativa ou um relatório não vinculativo sobre as conclusões. De seguida, apresentam-se as diferentes opções para a aplicação do Mecanismo de Resolução de Litígios às disposições relativas aos dados, bem como ao Protocolo sobre o Comércio Digital. Se for seleccionada a aplicação do Mecanismo de Resolução de Litígios (Opção 3 do tipo de disposição (i)), os outros tipos de disposições (a partir da disposição (ii)) podem ser remetidos para apreciação. É também prevista uma disposição sobre o objectivo do Mecanismo de Resolução de Litígios para sublinhar que as soluções mutuamente acordadas são o melhor resultado possível que deve orientar a acção de todos os Estados Partes no caso de surgir qualquer questão de desacordo durante a aplicação do Acordo.

Figura 9. Exemplo dos níveis de carácter obrigatório das disposições



Fonte: Com base em (Baker, 2022; Baker, 2021)

(I) APLICABILIDADE DO MECANISMO DE RESOLUÇÃO DE LITÍGIOS:

[Opção 1] Excluídos do Mecanismo de Resolução de Litígios: Nenhum Estado Parte poderá recorrer à resolução de litígios ao abrigo do Capítulo [*indicar o n.º do capítulo*] (Resolução de Litígios) para qualquer questão decorrente do presente capítulo.[71]

[Opção 2] Mecanismo de revisão integrado para a inclusão de disposições relativas aos dados no âmbito do Mecanismo de Resolução de Litígios: No âmbito de qualquer revisão geral do presente Acordo, os Estados Partes analisarão a aplicação do capítulo relativo à resolução de litígios ao presente capítulo <*identificar o número do capítulo*> [*Comércio digital, incluindo a disposição relativa aos dados*]. Após a conclusão da revisão, o capítulo relativo à resolução de litígios é aplicável a este capítulo entre as Partes que concordaram com a sua aplicação.[72]

[Opção 3] Aplicação de um Mecanismo de Resolução de Litígios específico para o capítulo relativo ao comércio digital (incluindo disposições relativas aos dados)/ Mecanismo de Resolução de Litígios geral: Com excepção de <*especificar as disposições a excluir da resolução de litígios, se for o caso*>, é aplicável o Mecanismo de Resolução de Litígios previsto no <*especificar o anexo/capítulo sobre a resolução de litígios*>:

a. relativamente à prevenção ou resolução de litígios entre os Estados Partes quanto à interpretação ou aplicação do presente Acordo; ou

b. quando um Estado Parte considerar que uma medida efectiva ou proposta de outro Estado Parte é ou seria incompatível com uma obrigação do presente Acordo, ou que outro Estado Parte não cumpriu uma obrigação decorrente do presente Acordo.[73]

(II) OBJECTIVOS

Os Estados Partes esforçar-se-ão sempre por chegar a acordo sobre a interpretação e a aplicação do presente Acordo e procurarão, através da cooperação e de consultas, chegar a uma resolução mutuamente satisfatória de qualquer questão que possa afectar o seu funcionamento.

71 Com base (parcialmente) no Artigo 12.17.3, RCEP.
72 Com base (parcialmente) no Artigo 12.17.3, RCEP.
73 Adaptado do Artigo 14.3, DEPA.

O objectivo do presente [*capítulo/disposição relativa à prevenção e resolução de litígios*] é proporcionar um processo eficaz, eficiente e transparente de consultas e resolução de litígios entre os Estados Partes sobre os seus direitos e obrigações ao abrigo do presente Acordo.

(III) PERÍODO DE TRANSIÇÃO PARA CERTOS ESTADOS PARTES

<*Especificar o Estado Parte/Estados Partes*> não estará sujeito à resolução de litígios ao abrigo do Capítulo <*especificar o número do capítulo*> (Resolução de Litígios) relativamente às suas obrigações nos termos do artigo <*especificar o número do artigo*> durante um período de <*especificar o número de anos de transição*> anos após a data de entrada em vigor do presente Acordo para <*especificar o Estado Parte/Estados Partes*>.[74]

(IV) CONSULTA

Em caso de divergências entre os Estados Partes sobre a interpretação e a aplicação do presente capítulo, os Estados Partes em causa iniciarão consultas de boa-fé e envidarão todos os esforços para chegar a uma solução mutuamente satisfatória. Um Estado Parte (Estado Parte requerente) pode, a qualquer momento, solicitar a realização de consultas com outro Estado Parte (Estado Parte respondente) relativamente a qualquer questão decorrente do presente capítulo, apresentando um pedido escrito ao ponto de contacto do Estado Parte respondente. No caso de as consultas não resolverem as divergências, qualquer Estado Parte envolvido nas consultas pode submeter a questão à [*instância institucional do Acordo*].[75]

(V) BONS OFÍCIOS E CONCILIAÇÃO

Os Estados Partes poderão, a qualquer momento, acordar em adoptar voluntariamente quaisquer métodos alternativos de resolução de litígios, tais como os bons ofícios ou a conciliação. Os processos que envolvam os bons ofícios ou a conciliação serão confidenciais e não prejudicarão os direitos das Partes em quaisquer outros processos. Os Estados Partes que participem em processos ao abrigo do presente artigo [*Bons Ofícios e Conciliação*] podem suspender ou terminar esses processos a qualquer momento. Se os Estados Partes em litígio concordarem, os bons ofícios ou a conciliação podem continuar enquanto o litígio prossegue para resolução perante um tribunal arbitral estabelecido ao abrigo do artigo <identificar o número do artigo> (Tribunais Arbitrais).[76]

(VI) ARBITRAGEM/PAINEL

Se os Estados Partes em consulta não tiverem conseguido resolver a questão o mais tardar <*indicando o número de dias*> dias após a data de recepção de um pedido de consulta, o Estado Parte requerente pode solicitar a constituição de um [*tribunal/painel de arbitragem*] nos termos do artigo <*indicando o número do artigo*> (Constituição de [*um tribunal/painel de arbitragem*]) e, conforme previsto no capítulo <*indicando o número do capítulo*> (Resolução de litígios).

74 Com base no Artigo 14.18, CPTPP.
75 Com base (parcialmente) no Artigo 12.17.2, RCEP.
76 Com base no Artigo 14.4, DEPA.

(VII) ESCOLHA DO FORO

Se surgir um litígio relativo a qualquer matéria ao abrigo do presente Acordo e de outro acordo comercial internacional em que os Estados Partes em litígio sejam partes, incluindo o Acordo da OMC, o Estado Parte requerente pode escolher a instância para a resolução do litígio. Se um Estado Parte requerente tiver solicitado a constituição de um painel ou outro tribunal ao abrigo de um acordo [como acima referido], ou a ele tiver submetido uma questão, a instância seleccionada será utilizada com exclusão de outras instâncias.[77]

Leitura complementar

- Draft Negotiating Text of the WTO E-Commerce Negotiations. INF/ECOM/62/Rev.2. 8 September 2021.
- Digital Economy Partnership Agreement (DEPA) between New Zealand, Chile and Singapore.
- Digital Economy Agreement (DEA) between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore.
- Chapter 14 (Electronic Commerce), Comprehensive and Progressive Agreement for Trans-Pacific Partnership.
- Chapter 19 (Digital Trade), Agreement between the United States of America, the United Mexican States, and Canada (USMCA).
- Title III (Digital Trade), Trade and Cooperation Agreement (TCA) between the European Union and the European Atomic Energy Community and the United Kingdom of Great Britain and Northern Ireland.
- Section F (Electronic Commerce), Chapter 8 (Services, Establishment, and Electronic Commerce), European Union-Singapore FTA.
- Chapter 12 (Electronic Commerce), Regional Comprehensive Economic Partnership.
- Burri, M. (Ed.). (2021). Big Data and Global Trade Law. Cambridge: Cambridge University Press. doi:10.1017/9781108919234

3.3 DIRECTRIZES PARA OS NEGOCIADORES SOBRE A CONSIDERAÇÃO DO FORNECIMENTO DE DADOS NOS PROTOCOLOS DO ZCLCA SOBRE COMÉRCIO

3.3.1. QUADRO INSTITUCIONAL GERAL

ABORDAGEM GERAL

Os países têm diferentes modelos de quadros institucionais para determinar a responsabilidade do ministério principal responsável pelas negociações comerciais e de outros ministérios

77 Com base no Artigo 14.7, DEPA.

sectoriais. Por exemplo, enquanto alguns países designam o Ministério dos Negócios Estrangeiros como o principal ministério, aproveitando a sua rede mundial e as suas competências diplomáticas, outros designam o Ministério do Comércio para aproveitar os seus conhecimentos especializados sobre comércio (Baker P. R., Le, Vanzetti, & Ngov, 2022). Relativamente às disposições sobre dados (incluindo a protecção de dados, o fluxo de dados, os dados governamentais abertos, etc.), os Ministérios das Tecnologias da Informação e da Comunicação (TIC) devem liderar os aspectos técnicos. As agências de protecção de dados, quando criadas, devem também ser estreitamente associadas ao processo. Em relação às identidades digitais, deve participar a autoridade nacional de identificação competente. Para a análise do texto jurídico, deve ser consultado o Ministério da Justiça ou o Departamento de Assuntos Jurídicos dos ministérios competentes. Em suma, qualquer quadro institucional para a política comercial deve enquadrar-se na agenda económica nacional global e na autoridade delegada no país.

Em qualquer negociação comercial, a coordenação interna e a consulta entre as agências governamentais relacionadas e o sector privado são fundamentais para o seu êxito. As consultas devem ser efectuadas com regularidade. Devem ser realizadas antes do início da negociação para recolher as informações necessárias, tais como os benefícios potenciais, as preocupações dos sectores privados, os desafios na aplicação, etc. Podem também ser utilizadas para decidir se vale a pena prosseguir com um determinado acordo e para estabelecer limites que ajudarão a formar a Zona de Possível Acordo (ZOPA) e a Melhor Alternativa a um Acordo Negociado (BATNA) para a equipa de negociação. Após a conclusão das negociações, consultas internas adequadas podem ajudar as partes relacionadas a implementar efectivamente essas políticas e a colher os benefícios em todo o seu potencial.

A IMPORTÂNCIA DA COORDENAÇÃO E DAS CONSULTAS INTERMINISTERIAIS

O objectivo das consultas entre organismos públicos é garantir que estes estão bem coordenados no seu respectivo mandato e que servem o objectivo de desenvolvimento "mais vasto" do país. Sem esta consulta interna adequada, os negociadores podem não dispor de informações suficientes para negociar com os seus homólogos estrangeiros e correm o risco de se desviarem dos interesses fundamentais do país. Além disso, pode também afectar a capacidade de obter apoio político a nível interno (UNCTAD, 2018).

A consulta deve ser feita regularmente antes do início das negociações para procurar factos importantes que afectem determinadas áreas do acordo, a fim de alcançar os objectivos globais da negociação. Também pode ser utilizada para responder à proposta do parceiro de negociação e ajustar a sua posição negocial sem perder muitas das vantagens.

A IMPORTÂNCIA DA CONSULTA AO SECTOR PRIVADO

A sociedade civil e os grupos de defesa do consumidor devem participar na definição da posição nacional, enquanto os operadores do sector privado, com um melhor conhecimento do mercado e da tecnologia subjacente aos mercados de dados, devem ser consultados e envolvidos neste processo, uma vez que, em última análise, são os operadores e as entidades reguladoras os principais "utilizadores" das disposições relativas aos dados contidas nos acordos comerciais. O sector privado, incluindo os consumidores individuais - especialmente

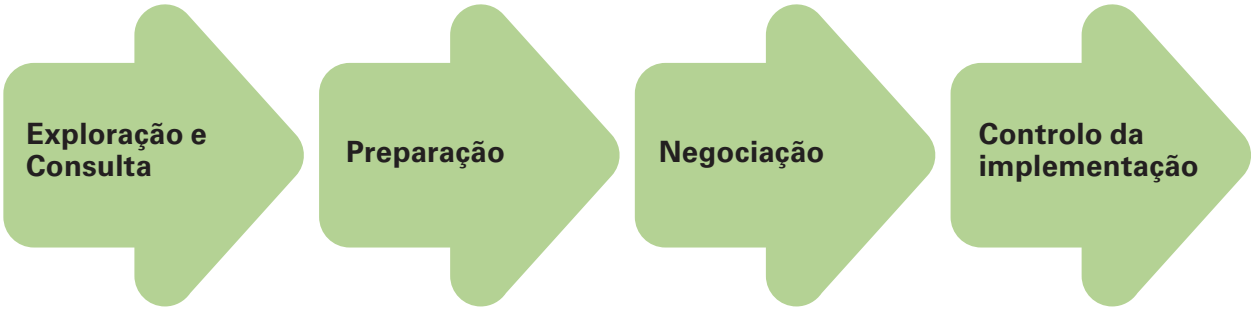
no caso da protecção de dados, são os beneficiários finais dos acordos comerciais. Por conseguinte, devem ser envolvidos, tanto quanto possível, desde o início de qualquer negociação comercial. O sector privado e os representantes das associações de consumidores são as principais fontes de informação no terreno. Podem fornecer aos negociadores informações sobre os benefícios e os desafios da utilização dos acordos comerciais, entre outras questões. A consulta atempada e regular do sector privado pode também permitir-lhe dispor de tempo suficiente para se preparar para o potencial acordo a concluir pelo governo. Por outro lado, não faria sentido se uma questão acordada não pudesse ser efectivamente implementada pelo sector privado no seu país.

3.3.2. QUADRO ANALÍTICO PARA A NEGOCIAÇÃO DAS DISPOSIÇÕES RELATIVAS AOS DADOS

Esta secção apresenta uma abordagem sugerida para o quadro analítico em preparação para a negociação comercial, com sugestões sobre as ferramentas que podem ser utilizadas em cada etapa do processo (Tabela 2). No entanto, importa salientar que estas devem ser vistas como etapas analíticas primárias, enquanto uma análise mais sofisticada (como a realização de uma Avaliação de Impacto Sustentável em grande escala e a consulta das partes interessadas nacionais) deve ser efectuada para garantir uma visão mais abrangente do potencial impacto de um acordo negociado (Baker & Le, 2022) (European Commission, 2016). Os resultados provenientes destas ferramentas devem ser lidos e interpretados em combinação com as observações e a experiência prática, a potencial influência das forças político-económicas e as visões do país na construção da parceria estratégica com as contrapartes em consideração.

Como já foi referido, podem ser envolvidas neste processo diferentes agências governamentais. Seria vantajoso que todas as agências chegassem a acordo numa fase inicial sobre o mecanismo de comunicação e coordenação. Por exemplo, o Ministério do Comércio pode ser responsável pela negociação de todo o capítulo do comércio digital, enquanto a equipa técnica incluirá delegados do Ministério das TIC e da Agência para a Protecção de Dados para assegurar os contributos técnicos.

Tabela 2. Quadro analítico para preparar a negociação das disposições relativas aos dados



Etapa	Trabalho analítico	Objectivo	Ferramenta analítica
1ª Etapa - Exploração e Consulta	Fazer o balanço dos actuais quadros regulamentares relativos aos dados	• Levantamento dos quadros regulamentares nacionais relativos aos dados e/ou eventuais desenvolvimentos/ alterações num futuro próximo (a nível político) • Identificar prioridades e áreas de preocupação das empresas nacionais e dos particulares em relação ao comércio/ transferência de dados transfronteiriços • Perfil regulamentar geral das partes sobre governação de dados: se existem leis/ regulamentos sobre governação de dados, abordagem geral • Os actuais compromissos propostos por outras partes nos domínios negociados nos ACR existentes (se for caso disso)	Detectores de legislação cibernética da CMUCED Análise de textos jurídicos Consultas
2ª Etapa - Preparação	Propostas de Texto Jurídico para as disposições relativas aos dados	Preparar opções para o texto jurídico das disposições relativas aos dados em função da análise efectuada na fase de exploração	Resumo da política de dados Análise de textos jurídicos
3ª Etapa - Negociação	Revisão dos documentos elaborados na 2ª Etapa	Rever para reflectir as alterações e novas informações obtidas durante as negociações.	Análise de textos jurídicos
4ª Etapa - Monitorização da Implementação	Avaliar a conformidade e a monitorização	• Avaliar a conformidade da regulamentação nacional em relação às disposições negociadas • Identificar as áreas que necessitam de alterações na regulamentação nacional • Implementar mudanças • Avaliar os desafios da implementação que devem ser resolvidos	Relatórios das partes interessadas Consultas Quadro de monitorização

4. CONCLUSÕES

O crescimento da economia global é cada vez mais impulsionado por sectores da economia orientados para os dados. Nesta tendência, os dados tornaram-se um activo fundamental que foi transformado em mercadoria e monetizado para criar um novo fluxo de receitas para as grandes empresas (WEF, 2011; Sadowski, 2016). Os dados estão agora no centro de muitas tecnologias de ponta que estão a impulsionar a economia digital. Não servem apenas como um factor de produção de bens e serviços, mas possuem também características únicas que permitem às empresas gerar novos fluxos de receitas e contribuir para a sua competitividade (Hagiu & Wright, 2020). No entanto, é de salientar que existe uma desigualdade no acesso e no crescimento dos mercados de dados, que pode ser resolvida através de negociações comerciais e de uma governação eficaz dos dados (União Africana, 2022)

Embora o valor dos dados seja indiscutível, existem divergências críticas nas abordagens regulamentares. À medida que os dados se tornam um factor de produção cada vez mais importante para o fornecimento de bens e serviços, a utilização de analogias imperfeitas de factores de produção de longa data pode fornecer algumas sugestões sobre a forma de os regular. No entanto, mesmo entre os académicos, tem havido diferentes pontos de vista sobre a forma de tratar os dados, seja como mão de obra, capital, propriedades individuais ou mesmo infra-estruturas (Aaronson, 2021). Estes diferentes pontos de vista, combinados com diferentes incentivos regulamentares, provocaram divergências nas abordagens à governação dos dados. Os três maiores mercados digitais - os EUA, a UE e a China - têm abordagens diferentes em relação à governação dos dados. Os Estados Unidos da América centram-se no controlo dos dados pelo sector privado, a China dá ênfase ao controlo dos dados pelo Governo, enquanto a União Europeia favorece o controlo dos dados pelos indivíduos com base nos direitos e valores fundamentais (UNCTAD, 2021). Seja qual for o ponto de vista, é inegável o papel que o governo desempenha na criação de um quadro regulamentar justo para promover uma utilização responsável, segura e equitativa dos dados. Estas considerações são relevantes no contexto de África, onde as fragilidades dos quadros institucionais, do desenvolvimento humano e da preparação digital impedem os países de tirar partido da enorme quantidade de dados gerados pelas suas instituições, pelo sector privado e pelos cidadãos. A dimensão potencial do mercado e os benefícios decorrentes dos esforços de harmonização foram reconhecidos no Quadro de Política de Dados da UA, onde foram identificadas e estão a ser implementadas intervenções políticas fundamentais para promover o fluxo de dados transfronteiras.

As novas utilizações dos dados exigem novas formas de pensar sobre os dados. As características únicas dos dados sugerem que estes devem ser tratados de forma diferente dos bens e serviços convencionais, incluindo nas suas transferências internacionais. No novo contexto da economia digital baseada em dados, a UNCTAD (2021) sugere que, em vez de tentar determinar quem "detém" os dados, os esforços políticos devem centrar-se no direito de acesso, controlo e utilização dos dados (UNCTAD, 2021). Para além dos dados utilizados no sector privado, a criação de valor a partir de dados públicos é também importante para reforçar os interesses públicos através de uma prestação de serviços mais segura e equitativa.

Para melhor desenvolver as regras que regulam os dados, os decisores políticos devem reconhecer e chegar a acordo sobre as características especiais dos dados. Actualmente, não existe uma definição ou taxonomia única acordada para os dados. Dependendo de critérios escolhidos de forma diferente, os dados podem ser categorizados como dados pessoais ou não pessoais; dados sensíveis ou não sensíveis; dados privados ou públicos; etc. (UNCTAD,

2021). Na sua forma mais pura, ou seja, muitos tipos de dados têm as características de bens públicos (World Bank, 2021), que exigiriam então intervenções do governo para assegurar a eliminação efectiva das externalidades.

Entre estes, os dados pessoais tornaram-se, sem dúvida, um activo importante que requer uma atenção especial (Ciuriak, 2018; WEF, 2011). Uma vez que a utilização de dados pessoais está intimamente associada à privacidade e à segurança dos indivíduos, os cidadãos devem ter a oportunidade de dar o seu contributo para o processo de elaboração das regras, a fim de garantir a transparência, a participação e a responsabilização das mesmas. Tal contribuirá para o elemento "confiança" subjacente ao crescimento da economia digital e centrar-se-á, em primeiro lugar, na criação de um ambiente propício eficaz e, em seguida, no reforço da confiança nessa nova economia, dando às pessoas de todo o mundo a possibilidade de controlarem os seus dados.

As regras de governação dos dados têm duas características desejáveis: permitir o acesso aos dados e gerar confiança. Um ambiente propício à utilização e ao fluxo de dados apoiaria sem dúvida a inovação e criaria mais valor para a sociedade do que a soma de todos os pontos de dados. No entanto, o elemento crítico da confiança seria prejudicado se não existisse um mecanismo para detectar e prevenir a utilização indevida, a usurpação de identidade ou outras violações. Por conseguinte, é importante ter em mente que os dados ajudam a impulsionar a inovação, mas devem existir alguns limites para garantir a privacidade dos cidadãos e os interesses de segurança do Estado. Um equilíbrio na abordagem é o mais desejável, mas também difícil de alcançar. Para tal, seria necessário ter em conta todas as condições e interesses no ambiente nacional. Neste contexto, o Quadro de Política de Dados da UA salienta a importância de criar sistemas de dados legítimos e fiáveis através de uma vasta gama de medidas, incluindo não só a segurança cibernética e a protecção de dados, mas também a promoção da justiça e da ética dos dados.

Embora seja difícil adoptar um único livro de regras para todos, os Estados-Membros da UA devem esforçar-se por chegar a normas e regras comuns baseadas nas recomendações do Quadro de Política de Dados da UA e nas disposições da Convenção de Malabo no que diz respeito à protecção dos dados pessoais. Isto ajudará a criar um ambiente digital menos fragmentado, em que "mais pessoas teriam maior acesso à informação e os indivíduos poderiam criar e partilhar mais informação" (Aaronson, 2016). É aqui que entram em jogo as regras do comércio digital e, especificamente, as disposições relativas aos dados. Conforme abordado anteriormente neste guia, embora as disposições relativas aos dados nos ACR não sejam elaboradas com o nível de pormenor que é fornecido nos regulamentos nacionais relativos aos dados, estabelecem as normas mínimas, enquanto permitem aos Estados Partes a discrição para determinar o método adequado de implementação das disposições do Acordo no âmbito do seu próprio sistema e prática jurídicos. Além disso, devem ser previstas considerações especiais, como períodos de transição e reforço das capacidades, para os Estados Partes menos avançados do ponto de vista digital, a fim de lhes dar espaço político suficiente para desenvolverem regulamentação em matéria de dados em conformidade com os compromissos assumidos, sem deixarem de satisfazer as suas necessidades internas.

Dado que os países se encontram em diferentes fases de desenvolvimento de quadros de governação de dados, serão necessárias acções de colaboração. Os países em desenvolvimento podem beneficiar de uma participação precoce nos debates regionais e plurilaterais sobre os fluxos de dados para garantir que as suas vozes são ouvidas e que os seus interesses são tidos em conta. A participação antecipada e pró-activa dará às economias em desenvolvimento uma maior influência no processo de elaboração de regras, em vez da posição normal de

quem as toma. Esta abordagem poderá ter em conta as diferenças nacionais relativamente à ética da utilização dos dados, à desinformação e a outras questões regulamentares, a fim de garantir que os dados e a economia baseada em dados sejam alcançados em conjunto com um crescimento justo e equitativo.

Este guia de referência sobre como considerar e integrar as disposições relativas aos dados na negociação de protocolos de comércio digital no âmbito do ZCLCA foi preparado com estas características dos dados, as melhores práticas das experiências globais e os princípios fundamentais mencionados anteriormente, em conformidade com o Quadro de Política de Dados da UA e a Estratégia de Transformação Digital de África. As directrizes servem para ajudar as equipas de negociação a considerar as principais disposições relacionadas com os dados contidas nos acordos de comércio livre e a considerar também as implicações económicas e sociais mais amplas da assunção de compromissos em nove áreas fundamentais para fazer avançar o comércio digital intra-africano e a integração regional, em conformidade com os objectivos da Agenda 2023, bem como a linguagem vinculativa dessas disposições. Dado que a natureza da governação dos dados está em evolução e é dinâmica, as informações contidas no guia de referência devem ser consideradas em paralelo com a evolução dos novos desenvolvimentos nos mercados de dados e na regulamentação dos dados.

BIBLIOGRAFIA

Aaronson, S. A. (2016). *The Digital Trade Imbalance and Its Implications for Internet Governance.* The Digital Trade Imbalance and Its Implications for Internet Governance. Retrieved from *https://www.cigionline.org/publications/digital-trade-imbalance-and-its-implications-internet-governance/*

Aaronson, S. A. (2021). Data Is Different, So Policymakers Should Pay Close Attention to Its Governance. In M. Buri, *Big Data and Global Trade Law* (pp. 340-360). Cambridge University Press.

Adams, R. (2022, May 30). *AI in Africa: Key Concerns and Policy Considerations for the Future of the Continent*. Retrieved from Africa Policy Research Institute: *https://afripoli.org/ai-in-africa-key-concerns-and-policy-considerations-for-the-future-of-the-continent*

African Union. (2020). *The Digital Transformation Strategy for Africa (2020-2030).*

African Union. (2022). *AU Data Policy Framework.*

African Union. (2022). *Decision on the Reports of the Sub-Committees of the Permanent Representatives' Committee (PRC). 40th Ordinary Session of the Executive Council (02-03 February 2022).* Retrieved from *https://au.int/sites/default/files/decisions/41584-EX_CL_Dec_1143-1167_XL_E.pdf*

African Union. (2023). *List of Countries Which Have Signed, Ratified/Acceded To The African Union Convention On Cyber Security And Personal Data Protection.*

African Union Commission. (2018). *African Forum on Cybercrime: African Union Convention on Cybersecurity and Personal Data Protection.*

African Union. (forthcoming). *Draft Continental Harmonisation Strategy on Policy and Regulatory Environment for Africa's Digital Single Market.*

APEC. (2005). *APEC Privacy Framework*. APEC Secretariat. Retrieved from *https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf*

APEC. (2019). *What is the Cross-Border Privacy Rules System?* Asia-Pacific Economic Cooperation. Retrieved from *https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System#:~:text=The%20APEC%20Cross%2DBorder%20Privacy,2005%20and%20updated%20in%202015*

Arasasingham, A., & Goodman, M. P. (2023, April 13). Operationalizing Data Free Flow with Trust (DFFT). *CSIS*.

Artyushina, A. (2021, June 10). *The future of data trusts and the global race to dominate AI*. Retrieved from Bennett Institute for Public Policy of Cambridge: *https://www.bennettinstitute.cam.ac.uk/blog/data-trusts1/*

AUDA-NEPAD. (2023, March 29). *Artificial Intelligence is at the core of discussions in Rwanda as the AU High-Level Panel on Emerging Technologies convenes experts to draft the AU-AI Continental Strategy*. Retrieved from African Union Development Agency (AUDA-NEPAD): *https://www.nepad.org/news/artificial-intelligence-core-of-discussions-rwanda-au-high-level-panel-emerging*

Ayalew, Y. E. (2023, June 15). *The African Union's Malabo Convention on Cyber Security and Personal Data Protection entered into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?* Retrieved from European Journal of International Law Blog: *https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/*

Babalola, O. (2022). *Data Protection Legal Regime and Data Governance in Africa: An Overview.* AERC Africa.

Baker McKenzie. (2023, January 28). *Data Protection Day - Key developments and trends for 2023*. Retrieved from Lexology: *https://www.lexology.com/library/detail.aspx?g=e4ead5f0-ccd4-4762-8e06-7dd84c8341ff*

Baker, P. (2022). Trade and Sustainable Development in EU Economic Partnership Agreement. *Cross-Regional Exchange on Trade and Sustainable Development in EU Economic Partnership Agreement.*

Baker, P. R. (2021). *Handbook on Negotiating Sustainable Development Provisions in Preferential Trade Agreements.* Retrieved from UNESCAP: *https://repository.unescap.org/bitstream/handle/20.500.12870/4285/ESCAP-2021-MN-Handbook-negotiating-sustainable-development.pdf?sequence=1&isAllowed=y*

Baker, P. R., Le, L., Vanzetti, D., & Ngov, P. (2022). *Handbook on Trade Analysis.* Sept: GIZ.

Baker, P., & Le, L. (2022). *Digital Trade under CPTPP and its implications for the UK.* Retrieved from UK Parliament: *https://committees.parliament.uk/writtenevidence/110995/pdf/*

Baker, P., & Le, L. (2022). *Guidebook on Trade Impact Assessments.* Retrieved from www.unctad.org: *https://unctad.org/system/files/official-document/ditctncd2021d4_en.pdf*

Banga, K., Macleod, J., & Mendez-Parra, M. (2021). *Digital trade provisions in the AfCFTA: What can we learn from South–South trade agreements?* Retrieved from *https://set.odi.org/wp-content/uploads/2021/04/Digital-trade-provisions-in-the-AfCFTA.pdf*

Berka, W. (2017). CETA, TTIP, TiSA, and Data Protection. In S. Griller, W. Obwexer, & E. Vranes, *Mega-Regional Trade Agreements: CETA, TTIP, and TiSA: New Orientations for EU External Economic Relations.* Oxford. Retrieved from *https://academic.oup.com/book/26602/chapter/195266134*

Borne, K. (2021, July 6). *Top 10 Data Innovation Trends During 2020*. Retrieved from Rocket-Powered Data Science: *http://rocketdatascience.org/?p=1589*

Bossmann, J. (2016, October 21). *Top 9 ethical issues in artificial intelligence*. Retrieved from World Economic Forum: *https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/?*

Bracy, J. (2023, March 8). UK introduces draft data protection reform. *International Association of Privacy Professionals*.

Bryant, J. (2021, May 25). Three years in, GDPR highlights privacy in global landscape. *International Association of Privacy Professionals*.

Bukht, R., & Heeks, R. (2017). *Defining, Conceptualising and Measuring the Digital Economy.* Development Informatics Working Paper no. 68. Retrieved from *https://ssrn.com/abstract=3431732 or http://dx.doi.org/10.2139/ssrn.3431732*

Burri, M. (2017). The Regulation of Data Flows Through Trade Agreements. *Georgetown Journal of International Law, Vol. 48, No. 1, 2017*. Retrieved from *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3028137*

Burri, M. (2021). *Big Data and Global Trade Law.* Cambridge: Cambridge University Press.

Burri, M., Callo-Müller, M. V., & Kugler, K. (2022). *TAPED: Trade Agreement Provisions on Electronic Commerce and Data*. Retrieved from *https://unilu.ch/taped*

Castro, D., & Korte, T. (2013, November 3). *Data Innovation 101*. Retrieved from Center for Data Innovation: *https://datainnovation.org/2013/11/data-innovation-101/*

Chenaoui, H. (2018, September 11). Moroccan data protection law: Moving to align with EU data protection? *International Association of Privacy Professionals*.

CIGI. (2018). *Data Governance in the Digital Age.* Centre for International Governance Innovation. Retrieved from *https://www.cigionline.org/static/documents/documents/Data%20Series%20Special%20Reportweb.pdf*

Ciuriak, D. (2018). *The Economics of Data: Implications for the Data-Driven Economy.* Centre for International Governance Innovation.

CloudSufi. (2021, November 16). *https://www.cloudsufi.com/why-is-data-the-backbone-of-the-digital-economy/*. Retrieved from CloudSufi: *https://www.cloudsufi.com/why-is-data-the-backbone-of-the-digital-economy/*

Cory, N. (2017, May 1). *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?* Retrieved from Information Technology & Innovation Foundation: *https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost/*

Cory, N., & Dascoli, L. (2021, July 19). How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. *Information Technology and Information Foundation*.

Crocetti, P., Peterson, S., & Hefner, K. (n.d.). *What is data protection and why is it important?* Retrieved from *https://www.techtarget.com/searchdatabackup/definition/data-protection*

Daigle, B. (2021). Data Protection Laws in Africa: A Pan-African Survey and Noted Trends. *Journal of International Commerce and Economics*.

data.gov.uk. (n.d.). *data.gov.uk*. Retrieved from *https://www.data.gov.uk/*

de la Cruz, R., & Hau, S. (2022, March). *UK: Requirements for international data transfers under UK and EU data protection regimes.* Retrieved from Data Guidance: *https://www.dataguidance.com/opinion/uk-requirements-international-data-transfers-under*

DLA Piper. (2023). Retrieved from *https://www.dlapiperdataprotection.com/*

DLA Piper. (2023, January 29). *Data Protection Laws around the World - United States*. Retrieved from *https://www.dlapiperdataprotection.com/index.html?t=law&c=US*

Dür, A., Baccini, L., & Elsig, M. (2022). *The Design of International Trade Agreements: Introducing a New Database.* Retrieved from *https://www.designoftradeagreements.org/*

European Commission. (2016, April). *Handbook for Trade Sustainability Impact Assessment.* Retrieved from trade.ec.europa.eu: *https://trade.ec.europa.eu/doclib/docs/2016/april/tradoc_154464.PDF*

European Commission. (2023, March 24). *https://digital-strategy.ec.europa.eu/en/policies/non-personal-data*. Retrieved from European Commission: *https://digital-strategy.ec.europa.eu/en/policies/non-personal-data*

European Commission. (n.d.). *Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection.* Retrieved from European Commission: *https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en*

European Commission. (n.d.). *Shaping Europe's digital future: Free flow of non-personal data*. Retrieved from *https://digital-strategy.ec.europa.eu/en/policies/non-personal-data#:~:text=The%20Regulation%20on%20the%20free,and%20IT%20systems%20in%20Europe*.

European Parliament. (2016, January 25). *Report 25 January 2016 Containing the European Parliament's Recommendations to the Commission on the Negotiations for the Trade in Services Agreement (TiSA)' (2015/2233(INI), [A8-0009/2016])*. Retrieved from *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2016-0009+0+DOC+XML+V0//EN*

Gao, H. (2022, January 18). Data sovereignty and trade agreements: Three digital kingdoms. *Hinrich Foundation*.

Gawen, E., Hirschfeld, A., Kenny, A., Stewart, J., & Middleton, E. (2021). *Open source in government: creating the conditions for success.* London: Public Digital. Retrieved from *https://assets.public.digital/Open_Source_Report.pdf*

GDPR.EU. (n.d.). *hat is GDPR, the EU's new data protection law?* Retrieved from GDPR.EU: *https://gdpr.eu/what-is-gdpr/*

Giddings, A., Islam, E., Kao, K., & Kopp, E. (2021). *Towards a Global Approach to Data in the Digital Age.* IMF. Retrieved from *https://www.elibrary.imf.org/view/journals/006/2021/005/article-A001-en.xml*

Githaiga, J., & Kurji, J. A. (2023, February 6). *Kenya: Data Privacy Comparative Guide*. Retrieved from Mondaq: *https://www.mondaq.com/privacy/1190020/data-privacy-comparative-guide*

González, J. L., Casalini, F., & Porras, J. (2022). *A Preliminary Mapping of Data Localisation Measures.* OECD Publishing.

Google & IFC. (2020). *e-Conomy Africa 2020 - Africa's $180 Billion Internet Economy Future.* Retrieved from *https://www.ifc.org/wps/wcm/connect/publications_ext_content/ifc_external_publication_site/publications_listing_page/google-e-conomy*

GovTech Singapore. (2018, October 03). *ABCD: not as easy as you might think*. Retrieved from GovTech Singapore: *https://www.tech.gov.sg/media/technews/stack-18-abcd-ot-as-easy-as-you-might-think*

Greenberg, B. A. (2016). Rethinking Technology Neutrality. *Minnesota Law Review. 207*. Retrieved from *https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1206&context=mlr*

Greenleaf, G. (2018). Looming Free Trade Agreements Pose Threats to Privacy. 152 Privacy Laws & Business International Report. *152 Privacy Laws & Business International Report*, 23-27. Retrieved from *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3199889*

Greenleaf, G., & Cottier, B. (2022). International and regional commitments in African data privacy laws: A comparative analysis. *Computer Law & Security Review, 44*.

GSMA. (2022). *The State of Mobile Internet Connectivity Report 2022.* Retrieved from *https://www.gsma.com/r/somic/*

GSMA. (2023). *The Mobile Economy 2023.* Retrieved from *https://www.gsma.com/mobileeconomy/wp-content/uploads/2023/03/270223-The-Mobile-Economy-2023.pdf*

Gurin, J. (2014). Big Data and Open Data: How open will the future be? *Journal of Law and Policy for the Information Society Vol 10:3*, 691-704. Retrieved from *https://core.ac.uk/download/pdf/159607722.pdf*

Gurin, J. (2014, April 15). *Big data and open data: what's what and why does it matter?* Retrieved from The Guardian: *https://www.theguardian.com/public-leaders-network/2014/apr/15/big-data-open-data-transform-government*

Hagiu, A., & Wright, J. (2020, February). *When Data Creates Competitive Advantage and When It Doesn't*. Retrieved from Harvard Business Review: *https://hbr.org/2020/01/when-data-creates-competitive-advantage*

Harvard Business Review. (2021). Customer Data: Designing for Transparency and Trust. *Harvard Business Review*.

Hinrich Foundation. (2019, February 21). Data localisation and other barriers to digital trade.

HM Government. (2013). *Open Data White Paper. Unleashing the Potential.* Retrieved from *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/78946/CM8353_acc.pdf*

Huawei & Oxford Economics. (2017). *Digital Spillover. Measuring the true impact of the digital economy.* Retrieved from *https://www.huawei.com/minisite/gci/en/digital-spillover/files/gci_digital_spillover.pdf*

Hulme, M. H. (2016). Preamble in Treaty Interpretation. *University of Pennsylvania Law Review Vol 164*, 1281-1343. Retrieved from *https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9527&context=penn_law_review&httpsredir=1&referer=*

IBM. (n.d.). *What is artificial intelligence?* Retrieved from IBM: *https://www.ibm.com/topics/artificial-intelligence*

IBM. (n.d.). *What is machine learning?* Retrieved from IBM: *https://www.ibm.com/topics/machine-learning*

ICC. (2022). *ICC White Paper on Delivering Universal Meaningful Connectivity.* Retrieved from *https://iccwbo.org/wp-content/uploads/sites/3/2022/05/2022-icc-white-paper-delivering-connectivity.pdf*

IIF. (2020). *Data Localization: Costs, Tradeoffs, and Impacts Across the Economy.* Institute of International Finance. Retrieved from *https://www.iif.com/portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf*

ITU. (2013). *HIPSSA –Data Protection: SADC Model Law.*

ITU. (2021). *Measuring digital development Facts and Figures 2021.* Retrieved from *https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf*

ITU. (2022). *Measuring digital development: Facts and Figures 2022.* International Telecommunication Union. Retrieved from *https://www.itu.int/dms_pub/itu-d/opb/ind/d-ind-ict_mdd-2022-pdf-e.pdf*

Kanwar, S., Reddy, A., Kedia, M., & Manish, M. (2022). *The Emerging Era of Digital Identities: Challenges and Opportunities for the G20.* ADBI Institute. Retrieved from *https://www.adb.org/sites/default/files/publication/822681/adbi-brief-emerging-era-digital-identities-challenges-and-opportunities-g20.pdf*

Kennedy, G., & Lee, K. H. (2021). *Finding Harmony - ASEAN Model Contractual Clauses and Data Management Framework Launched.* Retrieved from *https://www.lexology.com/library/detail.aspx?g=be41251e-f5f0-4062-a02b-5bffbb8f16ad*

Koigi, B. (2020, 08 10). *Africa data centre market to reach $3 billion by 2025.* Retrieved from Africa Tech: *https://africabusinesscommunities.com/tech/tech-news/africa-data-center-market-to-reach-$3-billion-by-2025-report/*

Kudo, F., & Soble, J. (2022, May 20). *Every country has its own digital laws. How can we get data flowing freely between them?* Retrieved from World Economic Forum: *https://www.weforum.org/agenda/2022/05/cross-border-data-regulation-dfft/*

Kuo, M. (2022, September 26). Trafficking Data: China's Pursuit of Digital Sovereignty: Insights from Aynne Kokas. *The Diplomat*.

Mattoo, A., & Schuknecht, L. (1999). *Trade Policies for Electronic Commerce.* World Bank. Retrieved from *https://elibrary.worldbank.org/doi/10.1596/1813-9450-2380*

Mbengue, M. M. (2006, September). *Preamble.* Retrieved from Oxford Public International Law: *https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1456*

McKinsey. (2013, October 1). *Open data: Unlocking innovation and performance with liquid information*. Retrieved from *https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information*

McKinsey. (2022, June 30). *Localisation of data privacy regulations creates competitive opportunities*. Retrieved from McKinsey: *https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities*

McKinsey. (2022, August 17). *What is the Internet of Things?* Retrieved from McKinsey: *https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-internet-of-things*

Meddin, E. (2020). The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and Article XVII of the General Agreement on Trade in Services. *American University International Law Review, 35*(4).

Mitchell, A. D., & Hepburn, J. (2017). Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer. *19 Yale Journal of Law and Technology 182 (2017)*, 182-237. Retrieved from *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2846830*

Mittelstadt, B. (2021). *The impact of Artificial Intelligence on the Doctor-Patent Relationship.* Council of Europe. Retrieved from *https://rm.coe.int/inf-2022-5-report-impact-of-ai-on-doctor-patient-relations-e/1680a68859*

Nordhaug, L. M., & Harris, L. (2021). Digital public goods: Enablers of digital sovereignty. In OECD, *Development Co-operation Report 2021: Shaping a Just Digital Transformation.* Retrieved from *https://www.oecd-ilibrary.org/sites/c023cb2e-en/index.html?itemId=/content/component/c023cb2e-en*

OAG California. (2023, April 24). *California Consumer Privacy Act (CCPA)*. Retrieved from Office of the Attorney General - State of California Department of Justice: *https://oag.ca.gov/privacy/ccpa*

OECD. (2011). *OECD Guide to Measuring the Information Society 2011.*

OECD. (2013). *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved from *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188*

OECD. (2013). *The OECD Privacy Framework.* Retrieved from *https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*

OECD. (2015). *Data-Driven Innovation: Big Data for Growth and Well-Being.* Paris: OECD Publishing.

OECD. (2015). *Data-Driven Innovation: Big Data for Growth and Well-Being.* Paris: OECD Publishing.

OECD. (2020). *OECD Open, Useful and Re-usable Data (OURdata) Index: 2019.*

OECD. (2022). *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188.* Retrieved from *https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188*

OECD. (n.d.). *Data-driven innovation for growth and well-being*. Retrieved from OECD: *https://www.oecd.org/sti/ieconomy/data-driven-innovation.htm*

OECD. (n.d.). *Digital trade*. Retrieved from Organisation for Economic Co-operation and Development: *https://www.oecd.org/trade/topics/digital-trade/*

OECD. (n.d.). *Why data governance matters*. Retrieved from Organisation for Economic Cooperation and Development: *https://search.oecd.org/digital/data-governance/*

OECD. (n.d.). *Personal Data Protection at the OECD*. Retrieved from *https://www.oecd.org/general/data-protection.htm*

OECD, WTO & IMF. (2020). *Handbook on Measuring Digital Trade.* Retrieved from *https://www.oecd.org/sdd/its/Handbook-on-Measuring-Digital-Trade-Version-1.pdf*

Okwara, E. (2022, September 27). A privacy pro's odyssey in Africa. *International Association of Privacy Professionals*.

One Trust Data Guidance. (2022, December 22). *Morocco: CNDP reminds controllers of data breach procedure*. Retrieved from Data Guidance: *https://www.dataguidance.com/news/morocco-cndp-reminds-controllers-data-breach-procedure*

One Trust Data Guidance. (n.d.). *Morocco*. Retrieved from Data Guidance: *https://www.dataguidance.com/jurisdiction/morocco*

OneTrust. (2022, September 16). *ECOWAS Act on Personal Data Protection*. Retrieved from OneTrust DataGuidance: *https://www.dataguidance.com/opinion/african-bodies-ecowas-act-personal-data-protection*

Onuoha, R. (2022, November 29). *Africa's Leading Lights: Regional Network Readiness for Digital Transformation*. Retrieved from Portulans Institute: *https://portulansinstitute.org/africas-leading-lights/*

Open Data Handbook. (2023). *The Open Data Handbook*. Retrieved from *https://opendatahandbook.org/guide/en/*

POPIA. (n.d.). *POPIA*. Retrieved from POPIA: *https://popia.co.za/*

Redman, T. C. (2015, May 20). *4 Business Models for the Data Age*. Retrieved from Harvard Business Review: *https://hbr.org/2015/05/4-business-models-for-the-data-age*

Research and Markets. (2022). *Africa Data Center Market - Industry Outlook & Forecast 2022-2027.*

Rotella, P. (2012, April 2). *Is Data The New Oil?* Retrieved from Forbes: *https://www.forbes.com/sites/perryrotella/*

SADC. (2021). *Selection of Individual Consultant: Consultancy for Revision and Modernisation of the SADC Data Protection Model Law.*

Sadowski, J. (2016, August 31). *Companies Are Making Money from Our Personal Data, but at What Cost?* Retrieved from The Guardian: *https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon*

Satariano, A. (2018, May 6). *What the G.D.P.R., Europe's Tough New Data Law, Means for You*. Retrieved from The New York Times: *https://www.nytimes.com/2018/05/06/technology/gdpr-european-privacy-law.html*

Schalkwyk, F. v., Willmers, M., & Schonwetter, T. (2015). *Embedding Open Data Practice: Developing Indicators on the Institutionalisation of Open Data Practices in two African Government.* World Wide Web Foundation. Retrieved from *http://webfoundation.org/docs/2015/08/ODDC-2-Embedding-Open-Data-Practice-FINAL.pdf*

Schenker, C. (2015). *Practice Guide to International Treaties.* Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera .

Simmons, D. (2022, January 13). *17 Countries with GDPR-like Data Privacy Laws*. Retrieved from Comforte: *https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws*

Smart Africa Alliance. (2021). *Artificial Intelligence for Africa Blueprint.* Smart Africa Alliance. Retrieved from *https://smart.africa/board/login/uploads/70029-eng_ai-for-africa-blueprint.pdf*

Smart Africa Alliance. (2021). *Blueprint for e-Payments for the Facilitation of Digital Trade across Africa.* Retrieved from *https://smartafrica.org/knowledge/blueprint-for-e-payments-for-the-facilitation-of-digital-trade-across-africa/*

Stanford University. (2020). *Artificial Intelligence Definitions*. Retrieved from Stanford University Human-Centered Artificial Intelligence: *https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf*

Thirani, V., & Gupta, A. (2017, September 22). *The value of data*. Retrieved from World Economic Forum: *https://www.weforum.org/agenda/2017/09/the-value-of-data/*

UK Parliament. (2023, March 8). *British Businesses to Save Billions Under New UK Version of GDPR*. Retrieved from *https://www.gov.uk/government/news/british-businesses-to-save-billions-under-new-uk-version-of-gdpr*

UK Parliament. (2023, April 18). *Parliamentary Bills: Data Protection and Digital Information (No. 2) Bill*. Retrieved from *https://bills.parliament.uk/bills/3430*

UN Global Pulse. (n.d.). *UN Global Pulse Principles on Data Protection and Privacy*. Retrieved from UN Global Pulse: *https://www.unglobalpulse.org/policy/ungp-principles-on-data-privacy-and-protection/*

UNCTAD. (2012). *Harmonising Cyberlaws and Regulations: The Experience of the East African Community.* New York and Geneva: United Nations Conference on Trade and Development. Retrieved from *https://au.int/sites/default/files/newsevents/workingdocuments/27223-wd-harmonizing_cyberlaws_regulations_the_experience_of_eac1.pdf*

UNCTAD. (2016). *Data protection regulations and international data flow: Implications for trade and development.*

UNCTAD. (2018). *Trade Policy Frameworks for Developing Countries: A Manual of Best Practice.*

UNCTAD. (2019). *Digital Economy Report 2019. Value creation and capture: Implications for Developing Countries.* New York: United Nations Conference in Trade and Development. Retrieved from *https://unctad.org/system/files/official-document/der2019_en.pdf*

UNCTAD. (2021). *Covid-19 and E-Commerce. A Global view.* New York: United Nations. Retrieved from *https://unctad.org/system/files/official-document/dtlstict2020d13_en_0.pdf*

UNCTAD. (2021, December 14). *Data Protection and Privacy Legislation Worldwide*. Retrieved from *https://unctad.org/page/data-protection-and-privacy-legislation-worldwide*

UNCTAD. (2021). *Digital Economy Report 2021. Cross-border data flows and development: For whom the data flow.* Geneva: United Nations. Retrieved from *https://unctad.org/system/files/official-document/der2021_en.pdf*

UNCTAD. (2021). *Estimates of global e-commerce 2019 and preliminary assessment of COVID-19 impact on online retail 2020. UNCTAD Technical Notes on ICT for Development No. 18.* United Nations. Retrieved from *https://unctad.org/system/files/official-document/tn_unctad_ict4d18_en.pdf*

UNCTAD. (2021). *Global E-Commerce Jumps to $26.7 Trillion, Covid-19 Boosts Online Retail Sales*. Retrieved from UNCTAD: *https://unctad.org/press-material/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-retail-sales*

UNCTAD. (2023). *G20 Members' Regulations of Cross-Border Data Flows.* Geneva: United Nations. Retrieved from *https://unctad.org/system/files/official-document/dtlecdc2023d1_en.pdf*

UNDG. (2017). *United Nations Sustainable Development Goals Guidance Note on Big Data for Achievement of the 2030 Agenda: Data Privacy, Ethics and Protection.* United Nations Development Group.

United Nations. (2018). *Personal Data Protection and Privacy Principles.* Retrieved from *https://archives.un.org/sites/archives.un.org/files/_un-principles-on-personal-data-protection-privacy-hlcm-2018.pdf*

United Nations. (2023). *Digital Inclusion.* Retrieved from *https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/general/Definition_Digital-Inclusion.pdf*

WEF. (2011). *Personal Data: The Emergence of a New Asset Class.* Geneva: World Economic Forum.

WEF. (2020). *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows.* World Economic Forum.

WEF. (2022, May 20). *Every country has its own digital laws. How can we get data flowing freely between them?* Retrieved from World Economic Forum: *https://www.weforum.org/agenda/2022/05/cross-border-data-regulation-dfft/*

WEF. (2023). *Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows.*

World Bank. (2019). *Starting an Open Data Initiative*. Retrieved from Open Data Toolkit: *http://opendatatoolkit.worldbank.org/en/starting.html*

World Bank. (2021, May 13). *http://opendatatoolkit.worldbank.org/en/starting.html*. Retrieved from Open Data Toolkit: *http://opendatatoolkit.worldbank.org/en/starting.html*

World Bank. (2021). *World Development Report 2021: Data for Better Lives.* Retrieved from *https://www.worldbank.org/en/publication/wdr2021*

World Bank. (2023). *Identification for Development (ID4D) Practitioner's Guide*. Retrieved from *https://id4d.worldbank.org/guide/*

World Bank. (n.d.). *Starting an Open Data Initiative*. Retrieved from *http://opendatatoolkit.worldbank.org/en/starting.html*

WTO. (1999). *Council for Trade in Services – Report of the Meeting Held on 14 and 15 December 1998 – Note by the Secretariat, Doc. S/C/M/32.*

WTO. (1999). *Work Programme on Electronic Commerce – Progress Report to the General Council – Adopted by the Council for Trade in Services on 19 July 1999, Doc. S/L/74, 27 July 1999.*

WTO. (2016). *GATS 3 Article XIV (DS reports).*

WTO. (2021). *WTO Joint Statement Initiative on E-commerce: Statement by Ministers of Australia, Japan and Singapore.*

WTO. (2023, March 30). *E-commerce negotiators advance work, discuss development and data issues*. Retrieved from World Trade Organisation: *https://www.wto.org/english/news_e/news23_e/jsec_30mar23_e.htm*

WTO. (n.d.). *Joint Initiative on E-commerce*. Retrieved from World Trade Organisation: *https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm*

WTO Plurilaterals. (n.d.). *Joint Statement Initiative on Electronic Commerce*. Retrieved from WTO Plurilaterals: *https://wtoplurilaterals.info/plural_initiative/e-commerce/*

Yayboke, E., & Ramos, C. G. (2021, July 23). The Real National Security Concerns over Data Localization. *CSIS*.

Zillner, S., & Neururer, S. (2016). Big Data in the Health Sector (Chapter 10). In J. M. Cavanillas, E. Curry, & W. Wahlster, *New Horizons for a Data-Driven Economy. A Roadmap for Usage and Exploitation of Big Data in Europe* (pp. 179-194). Springer Open.

ANEXOS

ANEXO 1. GLOSSÁRIO

Dado que o domínio digital ainda está a evoluir, não foram acordadas definições para muitos dos termos relacionados com o comércio digital e a economia digital. Por conseguinte, as definições que se seguem são apresentadas com o objectivo de facilitar o debate e não de impor uma interpretação fixa dos termos.

A Inteligência Artificial (IA) foi designada pelo professor emérito de Stanford, John McCarthy, em 1955, como "a ciência e a engenharia da criação de máquinas inteligentes" (Stanford University, 2020). A IA é a inteligência demonstrada pelas máquinas, ao contrário da inteligência natural demonstrada pelos seres humanos e pelos animais, que envolve consciência e emoção. Enquanto tecnologia, a IA é um domínio que combina a informática e conjuntos de dados robustos, para permitir a resolução de problemas. Engloba igualmente os subdomínios da aprendizagem automática e da aprendizagem profunda, que são frequentemente mencionados em conjunto com a inteligência artificial (IBM, n.d.).

A governação dos dados refere-se a diversos acordos, incluindo disposições técnicas, políticas, regulamentares ou institucionais, que afectam os dados e o seu ciclo (criação, recolha, armazenamento, utilização, protecção, acesso, partilha e eliminação) em domínios políticos e fronteiras organizacionais e nacionais (OECD, n.d.). Embora o âmbito possa ser interpretado de forma ampla, as questões centrais em torno da governação dos dados resumem-se a quatro temas fundamentais: a quem pertencem os dados e o que implicam esses direitos; quem está autorizado a recolher que dados; as regras para a agregação de dados; e as regras para a transferência de direitos de dados (CIGI, 2018).

A localização de dados é utilizada para referir os requisitos de que os dados sejam armazenados e/ou tratados no território nacional (González, Casalini, & Porras, 2022). Alguns vão mais longe e exigem que todo o tratamento e utilização derivada dos dados permaneçam dentro das fronteiras nacionais (IIF, 2020). No contexto dos acordos comerciais, a localização dos dados tende a ser abrangida pela disposição relativa à "localização dos meios informáticos", que exige "a utilização ou a localização de meios informáticos no território de [uma] Parte como condição para a realização de negócios nesse território".

A propriedade dos dados refere-se tanto à posse como à responsabilidade pela informação (Zillner & Neururer, 2016). Por outras palavras, a propriedade de dados pode ser entendida como uma forma de propriedade ou como uma forma de controlo. No entanto, é difícil enquadrar a "propriedade de dados" no direito de propriedade tradicional, uma vez que, sendo activos incorpóreos, os dados implicam normalmente uma atribuição complexa de diferentes direitos entre as diferentes partes interessadas nos dados, exigindo "a capacidade de aceder, criar, modificar, empacotar, obter benefícios, vender ou remover dados, mas também o direito de atribuir estes privilégios de acesso a outros" (OECD, 2015).

A soberania dos dados refere-se a uma abordagem política que defende que os dados devem estar sujeitos às leis e regulamentos do país em que são gerados. A procura de soberania dos dados é motivada por preocupações sobre o controlo e a propriedade dos dados, particularmente no contexto da computação em nuvem e dos fluxos de dados transfronteiriços (Gao, 2022). Ver também "soberania digital".

A inovação baseada em dados (IDD) refere-se à utilização de dados e análises para melhorar ou promover novos produtos, processos, métodos organizacionais e mercados (OCDE, 2015). Esta inovação está frequentemente associada à geração e utilização de grandes volumes de dados - geralmente designados por "grandes volumes de dados" - para promover novas indústrias, processos e produtos e criar vantagens competitivas significativas (OCDE, n.d.).

A economia digital foi designada durante quase 30 anos, desde a origem tipicamente citada do termo no livro de Don Tapscott de 1996 "*The Digital Economy: Promise and Peril in the Age of Networked Intelligence*". Desde então, surgiram várias definições com diferentes abordagens para definir a economia digital (Bukht & Heeks, 2017). Uma abordagem consiste em referir a economia digital como "a parte da produção económica derivada exclusiva ou principalmente de tecnologias digitais com um modelo de negócio baseado em bens ou serviços digitais" (UNCTAD, 2019; Bukht & Heeks, 2017).

A soberania digital refere-se ao poder e à autoridade de um governo nacional para tomar decisões livres que afectam os cidadãos e as empresas no domínio digital - com uma ampla cobertura que abrange dados, software, normas e protocolos, infra-estruturas e serviços públicos (Gawen, Hirschfeld, Kenny, Stewart, & Middleton, 2021; Nordhaug & Harris, 2021)

O comércio digital abrange todo o comércio que é encomendado e/ou entregue digitalmente (OCDE, OMC & FMI, 2020). A OCDE esclarece ainda que o comércio digital "engloba transacções digitais de comércio de bens e serviços que podem ser entregues digitalmente ou fisicamente e que envolvem consumidores, empresas e governos" (OCDE, n.d.)

O comércio electrónico refere-se à venda ou compra de bens ou serviços, realizada através de redes informáticas por métodos especificamente concebidos para receber ou fazer encomendas". Esta definição de comércio electrónico abrange as encomendas efectuadas em páginas Web, extranet ou EDI, excluindo as encomendas efectuadas por chamadas telefónicas, faxes ou correio electrónico escrito manualmente (OCDE, 2011). O texto de negociação consolidado da JSI sobre comércio electrónico da OMC em Setembro de 2021 propõe que "[Comércio digital/comércio electrónico] significa a produção, distribuição, comercialização, venda ou entrega de bens e serviços por meios electrónicos". Esta definição é mais ampla do que a da OCDE, uma vez que abrange todas as transacções em que pelo menos uma fase do comércio é efectuada por meios electrónicos.

A Internet das Coisas (IoT) descreve objectos físicos incorporados com sensores e actuadores que comunicam com sistemas informáticos através de redes com ou sem fios - permitindo que o mundo físico seja monitorizado digitalmente ou mesmo controlado (McKinsey, 2022).

A localização de equipamentos informáticos refere-se aos requisitos da regulamentação nacional para localizar servidores informáticos e dispositivos de armazenamento para processamento ou armazenamento de informações para utilização comercial no território de um país, como condição para a realização de negócios nesse território (Artigo 4.4, DEPA).

A aprendizagem automática, enquanto área de estudo, refere-se ao campo de estudo da forma como os agentes informáticos podem melhorar a sua percepção, conhecimento, pensamento ou acções com base na experiência ou nos dados. Para tal, a aprendizagem automática baseia-se na ciência da computação, na estatística, na psicologia, na neurociência, na economia e na teoria do controlo (Stanford University, 2020). Em termos de aplicação, a aprendizagem automática é um ramo da inteligência artificial (IA) e da ciência da computação que se centra na utilização de dados e algoritmos para imitar a forma como os seres humanos aprendem, melhorando gradualmente a sua precisão (IBM, n.d.).

Os dados abertos referem-se a dados digitais que são disponibilizados com as características técnicas e jurídicas necessárias para serem livremente utilizados, reutilizados e redistribuídos (Artigo 9.1, DEPA).

Por dados pessoais entende-se qualquer informação relativa a uma pessoa singular identificada ou identificável (OCDE, 2022). Alguns quadros utilizam um termo semelhante, "informações pessoais", que se refere a "informações, incluindo dados, sobre uma pessoa singular identificada ou identificável" (Artigo 1.3, DEPA).

A protecção dos dados pessoais refere-se ao domínio do direito que prevê medidas administrativas ou técnicas destinadas a proteger as pessoas contra a utilização abusiva dos dados que lhes dizem respeito e a conceder-lhes o direito de acesso aos dados com vista a verificar a sua exactidão e adequação (OCDE, 2013). Também podem ser referidas como "leis de protecção de dados" ou "leis de privacidade".

ANEXO 2. EXEMPLOS DE QUADROS INTERNACIONAIS SOBRE DIRECTRIZES DE DADOS

Alguns dos quadros internacionais mais notáveis são discutidos neste anexo como uma análise das boas práticas, enquanto alguns quadros regulamentares nacionais são também brevemente discutidos quanto à forma como as jurisdições correspondem às questões dos dados.

(I) PRINCÍPIOS E DIRECTRIZES DA ONU

A Organização das Nações Unidas (ONU) desenvolveu um conjunto de princípios de privacidade de dados que visam promover a utilização responsável dos dados para o desenvolvimento sustentável salvaguardando simultaneamente a privacidade e protegendo os direitos humanos (UN Global Pulse, n.d.). Estes incluem os Princípios das Nações Unidas sobre Protecção de Dados Pessoais e Privacidade 2018 (os "Princípios") e a Nota de Orientação das Nações Unidas sobre Grandes Dados para a Realização da Agenda 2030: Privacidade, Ética e Protecção de Dados (a "Orientação").

Os princípios, compostos por dez regras, estabelecem um quadro de base para o tratamento de "dados pessoais" pelas organizações do sistema das Nações Unidas, ou em seu nome, no exercício das suas actividades obrigatórias. Estes princípios têm por objectivo (i) harmonizar as normas para a protecção de dados pessoais em todo o Sistema das Nações Unidas; (ii) facilitar o tratamento responsável de dados pessoais; e (iii) assegurar o respeito pelos direitos humanos e liberdades fundamentais dos indivíduos, em particular o direito à privacidade. Estes princípios podem também ser utilizados como referência para o tratamento de dados não pessoais.

Figura 10. Dez Princípios das Nações Unidas sobre Protecção de Dados Pessoais e Privacidade

Fonte: (Nações Unidas, 2018)

As Directrizes centram-se em nove princípios (**Erro! A origem da referência não foi encontrada.**) concebidos para apoiar os membros e parceiros do Grupo de Desenvolvimento das Nações Unidas no estabelecimento de um quadro eficiente e coerente sobre privacidade de dados, protecção de dados e ética de dados para o Grupo de Desenvolvimento das Nações Unidas (UNDG) relativamente à utilização de grandes volumes de dados. Note-se que as Directrizes não são um documento jurídico; em vez disso, fornecem apenas uma base mínima para a auto-regulação que pode ser alargada e elaborada pelas organizações de implementação (UNDG, 2017). Dado o seu âmbito mais vasto, os princípios de orientação para os dados também fornecem directrizes mais elaboradas sobre as normas esperadas de processamento e utilização de dados, bem como sobre a gestão de riscos e o controlo da qualidade dos dados. O ⁋Anexo 4 apresenta um resumo dos princípios.

Figura 11. Nove princípios da Nota de Orientação das Nações Unidas sobre Grandes Dados

(II) AS DIRECTRIZES DE PRIVACIDADE DA OCDE

As Directrizes de Privacidade da Organização para a Cooperação e Desenvolvimento Económico (OCDE) são também um importante quadro internacional para a protecção de dados. As Directrizes de Privacidade da OCDE foram adoptadas pela primeira vez em 1980 para orientar o tratamento responsável de dados pessoais e, desde então, têm sido actualizadas e revistas para se adaptarem à rápida evolução do panorama da privacidade dos dados (OCDE, n.d.). As Directrizes de Privacidade da OCDE baseiam-se em determinados princípios fundamentais centrados na importância da qualidade dos dados, da especificação da finalidade, da responsabilidade e dos direitos individuais (OCDE, 2013). Assim, os princípios exigem, entre outras obrigações, que as organizações obtenham o consentimento dos indivíduos antes de recolherem ou utilizarem os seus dados pessoais e que sejam adoptadas medidas adequadas para proteger os dados pessoais contra o acesso ou utilização não autorizados (OCDE, 2013).

Uma das principais características das directrizes da OCDE relativas à protecção da vida privada é a sua ênfase nos fluxos de dados transfronteiriços. As Directrizes da OCDE sobre Privacidade sublinham a importância da adopção de leis abrangentes de protecção de dados que incluam disposições relativas às transferências transfronteiriças de dados, sendo necessário manter salvaguardas adequadas nessas transferências. Além disso, as Directrizes estipulam que quaisquer limitações impostas ao fluxo transfronteiriço de dados devem ser proporcionais aos riscos (OCDE, 2013). As Directrizes também sublinham a importância da cooperação internacional e da interoperabilidade.

(III) QUADRO DE PRIVACIDADE DA APEC E SISTEMA DE REGRAS TRANSFRONTEIRIÇAS DE PRIVACIDADE DA APEC (CBPR)

Entre as iniciativas bem estabelecidas para promover normas internacionais para a elaboração de regras de governação de dados contam-se o Quadro de Privacidade da APEC, o Sistema de Regras Transfronteiriças de Privacidade da APEC (CBPR) e o Quadro de Gestão de Dados da Associação das Nações do Sudeste Asiático (ASEAN) e as Cláusulas Contratuais Modelo (CCM) para os Fluxos Transfronteiriços de Dados.

- O Quadro de Privacidade da APEC estabelece princípios para a recolha, detenção, processamento, utilização, transferência ou divulgação de informações pessoais aplicados a pessoas ou organizações dos sectores público e privado que controlam cada um dos processos acima referidos. Este quadro promove uma abordagem flexível da protecção da privacidade da informação nas economias membros da APEC, evitando a criação de barreiras desnecessárias aos fluxos de informação (APEC, 2005).
- O Sistema de Regras de Privacidade Transfronteiriça da APEC (CBPR) é uma certificação de privacidade de dados apoiada pelo governo a que as empresas podem aderir para demonstrar a conformidade com protecções de privacidade de dados reconhecidas internacionalmente (APEC, 2019). O sistema CBPR exige que as empresas participantes desenvolvam e implementem políticas de privacidade de dados coerentes com o Quadro de Privacidade da APEC.
- O Quadro de Gestão de Dados da ASEAN foi concebido para fornecer directrizes práticas a todas as empresas do sector privado na implementação de um sistema de gestão de dados baseado em boas práticas de gestão e princípios fundamentais, utilizando uma metodologia baseada no risco.

- As CCM são termos e condições contratuais normalizados recomendados nos acordos relativos à transferência transfronteiriça de dados pessoais entre empresas da região e que se destinam a incluir as principais obrigações relativas à protecção de dados e a reduzir os custos de negociação e de conformidade (Kennedy & Lee, 2021).

Embora todas estas iniciativas estejam longe de ter um alcance e um impacto completos, constituem exemplos de boas práticas na criação de normas regionais e internacionais de governação de dados com vista a uma economia digital aberta.

(IV) INICIATIVA "FLUXO LIVRE DE DADOS COM CONFIANÇA"

Uma iniciativa mais recente, o Fluxo Livre de Dados com Confiança do Fórum Económico Mundial (FEM), visa igualmente facilitar o fluxo livre de dados, garantindo simultaneamente a confiança na privacidade e segurança dos dados. Lançada pelo antigo Primeiro-Ministro japonês, Abe Shinzo, em 2019, a iniciativa Fluxo Livre de Dados com Confiança (DFFT) do FEM assenta na premissa de que o fluxo livre de dados é crucial para o crescimento económico e a inovação e que a protecção e a privacidade dos dados são fundamentais para manter a confiança na economia digital (WEF, 2020). Assim, a iniciativa procura encontrar um equilíbrio entre a promoção do livre fluxo de dados e a protecção de dados pessoais.

Os princípios delineados na iniciativa do Fluxo Livre de Dados com Confiança do FEM visam fornecer um quadro para os decisores políticos e os líderes da indústria desenvolverem quadros regulamentares favoráveis (WEF, 2022). Em 2021, foi adoptado um roteiro para a cooperação, centrado em quatro áreas de cooperação, nomeadamente a localização de dados; a cooperação regulamentar; o acesso do governo aos dados; e a partilha de dados para sectores prioritários (Arasasingham & Goodman, 2023). Em 2022, foi elaborado um plano de acção que alarga a cooperação sobre a futura interoperabilidade regulamentar digital e a partilha de conhecimentos sobre espaços de dados internacionais (Arasasingham & Goodman, 2023). Dado o seu âmbito internacional e o enfoque no sector privado, a iniciativa poderia ajudar a reduzir a fragmentação regulamentar a nível mundial, o que facilitaria o acesso das empresas e a utilização de dados além-fronteiras. No entanto, uma ressalva comum à iniciativa, bem como aos outros quadros discutidos, é que é difícil para os países desenvolverem um quadro regulamentar comum, uma vez que as diferentes jurisdições têm diferentes quadros jurídicos e regulamentares e entendimentos de protecção de dados e privacidade que dificultam o desenvolvimento de um conjunto comum de princípios e directrizes que podem ser aplicados em todo o lado (WEF, 2023).

O RGPD da UE é considerado um regulamento abrangente e sólido sobre protecção de dados. Dada a sua profundidade e o seu vasto âmbito de cobertura, o RGPD serviu de inspiração para muitas legislações em todo o mundo. Entre elas contam-se a Lei Geral de Protecção de Dados Pessoais do Brasil, a legislação de protecção de dados da Califórnia e da Virgínia, bem como a proposta de Lei de Protecção de Dados Pessoais Digitais da Índia (Bryant, 2021). Algumas das disposições distintivas do RGPD da UE que deram à lei a sua reputação incluem:

- Aplicação extraterritorial: Embora o RGPD da UE tenha sido adoptado pela UE, é aplicável a qualquer entidade que processe ou recolha dados relativos aos cidadãos da UE, independentemente de a entidade estar ou não localizada na UE (GDPR.EU, n.d.).
- Consentimento: Ao processar, recolher ou utilizar as informações de cidadãos da UE, o RGPD exige que todas as entidades obtenham o consentimento inequívoco das pessoas em causa. Além disso, os titulares dos dados podem retirar o consentimento previamente dado a qualquer momento.

- Direitos dos titulares dos dados: O RGPD reconhece numerosos direitos de privacidade aos titulares dos dados, que dão aos indivíduos um maior controlo sobre os dados que as organizações podem recolher, armazenar ou processar sobre eles.
- Aplicação e sanções: O incumprimento do RGPD pode resultar em sanções que podem ir até 20 milhões de euros ou 4% das receitas anuais globais, consoante o valor mais elevado.

TO RGPD da UE também impõe restrições ao fluxo transfronteiriço de dados pessoais. De acordo com as disposições do RGPD, os dados pessoais só podem ser transferidos para territórios onde esteja garantido um nível de protecção adequado ao abrigo da legislação nacional. A Comissão Europeia é responsável por determinar a adequação do nível de protecção de dados em países não pertencentes à UE. Apenas alguns países são reconhecidos como tendo leis adequadas (European Commission, n.d.).[78] Quando não existe adequação, as organizações recorrem a outros mecanismos legais para transferir dados pessoais para fora da UE. Estes podem incluir cláusulas contratuais-tipo, regras empresariais vinculativas, códigos de conduta e mecanismos de certificação (Comissão Europeia, n.d.).

A UE adoptou igualmente legislação relativa ao fluxo de dados não pessoais. Um dos objectivos da UE é facilitar a circulação de dados na Europa, permitindo às organizações e aos governos recolher e gerir dados não pessoais em qualquer local à sua escolha dentro do bloco (European Commission, n.d.). O Regulamento relativo a um quadro para o livre fluxo de dados não pessoais tem, assim, como objectivo eliminar quaisquer obstáculos que impeçam o livre fluxo de dados não pessoais entre diferentes países da UE. O regulamento complementa o RGPD e assegura uma abordagem consistente e coerente da livre circulação de todos os dados na UE. Algumas das principais obrigações decorrentes do regulamento incluem a disponibilidade de dados para controlo regulamentar, a portabilidade de dados entre prestadores de serviços em nuvem para utilizadores profissionais e uma maior consistência e coerência com as preocupações de segurança cibernética (European Commission, n.d.).

ANEXO 3. PRINCÍPIOS DE PROTECÇÃO DOS DADOS PESSOAIS E DA PRIVACIDADE DA ONU

1. TRATAMENTO JUSTO E LEGÍTIMO

As Organizações do Sistema das Nações Unidas devem tratar os dados pessoais de forma justa, em conformidade com os seus mandatos e instrumentos orientadores e com base num dos seguintes elementos (i) o consentimento do titular dos dados; (ii) o interesse superior do titular dos dados, em conformidade com os mandatos da Organização do Sistema das Nações Unidas em causa; (iii) os mandatos e instrumentos de governação da Organização do Sistema das Nações Unidas em causa; ou (iv) qualquer outra base jurídica especificamente identificada pela Organização do Sistema das Nações Unidas em causa.

78 Os países que foram reconhecidos como tendo legislação adequada sobre proteção de dados pela Comissão da UE incluem Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, República da Coreia, Suíça, Reino Unido e Uruguai.

2. ESPECIFICAÇÃO DO OBJECTIVO

Os dados pessoais devem ser tratados para fins específicos que sejam coerentes com os mandatos da Organização do Sistema das Nações Unidas em causa e que tenham em conta o equilíbrio dos direitos, liberdades e interesses relevantes. Os dados pessoais não devem ser tratados de forma incompatível com esses objectivos.

3. PROPORCIONALIDADE E NECESSIDADE

O tratamento de dados pessoais deve ser pertinente, limitado e adequado ao que é necessário em relação às finalidades especificadas do tratamento de dados pessoais.

4. RETENÇÃO

Os dados pessoais só devem ser conservados durante o tempo necessário para os fins especificados.

5. PRECISÃO

Os dados pessoais devem ser exactos e, se necessário, actualizados para cumprir as finalidades especificadas.

6. SIGILO

Os dados pessoais devem ser tratados com o devido respeito pelo princípio do sigilo.

7. SEGURANÇA

Devem ser aplicadas garantias e procedimentos organizacionais, administrativos, físicos e técnicos adequados para proteger a segurança dos dados pessoais, nomeadamente contra o acesso não autorizado ou acidental, danos, perdas ou outros riscos decorrentes do tratamento de dados.

8. TRANSPARÊNCIA

O tratamento de dados pessoais deve ser efectuado com transparência para os titulares dos dados, conforme adequado e sempre que possível. Tal deve incluir, por exemplo, a prestação de informações sobre o tratamento dos seus dados pessoais, bem como informações sobre a forma de solicitar o acesso, a verificação, a rectificação e/ou a eliminação desses dados pessoais, na medida em que a finalidade especificada para a qual os dados pessoais são tratados não seja frustrada.

9. TRANSFERÊNCIAS

No exercício das actividades incumbidas, uma Organização do Sistema das Nações Unidas pode transferir dados pessoais para terceiros, desde que, dadas as circunstâncias, a Organização do Sistema das Nações Unidas se certifique de que esses terceiros asseguram uma protecção adequada dos dados pessoais.

10. RESPONSABILIZAÇÃO

As Organizações do Sistema das Nações Unidas devem ter políticas e mecanismos adequados para aderir a estes princípios.

ANEXO 4. NOTA DE ORIENTAÇÃO DA ONU SOBRE MEGA DADOS: PRINCÍPIOS FUNDAMENTAIS

1. UTILIZAÇÃO LEGAL, LEGÍTIMA E JUSTA

Os dados devem ser recolhidos e utilizados de forma legal, legítima e justa, quer directamente, quer através de um contrato com um fornecedor de dados terceiro. O acesso aos dados, a sua análise ou outras utilizações devem respeitar a legislação aplicável, incluindo a legislação relativa à privacidade e à protecção de dados, bem como os mais elevados padrões de sigilo e de conduta moral e ética. É também sublinhado o consentimento adequado da pessoa cujos dados estão a ser utilizados. Os interesses legítimos das pessoas cujos dados estão a ser utilizados devem ser tidos em conta quando se acede, analisa ou utiliza dados para garantir que a utilização dos dados é justa. Os dados não devem ser utilizados de uma forma que viole os direitos humanos ou que seja susceptível de causar efeitos injustificados ou adversos. Assim, para garantir que a utilização dos dados é legítima e justa, devem ser sempre avaliados os riscos, os danos e os benefícios.

2. ESPECIFICAÇÃO DA FINALIDADE, LIMITAÇÃO DA UTILIZAÇÃO E COMPATIBILIDADE DA FINALIDADE

A utilização dos dados deve estar em conformidade com a finalidade para a qual foram obtidos. A finalidade não pode ser alterada a menos que exista uma base legítima. Além disso, a finalidade deve ser legal e deve ser tão estritamente definida e precisa quanto possível. Além disso, a finalidade do acesso e da recolha de dados deve ser claramente indicada no momento do acesso ou da recolha.

3. MITIGAÇÃO DOS RISCOS E AVALIAÇÃO DOS RISCOS, DANOS E BENEFÍCIOS

Os dados devem ser recolhidos e utilizados em conformidade com a legislação aplicável, respeitando a privacidade das pessoas e protegendo os seus direitos. A utilização de dados sensíveis deve implicar a consulta dos grupos interessados ou dos seus representantes para atenuar os riscos associados. Os riscos e danos potenciais não devem ser excessivos em relação aos benefícios da utilização dos dados.

4. DADOS SENSÍVEIS E CONTEXTOS SENSÍVEIS

Quando se recolhem, acedem ou analisam dados relacionados com grupos vulneráveis ou que são classificados como sensíveis, devem ser aplicadas medidas mais rigorosas de protecção de dados. Além disso, é importante ter em conta que os dados não sensíveis podem tornar-se sensíveis em função do contexto em que são utilizados, como factores culturais ou políticos, e da forma como afectam indivíduos ou grupos.

5. SEGURANÇA DOS DADOS

Devem ser implementadas salvaguardas técnicas e organizacionais sólidas para garantir a gestão adequada dos dados e impedir qualquer utilização ou divulgação não autorizada de dados pessoais. Para o efeito, devem ser utilizadas tecnologias de protecção da privacidade ao longo de todo o ciclo de vida dos dados. Além disso, sempre que aplicável, os dados pessoais devem ser desidentificados numa tentativa de atenuar quaisquer riscos para a privacidade.

6. RETENÇÃO DE DADOS E MINIMIZAÇÃO DE DADOS

O acesso, a análise e a utilização dos dados devem ser limitados ao mínimo necessário para que apenas cumpram o objectivo pretendido. Além disso, a quantidade de dados recolhidos também deve ser limitada ao mínimo necessário. A fim de garantir o cumprimento destas disposições, a utilização dos dados deve ser objecto de controlo. Além disso, após a utilização dos dados, estes devem ser permanentemente apagados, excepto se a sua conservação se justificar.

7. QUALIDADE DOS DADOS

Os dados devem ser verificados quanto à sua exactidão, pertinência, integridade, exaustividade e facilidade de utilização, e mantidos actualizados. Os dados de baixa qualidade implicam riscos e devem ser avaliados para detectar preconceitos que possam resultar em discriminação ilegal e arbitrária. O processamento automático de dados deve ser evitado, especialmente quando pode ter um impacto sobre indivíduos ou grupos. Além disso, devem ser efectuadas avaliações periódicas da qualidade dos dados durante o seu ciclo de vida.

8. DADOS ABERTOS, TRANSPARÊNCIA E RESPONSABILIZAÇÃO

Os dados abertos são importantes para promover a inovação, a transparência e a responsabilização, pelo que devem ser abertos sempre que possível, excepto se os riscos forem superiores aos benefícios ou se existirem outras razões legítimas para não o fazer. É igualmente importante estabelecer mecanismos adequados de governação e responsabilização para garantir o cumprimento da legislação aplicável. A transparência é crucial para a responsabilização. Recomenda-se a divulgação pública de informações sobre a utilização de dados, incluindo a natureza, a finalidade e o período de retenção, bem como os algoritmos utilizados para o tratamento de dados, numa linguagem clara e simples, compreensível para o público em geral.

9. DILIGÊNCIA DEVIDA PARA COLABORADORES TERCEIROS

Ao trabalhar com colaboradores terceiros que utilizam dados, estes devem cumprir a legislação relevante, incluindo a legislação sobre privacidade, e aderir a elevados padrões de sigilo, moralidade e ética. Para garantir a conformidade, deve-se proceder a um processo de diligência devida para avaliar as práticas de dados de potenciais colaboradores terceiros. Além disso, deve-se estabelecer acordos juridicamente vinculativos que definam os parâmetros de acesso e tratamento de dados.

African Union Headquaters
P.O. Box 3243, Roosevelt Street
W21K19, Addis Ababa, Ethiopia
www.au.int