AFRICAN UNION
الاتحاد الأفريقي

UNION AFRICAINE

UNIÃO AFRICANA

Addis Ababa, Ethiopia P. O. Box 3243 Telephone: 5517 700 Fax: 5517844
Website: www.au.int

CONSELHO EXECUTIVO
Quadragésima Sessão Ordinária
20 de Janeiro - 03 de Fevereiro de 2022
Adis Abeba, Etiópia

EX.CL/1308(XL)
Original : Inglês

QUARTA SESSÃO ORDINÁRIA DO COMITÉ TÉCNICO ESPECIALIZADO EM MATÉRIA DE TECNOLOGIAS DE INFORMAÇÃO E DE COMUNICAÇÃO (CCITC-4), 25 A 27 DE OUTUBRO DE 2021

QUARTA SESSÃO ORDINÁRIA DO COMITÉ TÉCNICO ESPECIALIZADO EM MATÉRIA DE TECNOLOGIAS DE INFORMAÇÃO E DE COMUNICAÇÃO (CCITC-4)
25 a 27 de Outubro de 2021
Por Videoconferência

SESSÃO MINISTERIAL

27 de Outubro de 2021

RELATÓRIO DA REUNIÃO

INTRODUÇÃO

1. A Quarta Sessão Ordinária do Comité Técnico Especializado da União Africana em matéria de Tecnologias da Comunicação e da Informação (CTE-TIC-4) foi realizada por videoconferência no dia 27 de Outubro de 2021. A sessão do Comité foi precedida por uma Reunião de Peritos realizada nos dias 25 e 26 de Outubro de 2021.

PARTICIPAÇÃO

2. A reunião contou com a participação de representantes dos seguintes Estados-membros: Argélia, Angola, Botsuana, Burkina Faso, Burundi, Camarões, Chade, República Centro Africana, Comores, Congo (República Democrática), Congo (República), Costa do Marfim, Djibuti, Egipto, Guiné Equatorial, Eritreia, Etiópia, Gabão, Gâmbia, Gana, Quénia, Lesoto, Líbia, Marrocos, Moçambique, Namíbia, Níger, Ruanda, República Árabe Saharaoui Democrática, Senegal, África do Sul, Tanzânia, Togo, Tunísia, Uganda, Zâmbia e Zimbabué. A lista de participantes está apensa ao presente relatório como **Anexo I.**

3. Estiveram igualmente presentes representantes da AUDA/NEPAD e da Comunidade Económica dos Estados da África Central (ECCAS).

4. A reunião contou a ainda com a participação das seguintes organizações e agências africanas e internacionais: União Africana das Telecomunicações (ATU), União Postal Pan-Africana (PAPU) e Smart Africa.

5. De igual modo, estiveram presentes as seguintes organizações: União Internacional das Telecomunicações (UIT), União Europeia (UE), Banco Mundial (BM), GIZ, Sociedade da Internet (ISOC), Huawei e ICT Research Africa.

I. CERIMÓNIA DE ABERTURA

6. A cerimónia de abertura não foi realizada a fim de dedicar atenção à obtenção do quórum necessário para que a reunião prosseguisse.

II. ELEIÇÃO DA MESA DO CTIC-4

7. Com base no princípio de rotatividade e representação geográfica, foi eleita a seguinte Mesa do STC-CICT-4.

AFRICA	
Congo (Rep)	Presidente da Mesa
AFRICA	
África do Sul	1.º Vice-presidente
AFRICA	
Níger	2.º Vice-presidente
AFRICA	
Ruanda	3.º Vice-presidente
AFRICA	

Egipto	Relator Interino da Mesa

8. A África do Norte irá realizar consultas e irá confirmar oportunamente o Estado-membro que será designado como Relator.

III. APROVAÇÃO DA AGENDA E DO PROGRAMA DE TRABALHO

9. A reunião adoptou a seguinte agenda com alterações:

1) Cerimónia de abertura;
2) Eleição da Mesa;
3) Adopção da agenda e do programa de trabalho;
4) Análise do Relatório dos Peritos;
5) Análise e adopção da Declaração de 2021;
6) Apreciação de projectos de quadros continentais sobre interoperabilidade de identificação digital e política continental de dados;
7) Apreciação e adopção do Relatório Ministerial;
8) Diversos
9) Cerimónia de encerramento.

10. O programa de trabalho adoptado é apresentado como Anexo II.

IV. ANÁLISE DO RELATÓRIO DOS PERITOS

11. O Relator Interino, o Egipto, apresentou o relatório dos peritos. O relatório destacou as realizações e desafios encontrados e os peritos formularam os seguintes comentários:

Comissão da UA

- Estratégia de Transformação Digital (ETD) para África com o desenvolvimento da Estratégia e Plano de Implementação da Saúde Digital da UA, Estratégia e Plano de Implementação da Educação Digital da UA, Estratégia e Plano de Implementação da Agricultura Digital da UA, Estratégia de Comércio Electrónico da UA, Directrizes sobre a abordagem comum da transformação digital postal em África e desenvolvimento do Quadro de Monitorização e Avaliação (M&A) para a Estratégia de Transformação Digital para África (ETED);

- Projecto de Quadro de Interoperabilidade da UA para a Identificação Digital e Quadro Continental de Política de Dados da UA;

- Segunda fase do PIDA (2021-2030) que inclui projectos sobre TIC juntamente com Recursos Hídricos, Energia e Transportes, um total de 12/69 projectos sobre TIC foram seleccionados e validados pela cimeira da UA em Fevereiro de 2021, para reforçar a conectividade interna a nível de África e baseia-se na abordagem integrada de corredor que procura alavancar as tecnologias digitais para o desenvolvimento de infra-estruturas inteligentes.

- Iniciativa de Política e Regulamentação para África Digital (PRIDA) com a selecção das Condições de Entrada no Mercado (Regime de Autorização/Licenciamento) e Protecção de Dados Pessoais e Localização de Dados como tópicos para harmonização de indicadores e Metodologia de Monitorização e Avaliação (M&A) sobre os dois tópicos e o desenvolvimento de dois Protótipos de M&A para medir o grau de harmonização de cada tópico em todo o continente.

- Segurança Cibernética destacando os progressos alcançados na revisão da Convenção de Malabo e o desenvolvimento de uma Política Continental de Segurança Infantil Online e de uma Estratégia Continental de Segurança Cibernética;

- Recomendações da Política da UA sobre Soluções Digitais para Rastrear, Diagnosticar e Partilhar Informação sobre Pandemias em África.

- Construção da Identidade da Marca da UA e Promoção do Mandato e Agenda da UA marcados pela instituição da nova identidade da marca em toda a CUA e outros Órgãos da UA, promoção da Agenda 2063 tanto em meios tradicionais como em plataformas digitais para melhorar a sensibilização e o conhecimento da Agenda 2063, bem como a compreensão dos Mandatos e Programas da UA;

- Melhoria da Visibilidade Empresarial, Advocacia e Relações Públicas destacando o desenvolvimento e lançamento de 2 aplicações móveis para chegar aos utilizadores de telemóveis e tablets, iniciativas de advocacia para ratificar os tratados da UA, realização de uma campanha anual das Mulheres Africanas nos Meios de Comunicação Social e redefinição das prioridades das actividades no sentido de posicionar a União Africana e o CDC África na vanguarda da gestão e combate à pandemia de COVID-19 em África.

AUDA NEPAD

- Em conformidade com a Convenção de Malabo sobre Segurança Cibernética e Protecção de Dados Pessoais, a AUDA-NEPAD realizou avaliações de segurança cibernética em dez Estados-membros da União Africana, nomeadamente Benin, Chade, República do Congo, República Democrática do Congo, Guiné, Quénia, Mauritânia, Marrocos, Senegal e Tunísia e publicou relatórios individuais de países, bem como um relatório consolidado: Relatório de Avaliação de Segurança Cibernética da AUDA-NEPAD (https://www.au-pida.org/download/cybersecurity-assessment-report/).

- A AUDA-NEPAD está igualmente a colaborar com o Fórum Global sobre Conhecimentos Cibernéticos (GFCE) num projecto que visa desenvolver os conhecimentos em matéria de Reforço de Capacidade no domínio da Cibernética (CCB) para permitir aos Estados-membros da UA compreender melhor as capacidades cibernéticas, bem como identificar e abordar as suas

necessidades nacionais em matéria de capacidades cibernética, bem como reforçar a sua resiliência cibernética.

- O segundo Plano de Acção Prioritário do PIDA (PIDA PAP II) foi adoptado pela Assembleia da UA em Fevereiro de 2021. Dos 69 projectos, 11 encontram-se no sector das TIC.

PAPU

- Os progressos alcançados na implementação do projecto sobre conectividade e Electrificação e conectividade dos Correios nas zonas rurais do Quénia, Malawi, Tanzânia e Uganda mostraram progressos notáveis na mobilização de fundos e na implementação do projecto.

- A PAPU e Estados-membros implementaram estratégias de combate à COVID-19, incluindo a intensificação das remessas e dos serviços electrónicos oferecidos.

- PAPU aconselhou os países membros a emitir EmiS (Mensagens do Sistema de Informação de Emergência) sobre os efeitos da COVID-19, melhores práticas que devem ser adoptadas durante o período da pandemia, bem como sobre como o posto pode continuar a ser relevante;

- PAPU enviou um questionário em Abril de 2020 para avaliar a situação nos Estados-membros e a forma como estes estavam a lidar com as circunstâncias;

- Realizou um webinar com a AFRAA em 12 de Maio de 2020, e concluiu que o correio oferece serviços essenciais e que os governos devem, portanto, ser sensibilizados como tal para facilitar a circulação do correio utilizando aviões de carga.

ATU

- Preparação da Conferência Mundial de Radiocomunicações da UIT (WRC-23), Assembleia de Normalização de 2020 (WTSA-20), Conferência Mundial de Desenvolvimento das Telecomunicações 2021 (WTDC-21) Reuniões Preparatórias Africanas para a UIT PP-22.

- **ESTUDOS E RELATÓRIOS DESENVOLVIDOS PELA ATU**

  (a) **Estratégia de 4RI:** com o apoio do Governo da África do Sul foi recrutado um Consultor que desenvolveu o projecto de Estratégia da 4ª Revolução Industrial (4RI) que foi apresentado aos Membros da ATU pela primeira vez em Outubro de 2020 durante um Workshop de validação e foi posteriormente revisto tendo em conta os subsídios e comentários dos Membros e submetido à sessão do Conselho da ATU de 2021.

  (b) **Gestão de Resíduos Electrónico**: A ATU também desenvolveu directrizes sobre gestão de resíduos electrónicos para África e está a interagir com os

membros sobre a implementação destas directrizes. A ATU espera poder colaborar mais com a CUA no apoio a este processo, uma vez que todos se esforçam no sentido de servir o continente.

(c) **Desafio da Inovação Digital**: A ATU também realizou com êxito duas edições do "Desafio da Inovação Africana" de 2020 e 2021 respectivamente, em colaboração com a ITU e outros parceiros com o objectivo de promover o espírito de inovação em África e proporcionar uma oportunidade única aos jovens africanos para expressarem as suas ideias e talento inovadores e reconhecerem o papel preponderante do ecossistema para alcançar o desenvolvimento digital em África. Este ano, a edição de 2021 do Desafio identificou instituições africanas que criam um ambiente favorável à juventude para desenvolver inovações no domínio das TIC. Entre as instituições que participaram no concurso figuram organismos responsáveis pela definição de políticas, incubadoras, universidades e organizações sem fins lucrativos. Esta iniciativa surge em reconhecimento do papel crítico que tais organizações desempenham e da importância de investir em solo fértil a partir do qual os inovadores podem crescer. O Desafio culminou numa cerimónia de entrega de prémios realizada em Outubro de 2021, onde os 10 primeiros classificados foram atribuídos prémios em dinheiro e receberam o título de "Melhor Prática de Ecossistema da ATU em África 2021 Permitindo à Juventude a Inovação no domínio das TIC".

(d) **Migração para a estratégia IPv6:** A ATU também desenvolveu um quadro estratégico de Migração para IPv6 para o continente e, em parceria com a Afrinic, a ATU pretende conceber um programa de desenvolvimento de capacidades neste domínio e aguarda com expectativa interagir com os seus membros e partes interessadas a fim de implementar a estratégia em colaboração com a CUA e organizações congéneres no apoio a este processo, uma vez que todos se esforçam no sentido de servir o continente.

(e) **Modelo de estrutura de competências na área electrónica:** A ATU desenvolveu igualmente um modelo de estrutura de competência cibernética para África de modo que possa responder às necessidades futuras do mercado digital africano e aguarda com expectativa a interacção com os seus membros, parceiros e partes interessadas, a implementação deste modelo em colaboração com a CUA e organizações congéneres no apoio a este processo, uma vez que todos se esforçam para servir o continente. O dia das Tecnologias de Comunicação e Informação da ATU, que terá lugar a 7 de Dezembro de 2021, será celebrado sob o seguinte tema: "Desenvolvimento de Competências Digitais para a Transformação Digital de África".

PROGRAMAS EM CURSO OU RECENTEMENTE CONCLUÍDOS

- **Comunicação Radiofónica**

(a) Desenvolvimento de recomendações sobre a implementação de tecnologias emergentes destinadas a orientar os países africanos na sua implementação, incluindo 5G;

(b) Desenvolvimento de recomendações destinadas a orientar os países africanos nas práticas modernas de gestão do espectro;

(c) Optimização do Plano de Frequência de Radiodifusão FM (o Plano GE84) para África com o objectivo de identificar novos canais utilizáveis para sustentar o crescimento da rádio FM em África;

(d) Desenvolvimento de uma Estratégia para a introdução da radiodifusão sonora digital em África;

(e) Foi realizada a 1ª edição do Plano de Espectro Africano (AfriSAP), que visava servir de referência para os planos de espectro sub-regionais e/ou nacionais;

(f) Foi concluída, juntamente com o referido AfriSAP, a harmonização de frequências para telecomunicações de emergência (PPDR);

(g) Foi desenvolvida uma estratégia de gestão de recursos orbitais e de frequências de satélite destinada a optimizar a aquisição, retenção e utilização destes recursos em África;

(h) Foram formuladas recomendações destinadas a orientar os países africanos sobre a forma como a política, regulamentação e práticas do espectro podem fomentar a conectividade rural.

- **Padronização e sectores de desenvolvimento**

(a) Desenvolvimento de um modelo de enquadramento/directrizes sobre Centros de Dados e Serviços de Computação em Nuvem e Infra-estruturas para África;

(b) Desenvolvimento de um livro branco sobre as melhores práticas de conectividade e acessibilidade em África e de um quadro regional para facilitar o acesso aos cabos submarinos a todos os países, particularmente os do interior.

(c) Desenvolvimento de uma política e normas comuns de segurança digital para a segurança das redes e sistemas de informação;

(d) Reforço de capacidades em parceria com a Huawei sobre tecnologias emergentes e ferramentas digitais (computação em nuvem, etc...);

(e) Livro branco sobre acesso e conectividade e quadro de cooperação para facilitar o acesso a cabos FO submarinos para os países do interior;

(f) Estudo para desenvolver um Observatório das TIC para África.

12. Os desafios apresentados incluem o seguinte:

(i) Recursos limitados para implementar a Estratégia de Transformação Digital para África e falta de enquadramento e mecanismo para monitorizar e avaliar a implementação da estratégia;

(ii) Restrições de viagem decorrentes da pandemia da COVID-19 e encerramento de escritórios governamentais devido à COVID-19 (um desafio onde a informação online é limitada);

(iii) Poucas políticas de economia digital a nível dos Estados-membros e Regional que facilitem um ambiente favorável ao comércio digital e à economia digital;

(iv) Participação limitada na partilha ou recolha de dados, fraca mobilização de recursos para a preparação de projectos do PIDA, particularmente os recursos nacionais;

(v) Atrasos nos acordos do PIDA entre países e não-alinhamento do quadro jurídico e regulamentar para os países em causa e nomeação de pontos focais sectoriais do PIDA de alguns Estados-membros/Ministérios;

(vi) Orçamento insuficiente e falta de pessoal da direcção de comunicação;

(vii) Insuficiência de fundos para o financiamento de projectos tais como Endereços e Códigos Postais, Projecto de Electrificação e Conectividade;

(viii) Procura de soluções digitais para serviços financeiros postais, especialmente na sequência da Pandemia COVID-19; e

(ix) Taxas de transporte elevadas devido à utilização de taxas de carga para o transporte de correio em vez de utilizar as taxas de correio UPU/IATA mais baixas;

(x) Implementação de estratégias para combater a COVID-19 incluindo o reforço das remessas e dos serviços electrónicos oferecidos.

13. O relatório é apenso como **Anexo III.**

14. Os Ministros tomaram nota do relatório e fizeram os seguintes comentários:

(i) Saudaram os peritos pelo trabalho realizado neste período difícil;

(ii) Deram a conhecer que o Egipto é o Relator interino uma vez que a região da África do Norte realiza consultas visando chegar a acordo sobre o país que será designado como relator.

V. Apreciação do Quadro de Interoperabilidade da UA para a Identificação Digital e do Quadro de Política de Dados Continental da UA

15. Após a apresentação dos dois quadros, os Ministros fizeram as seguintes recomendações:

Quadro de Interoperabilidade da UA para a Identificação Digital

(i) Os Estados-membros devem fornecer subsídios no prazo de 1 mês no âmbito do projecto de Quadro de Interoperabilidade da UA para a Identificação Digital, a fim de permitir a sua adopção pelos órgãos deliberativos da UA;

(ii) Elogiar a CUA pelo excelente trabalho realizado;

Quadro Continental de Política de Dados da UA

(i) Os Estados-membros devem fornecer subsídios no prazo de 1 mês no âmbito do Projecto de Quadro Continental de Política de Dados para permitir a sua adopção pelos Órgãos Deliberativos da UA.

(ii) Elogiar a CUA pelo excelente trabalho realizado.

VI. Consideração e adopção da declaração de 2021 (Anexo IV).

16. A declaração foi adoptada com alterações.

VII. Consideração da data e local do próximo CTE

17. A República do Congo ofereceu-se para acolher a 5ª Sessão Ordinária do CTE em 2023.

18. A data do CTE será fixada oportunamente em colaboração com a Mesa do CTE e a Comissão da UA,.

VIII. Análise e adopção do Relatório Ministerial

19. A Comissão da UA foi convidada a enviar o relatório para os Estados-membros.

IX. Diversos

20. Neste ponto não foi levantada nenhuma questão.

X. Encerramento da reunião

21. Na sua intervenção de encerramento, S.E. Dr. Amani ABOU-ZEID, Comissário da UA para Infra-estruturas e Energia, em nome da Comissão da União Africana, agradeceu ao Presidente da Mesa cessante do CTE sobre Comunicação e TIC pela sua liderança na orientação dos trabalhos do CTE durante o período 2019-2021 e felicitou-o pela realização nos dois sectores apesar do desafio imposto pela pandemia da COVID-19.

22. Igualmente, desejou calorosas boas-vindas à nova Presidente do CTE sobre Comunicação e TIC e à Mesa eleita e assegurou-lhes que, juntamente com a sua equipa, trabalhariam incansavelmente com a Mesa para melhorar a Transformação Digital de África.

23. Concluiu a sua intervenção assegurando aos Ministros que a Comissão da União Africana continuará a criar parcerias e colaborações mais fortes e trabalhará com todas as partes interessadas para aproveitar a tecnologia para o bem, e assegurar que ela seja inclusiva e segura e a utilizará para aumentar a dinâmica da recuperação da pandemia da COVID-19.

24. Por seu turno, S.E. o Ministro Léon Juste IBOUMBO, Ministro dos Correios, Telecomunicações e Economia Digital da República do Congo, Presidente da Mesa eleito, congratulou os Ministros e outros participantes pelo seu empenho e participação activa, apesar do actual contexto difícil.

25. O Presidente manifestou a gratidão da República do Congo aos seus pares, especialmente aos Ministros da região do ECCAS, pela sua eleição como Presidente da Mesa, o que confirma a pertinência da visão da República do Congo sobre a digitalização.

26. Outrossim, o Sr. IBOMBO reconheceu as realizações da Mesa presidida pelo Egipto e expressou o seu desejo de beneficiar da valiosa experiência dos membros da Mesa cessante.

27. Antes de concluir a sua intervenção, o Ministro informou os participantes sobre a operacionalização do Centro Africano de Pesquisa em Inteligência Artificial pelo seu país e salientou a sua prontidão para receber todos os africanos.

IEN61748 – 48/48/22/10

QUARTA SESSÃO ORDINÁRIA DO COMITÉ TÉCNICO ESPECIALIZADO DE COMUNICAÇÃO E TIC (CTE-CTIC)

27 de Outubro de 2021, Por Videoconferência

AU/STC-CICT-4/MIN/Decl.
Original: Inglês

DECLARAÇÃO DO CTE-CTIC 2021

PREÂMBULO

NÓS, os Ministros responsáveis pela Comunicação e TIC, reunidos por videoconferência a 27 de Outubro de 2021 na Quarta Sessão Ordinária do **Comité Técnico Especializado de Comunicação e TIC**;

ORIENTADOS PELO Acto Constitutivo da União Africana(UA);

RECORDANDO as Decisões Assembly/AU/Dec.227(XII) e Assembly/AU/Dec.365(XIVI), adoptadas em Janeiro de 2009 e Julho de 2011, respectivamente, sobre a configuração dos Comités Técnicos Especializados (CTE) e as modalidades de sua operacionalização;

TENDO PRESENTE a DECLARAÇÃO Assembly/AU/Decl.1(XIV), adoptada na 14.ª Sessão Ordinária da Conferência da UA sobre as Tecnologias da Informação e de Comunicação em África, Desafios e Perspectivas de Desenvolvimento, realizada em Adis Abeba, Etiópia, em Fevereiro de 2010;

CONSIDERANDO a Declaração Assembly/AU/Decl.2(XVIII), adoptada na 18.ª Sessão Ordinária da Conferência da UA, realizada em Adis Abeba, Etiópia, em Janeiro de 2012, sobre o Programa para o Desenvolvimento de Infra-estruturas em África (PIDA) e a Decisão Assembly/AU/Dec.529(XXIII) da 23.ª Sessão Ordinária da Conferência da UA, realizada em Malabo, Guiné Equatorial, em Junho de 2014, que adoptou a Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais;

CONSIDERANDO IGUALMENTE a Declaração Assembly/AU/Decl.3(XXX) adoptada na 30.ª Sessão Ordinária da Conferência da UA em Adis Abeba, Etiópia, realizada nos dias 28 e 29 de Janeiro de 2018 sobre Governação da Internet e Desenvolvimento da Economia Digital de África;

RECORDANDO a Decisão 1074(XXXVI) do Conselho Executivo sobre os relatórios dos Comités Técnicos Especializados, incluindo a 3.ª Sessão Ordinária do CTE de Comunicação e TIC, realizada em Sharm El Sheikh, República Árabe do Egipto, nos dias 25 e 26 de Outubro de 2019, que aprovou a Estratégia de Transformação Digital para África (ETD) com vista a tirar proveito das tecnologias digitais e da inovação para transformar as sociedades e economias africanas, e solicitou à Comissão para, entre outros:

(i) Mobilizar os recursos necessários para pôr em prática a Estratégia Global de Transformação Digital para África e elaborar a matriz para a execução da Estratégia;

(ii) Promover a estratégia em todas as actividades relevantes da UA, incluindo os CTE;

(iii) Elaborar estratégias/planos de execução sectorial da ETD, incluindo os críticos já identificados para ter uma ETD abrangente para o continente;

(iv) Elaborar directrizes sobre Privacidade, distribuição de conteúdos audiovisuais em linha (OTT), um quadro continental sobre política de dados e um roteiro e directrizes para harmonização e implantação de espectro para redes actuais e

futuras de banda larga móvel e sem fio, tais como Telecomunicações Móveis Internacionais (IMT) 2020 /5G;

(v) Dedicar recursos apropriados para a execução de um programa abrangente de Cibersegurança que inclua assistência aos Estados-Membros da UA para a adopção de estratégias cibernéticas, legislação cibernética e estabelecimento de Equipas de Resposta a Incidentes Informáticos (CIRT-Computer Security Incident Response Team)/Equipas de Resposta a Emergências de Segurança (CERT-Computer Emergency Response Teams);

(vi) Apresentar um relatório de auditoria dos activos comuns da Rede Electrónica Pan-Africana com implicações financeiras antes de aplicar a recomendação dos ministros competentes de transferir os seus activos para a Organização Regional Africana de Comunicação por Satélite (RASCOM); e

(vii) Assegurar a instituição do guia de estilo de marca e de comunicação e das políticas e procedimentos de comunicação na Organização.

TENDO EM CONTA o advento da pandemia da COVID-19 e a resposta do sector da Comunicação e das TIC à pandemia, conforme descrito na Declaração da Mesa da reunião do CTE-CTIC de 5 de Maio de 2020;

RECONHECENDO os esforços feitos pela CUA, pelas Agências Especializadas da UA e pelas Organizações Regionais, bem como as organizações internacionais que facilitam e executam a Estratégia de Transformação Digital para África (ETD) em todo o continente e elaboram estratégias digitais sectoriais para a Educação, Saúde, Agricultura, Comércio Electrónico e Sector Postal, elaboração do Quadro Continental de Políticas de Dados da UA e do Quadro de Interoperabilidade para a Identificação Digital, estratégia de segurança cibernética continental, documento de política de protecção da criança em linha, metodologia de harmonização e modelo destinado a recolher projectos em curso e projectos concluídos relacionados com a transformação digital nos Estados-Membros e nas CER para melhorar a coordenação e facilitar sinergias;

TENDO PRESENTE a procura sem precedentes por tecnologias digitais para facilitar a contenção da pandemia da COVID-19 e aplaudindo as diversas iniciativas para reduzir a propagação da COVID-19, bem como mitigar seus efeitos sociais e económicos;

RECORDANDO a visão da Estratégia de Transformação Digital para África que visa uma sociedade e economia digital integrada e inclusiva em África que melhore a qualidade de vida dos cidadãos africanos, reforce o sector económico existente, permita a sua diversificação e desenvolvimento e assegure a apropriação continental, tendo África como um continente produtor e não apenas consumidor na economia global;

RECORDANDO IGUALMENTE o compromisso de continuar a implementação da estratégia de comunicação e promoção da UA, melhorar a visibilidade corporativa e criar a marca da UA no âmbito da Agenda 2063;

RECORDANDO AINDA a Declaração Solene do 50.º Aniversário da OUA/UA de Maio de 2013 onde os Chefes de Estado e de Governo declararam o seu compromisso de hastear a bandeira da UA e cantar o hino da UA juntamente com as nossas bandeiras e hinos nacionais; e de promover e harmonizar o ensino da história, valores e pan-africanismo

africanos em todas as nossas escolas e instituições educacionais no quadro da promoção da nossa identidade e renascimento africanos;

TENDO PRESENTE a importância da comunicação, marca, promoção e relações públicas para a reputação, reconhecimento e apreciação da União Africana entre todos os seus intervenientes;

CONSCIENTE DA NECESSIDADE de celebrar o 20.º aniversário da União Africana em 2022 a nível continental e da necessidade de elevar a marca da UA a todas as populações africanas no contexto da propagação da COVID-19;

CONSIDERANDO o Relatório da Sessão de Peritos realizada virtualmente, nos dias 25 e 26 de Outubro de 2021;

TENDO ELEITO a seguinte Mesa do CTE-CTIC para um período de dois (2) anos:

ÁFRICA CENTRAL	
República do Congo	Presidente
ÁFRICA AUSTRAL	
África do Sul	1.º Vice-Presidente
ÁFRICA OCIDENTAL	
Níger	2.º Vice-Presidente
ÁFRICA ORIENTAL	
Ruanda	3.º Vice-Presidente
ÁFRICA DO NORTE	
A CONFIRMAR	Relator

TOMAMOS NOTA do relatório da Mesa e **FELICITAMOS** a Mesa pelos resultados;

FELICITA IGUALMENTE a Comissão da UA pelo desenvolvimento de políticas inovadoras e quadros continentais prospectivos para a Interoperabilidade da Identificação Digital e a Política de Dados que estejam em linha com as melhores práticas mundiais.

TOMAMOS IGUALMENTE NOTA do progresso feito para acelerar a implementação da Estratégia de Transformação Digital em sectores críticos, nomeadamente a elaboração da Estratégia e Plano de Implementação da Saúde Digital da UA, a Estratégia e Plano de Implementação da Educação Digital da UA, a Estratégia e Plano de Implementação da Agricultura Digital da UA, a Estratégia de Comércio Electrónico da UA, o Quadro de Política de Dados para África, o Quadro de Interoperabilidade da UA para Identificação Digital, a iniciativa para a revisão da Convenção da UA sobre Cibersegurança e Protecção de Dados Pessoais (“Convenção Malabo”) para estar em conformidade com os mais recentes padrões e normas mundiais no ciberespaço; a iniciativa de elaborar a estratégia continental de segurança cibernética e uma política da União Africana de segurança e empoderamento da criança em linha, a Metodologia e Ferramenta de M&A para medir o grau de harmonização das políticas e regulamentos das TIC & Digitais, e criar a identidade de marca da UA e trabalhar para a criação de um ambiente propício por forma a facilitar o estabelecimento do Mercado Único Digital Africano em linha na ZCLCA, bem como o trabalho realizado para criar a identidade de marca da UA;

COMPROMETEMO-NOS PELA PRESENTE A:

1. **CONTRIBUIR** para a resposta continental coordenada à pandemia da COVID-19 e **mitigar** os seus impactos negativos;

2. **CONTINUAR a** elaborar políticas e regulamentos para facilitar a implantação e utilização de instrumentos digitais seguros e protegidos para melhorar as **respostas** à COVID-19;

3. **PROVIDENCIAR** um parecer no prazo de um mês para enriquecer o Projecto de Quadro de Interoperabilidade da UA para Identificação Digital e o Projecto de Quadro de Política de Dados Continentais da UA para permitir a adopção dos dois quadros pelos Órgãos Deliberativos da UA;

4. **MOBILIZAR** os recursos necessários para implementar o Quadro Continental de Políticas de Dados da UA

5. **TOMAR NOTA** dos resultados do Relatório de Auditoria do Activo Comum da Rede Electrónica Pan-Africana (PAeN) de Telemedicina e Ensino à Distância, bem como da iniciativa de redefinir a Rede para prestar serviços de educação e **saúde** em linha actualizados.

6. **REAFIRMAR** o reconhecimento do sector postal como importante infra-estrutura **nacional** para a inclusão digital, social, financeira e comercial, bem como rede física que complementa as necessidades digitais das pessoas - ligar o mundo físico ao digital;

7. **PROSSEGUIR** as reformas políticas e regulamentares do sector postal a nível **nacional**, regional e continental e a facilitar um maior investimento em infra-estruturas digitais e a reforçar o ritmo da sua transformação digital.

SOLICITAMOS AOS ESTADOS-MEMBROS PARA:

8. **CRIAR** e apoiar a adopção de políticas e regulamentos adequados que facilitem a **implantação** e o uso de ferramentas e soluções digitais para permitir o cruzamento de sectores e a interoperabilidade dos dados para melhorar as respostas à COVID-19;

9. **PROMOVER** a taxa zero de acesso a conteúdos de saúde e educativos como **uma** intervenção crítica e urgente, para combater à pandemia e para apoiar alunos e estudantes confinados em casa devido ao encerramento de escolas, faculdades e universidades;

10. **UTILIZAR** Plataformas Digitais, Portais e Aplicações especialmente aqueles desenvolvidos por africanos para africanos, que podem ajudar a seguir, localizar e testar pessoas que entraram em contacto com uma pessoa infectada, equilibrando os imperativos de saúde, preocupações com privacidade e protecção de dados;

11. **CRIAR parcerias** com empresas tecnológicas privadas, empreendedores

sociais, organizações nacionais e internacionais para fazer uso das tecnologias existentes para gerir a crise da COVID-19;

12. **INCENTIVAR** a concepção de novas aplicações e serviços para ajudar na luta contra a COVID-19, para facilitar serviços como o fornecimento de alimentos e outros artigos essenciais para os mais necessitados, optimizando toda a cadeia de fornecimento através de serviços públicos digitais;

13. **INCENTIVAR** a partilha das melhores práticas sobre a digitalização do seu sector postal para permitir à CUA finalizar e divulgar as directrizes sobre a abordagem comum para a transformação postal digital até 31 de Dezembro de 2021;

14. **MELHORAR** programas de reforço de capacidades em TIC e cibersegurança no continente e **CONECTAR** os não conectados para colmatar o fosso digital e garantir que todos os cidadãos se beneficiem do uso de soluções inovadoras de tecnologia digital para ter acesso a serviços básicos em linha;

15. **CONECTAR** e envolver os correios na implementação de estratégias de combate à COVID-19, incluindo o alargamento do fornecimento de remessas e serviços electrónicos;

16. **PROMOVER** a implementação do Guia de Estilo de Marca e de Comunicação da UA e das Políticas e Procedimentos de Comunicação e assegurar a adopção e utilização da marca UA em todos os Estados-Membros;

17. **COOPERAR** com a CUA na disponibilização das suas emissoras públicas **nacionais** para divulgar a informação proveniente da Comissão no mês de Setembro de 2022 e Maio de 2023, quando o continente celebrará o 20.º aniversário da CUA e o 60.º aniversário da OUA, respectivamente. Isto será feito com o intuito de garantir que todos os cidadãos africanos saibam mais sobre as celebrações e o papel da UA, no contexto da construção da identidade institucional da UA;

18. **PROMOVER** o diálogo com os Ministérios da Educação dos Estados-Membros para encorajar a adopção do ensino e a disseminação de símbolos continentais como o Hino da UA e promover a inclusão da Agenda 2063 nos currículos nacionais;

19. **INCENTIVAR A DIGITALIZAÇÃO DE CERTIFICADOS DE SAÚDE HARMONIZADOS E INTEROPERÁVEIS** que cumprem os requisitos[1] recomendados de viagem da PANABIOS para garantir a mobilidade contínua dos cidadãos africanos dentro do continente para o aumento do comércio intra-africano por forma a facilitar a implementação da ZCLCA.

20. **APOIAR e FACILITAR** a implementação continental dos Modelos de M&A sobre harmonização das Condições de Entrada no Mercado e os Quadros Jurídicos e

[1] A PanaBIOS é construída por tecnólogos africanos e pensadores de IA para fornecer tecnologia de biovigilância e biossegurança, dados e conhecimentos para permitir a criação de corredores de saúde pública na Iniciativa mais ampla de corredores abertos da UA.

Regulamentares de Protecção de Dados;

21. **INCENTIVAR A UTILIZAÇÃO** da Metodologia e Ferramenta de Harmonização para medir o grau de harmonização das TIC & políticas digitais, dos quadros jurídicos e regulamentares, tanto a nível regional como continental;

22. **REFORÇAR** a cooperação regulamentar a nível continental para responder colectivamente aos novos desafios que surgem da digitalização e da crescente convergência dos serviços.

23. **ACELERAR** a implementação do projecto PIDA-PAP2 sobre TIC e defender a integração das tecnologias digitais no desenvolvimento de infra-estruturas inteligentes;

24. **DESENVOLVER** dois projectos-piloto ao longo dos corredores principais do PIDA e em zonas remotas, em linha com a estratégia da UA de desbloqueio do acesso a infra-estruturas e serviços básicos para as zonas rurais e remotas;

25. **CRIAR** grupos de trabalho multi-institucionais sobre identificação digital e a política de dados a nível nacional.

26. **INTEGRAR** o Quadro de Interoperabilidade da UA para a identificação digital e o Quadro Continental de Política de Dados da UA, após a sua adopção, bem como estabelecer a adesão de múltiplos interessados para permitir a circulação e utilização eficaz e responsável de dados a nível nacional.

27. **SOLICITAR AINDA AOS ESTADOS-MEMBROS E ÀS CER** que agilizem a elaboração de políticas, agendas e estruturas nacionais sobre economia digital e comércio digital e intensifiquem a cooperação e o compromisso dos actores privados e os diálogos para desenvolver padrões comuns que, no futuro, actuarão como base da harmonização dos quadros para a integração das economias digitais no continente.

ENCARREGAMOS A COMISSÃO DA UA DE:

28. **VOLTAR A CIRCULAR** o projecto de quadro de interoperabilidade da identificação digital e o quadro de política continental de dados aos Estados-Membros para contributos finais e finalizar os documentos para permitir a sua adopção pelos órgãos deliberativos da UA.

29. **PROSSEGUIR** a elaboração das seguintes estratégias digitais, quadros de políticas e projectos:

    (i) Estratégia e Plano de Implementação da Educação Digital da UA, Educação e Plano de Implementação Digital da UA, Estratégia e Plano de Implementação da Agricultura Digital da UA e estratégia de comércio electrónico;

    (ii) Estratégia de cibersegurança continental;

    (iii) Política de segurança e empoderamento da criança em linha;

(iv) Revisão da Convenção de Malabo sobre Cibersegurança e Protecção de Dados Pessoais e agilizar a entrada em vigor;

(v) Transformação digital do sector postal em África;

(vi) Estratégia continental para melhorar a harmonização de políticas digitais, dos quadros jurídicos e regulamentares para apoiar o estabelecimento do Mercado Único Digital Africano;

(vii) Mapeamento dos projectos ou actividades digitais para as acções propostas pela ETD;

(viii) Arquitectura de implementação da ETD e quadro de M&A;

(ix) Redefinição da Rede Electrónica Pan-Africana para a prestação de serviços de saúde e de educação em linha;

(x) Estratégia continental de IA

(xi) Estatísticas sobre a conectividade digital e o nível de preparação digital dos países africanos

30. **TRABALHAR** com instituições regionais e actores relevantes para elaborar um Plano de Acção com vista a orientar a implementação do Quadro Continental de Política de Dados da UA (curto, médio e longo prazo) após a sua adopção, incluindo acções imediatas para alcançar o mesmo nível de prontidão de dados a nível continental

31. **COORDENAR** a elaboração de um Quadro Comum de Categorização de Dados e Mecanismo de Fluxos de Dados Transfronteiriços que tenha em conta os amplos tipos de dados, os seus diferentes níveis de privacidade e segurança, bem como os diferentes níveis de maturidade de dados e prontidão digital dos países

32. **PONDERAR** alinhamentos do quadro da Política de Dados Continental da UA, após a sua adopção, com o processo da ZCLCA através da inclusão de disposições sobre dados nas negociações dos capítulos da concorrência e da propriedade intelectual.

33. **GARANTIR** que a instituição do Guia de Estilo de Marca & de Comunicação e das políticas e procedimentos de comunicação na organização e nos órgãos e instituições da União Africana;

34. **EFECTUAR** um exercício de avaliação comparativa das dotações orçamentais de comunicação para instituições de natureza e tamanho semelhantes aos da União Africana por forma a estabelecer uma base de referência para o orçamento de comunicação a ser utilizado como um guia de recomendação para um financiamento adequado;

35. **ATRIBUIR** recursos financeiros realistas para capacitar a Direcção de

Informação e Comunicação (ICD) para que possa comunicar melhor e efectivamente com os vários interessados e públicos em diferentes plataformas de comunicação social de forma estratégica e consistente;

36. **PRIORIZAR** a capacitação da Direcção de Informação e Comunicação na primeira fase das reformas institucionais;

37. **IMPLEMENTAR** a Decisão do Conselho Executivo EX.CL/Dec.1069 (XXXV) de Julho de 2019, que todas as actividades da UA relacionadas com as comunicações devem ser geridas pela Direcção de Informação e Comunicação.

38. **APROVAR** iniciativas destinadas a inundar o continente e alcançar os africanos através do uso de estações nacionais de televisão e rádio para realizar as seguintes actividades para o mês de Setembro de 2022 em comemoração do 20.º aniversário da União Africana:

(i) Tocar o hino da UA em todas as estações nacionais no início e no final do dia;

(ii) Içar a bandeira da UA ao lado das bandeiras nacionais nos Estados-Membros,

(iii) Reproduzir um vídeo de celebração a ser produzido pela Direcção de Informação e Comunicação em todas as estações de televisão dos Estados-Membros da UA; este vídeo destacará o caminho que África percorreu sob a UA, bem como os sucessos, os desafios e as medidas de atenuação;

(iv) Transmissão na TV e estações de rádio nacionais de uma conversa em linha com África pelos Presidentes da União e da Comissão, na qual eles irão descrever o impacto da UA e responder a algumas perguntas do público.

39. **SOLICITAR À AUDA-NEPAD** para:

(i) Acelerar a implementação dos projectos PIDA-PAP2 sobre TIC e acelerar a implementação das políticas e regulamentos necessários para facilitar a conectividade transfronteiriça e a integração regional;

(ii) Expandir, em colaboração com actores relevantes, as avaliações de cibersegurança e o desenvolvimento de capacidades para todos os Estados-Membros da UA e trabalhar com os Estados-Membros na concepção de planos de acção específicos para a cibersegurança e a ciber-resiliência;

(iii) Expandir o conjunto de ferramentas de criação de empregos do PIDA para cobrir todos os subsectores das TIC, formar os Estados-Membros sobre a sua utilização e realizar uma análise pormenorizada do potencial de emprego do PIDA e de outros projectos TIC significativos no continente;

(iv) Em conformidade com a abordagem do Corredor Integrado PIDA-PAP 2, incorporar as TIC, a Digitalização e a Cibersegurança na implementação de projectos emblemáticos da Agenda 2063, tais como a Rede Africana Integrada de Comboios de Alta Velocidade, o Mercado Único Africano de

Transporte Aéreo (SAATM), a Zona de Comércio Livre Continental Africana, a Livre Circulação de Pessoas, bem como iniciativas continentais como o Mercado Único Africano de Electricidade (AfSEM);

40. **SOLICITAR ao Secretariado da União Postal Pan-Africana (PAPU)** que ponha em prática e implemente, em coordenação com a CUA, um programa de transformação digital sistemático e coordenado para assegurar que sector postal africano esteja actualizado;

41. **SOLICITAR** ao Secretariado da União Africana de Telecomunicações (ATU) que crie e implemente, em coordenação com a CUA, Programa e iniciativas para facilitar uma utilização harmonizada e óptima do espectro radioeléctrico em todo o continente, com vista a contribuir eficazmente para colmatar a lacuna da conectividade digital em África;

42. **APROVAR** iniciativas semelhantes para o 60.º aniversário da Organização da Unidade Africana em 2023, cujo conteúdo estabeleceria uma correspondência das conquistas alcançadas desde 1963, em vez de começar em 2002 como no 20.º aniversário;

43. **REAFIRMA AINDA O NOSSO PEDIDO** aos parceiros e instituições financeiras multilaterais, incluindo o BAD, o Banco Mundial e outros, para continuarem a prestar apoio na utilização das tecnologias existentes para gerir a pandemia da COVID-19, a implementação da estratégia de transformação digital para África e a implementação global da presente Declaração.

AGRADECIMENTOS:

44. **MANIFESTAR** a nossa gratidão à Comissão da UA pela excelente organização desta conferência.

Feito em 27 de Outubro 2021

AFRICAN UNION

الاتحاد الأفريقي

UNION AFRICAINE

UNIÃO AFRICANA

Addis Ababa, ETHIOPIA P. O. Box 3243 Telephone: 251 11 551 7700 Fax: 251 11 551 7844
Website: www.au.int

EX.CL/1308(XL) Annex 2

PROJECTO DE QUADRO DE INTEROPERACIONALIDADE DA UA PARA A IDENTIFICAÇÃO DIGITAL

Dezembro, 2021

ÍNDICE

SUMÁRIO EXECUTIVO

Centenas de milhões de pessoas em África carecem de identificação legal e muitas mais têm identificações que não são adequadas à era digital. Consequentemente, enfrentam desafios de acesso a serviços e oportunidades que estão a ser criadas através da digitalização. Por conseguinte, sistemas de identificação digital interoperacionais, fiáveis e inclusivos, que proporcionam às pessoas a capacidade de verificar a sua identidade legal num ambiente virtual e não virtual, podem ajudar a enfrentar esses desafios e têm um potencial significativo para acelerar a digitalização das economias e sociedades africanas, apoiando o empreendedorismo e contribuindo para a implementação bem-sucedida da Zona de Comércio Livre Continental Africana (ZCLCA). É por estas razões que a maioria dos países africanos está actualmente a modernizar os seus ecossistemas de identificação, embora em fases diferentes.

O Projecto de Quadro de Interoperacionalidade da UA para a Identificação Digital (o Quadro) estabelece uma visão que **permitirá que todos os cidadãos africanos tenham a possibilidade de aceder com facilidade e segurança aos serviços públicos e privados de que necessitam, quando precisam deles, independentemente da sua localização**. Para este efeito, o Quadro define requisitos comuns, normas mínimas, mecanismos de governação e um maior alinhamento entre os quadros jurídicos com os objectivos que se propõem:

1. Permitir os cidadãos africanos autenticar e verificar a sua identidade jurídica num ambiente virtual e não virtual para aceder aos serviços dos sectores público e privado nos Estados-membros da UA;
2. Capacitar os cidadãos africanos com controlo sobre os seus dados pessoais, incluindo a capacidade de revelar selectivamente apenas os atributos necessários para uma determinada transacção; a informação pessoal a revelar deve ser mínima, proporcional e conter apenas a informação relevante para essa transacção que considerou a situação particular de África e em conformidade com as melhores práticas internacionais[2].
3. Reforçar a confiança e a interoperacionalidade entre os sistemas de identificação fundacional dos Estados-membros da UA.

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 interoperacionalidade em todo o continente. Os indivíduos que possuem uma identificação de um sistema nacional poderão obter uma credencial de identidade digital interoperacional (IDC-ID) que assumirá a forma de um crédito verificável[3]. Serão estabelecidas normas para o quadro de interoperacionalidade que definirão elementos fundamentais, pela IDC-ID e que demonstrarão a confiança nas credenciais digitais conforme criadas sob a governação de um quadro fiável que define as condições sob as quais tais credenciais serão emitidas por fontes fidedignas dos Estados-membros da UA.

[2] O Regulamento Geral da UE sobre Protecção de Dados (GDPR)
[3] As reivindicações são uma colecção de atributos sobre uma pessoa em causa: por exemplo, nome de família, dados de nascimento. Uma alegação verificável é uma versão inviolável desta informação que pode ser verificada criptograficamente para verificar a sua autenticidade.

Os Estados-membros da UA são livres de escolher como querem emitir esta credencial digital. Pode ser armazenado num formato puramente digital numa aplicação baseada em telefones inteligentes, um servidor baseado em nuvem, um cartão inteligente ou uma ligação à representação digital pode ser estabelecida usando um código de barras de uma ou duas dimensões num documento em papel (impresso em papel, cartão plástico). Podem igualmente decidir reutilizar esta norma para representar dados de identidade a nível nacional, como parte de uma solução de identificação digital a nível continental ou das CER, ou mesmo emitida separadamente em complemento dos sistemas de identificação digital preexistentes.

A Estrutura será baseada no desenvolvimento de sistemas de identificação fundacionais interoperacionais, inclusivos e de confiança, uma vez que estes fornecem a espinha dorsal de fontes de dados fiáveis sobre a identidade legal das pessoas, permitindo assim ao IDC-ID alcançar níveis mais elevados de garantia. Os Estados-membros da UA são, portanto, incentivados a reforçar os seus sistemas de identificação fundacionais e os *Princípios de Identificação para o Desenvolvimento Sustentável.* Este quadro baseia-se igualmente em esforços continentais paralelos para criar um ambiente propício com vista a proteger os dados pessoais, manter a segurança cibernética e salvaguardar os direitos das pessoas, com a adopção da Convenção de Malabo sobre Segurança Cibernética e Protecção de Dados Pessoais[4] e o trabalho em curso para desenvolver um quadro de política continental de dados.

A emissão do IDC-ID pode ser completada com uma infra-estrutura que permita casos de utilização mais avançada, tais como a autenticação à distância. Este Quadro destaca várias opções técnicas à disposição dos Estados-membros da UA para implementar este nível, por exemplo, uma federação de fornecedores de identidade que proporcione mecanismos de autenticação aos detentores de IDC-ID, ou o desenvolvimento de soluções de carteira de identidade digital ou quaisquer outros modelos que permitam a interoperacionalidade. Os Estados-membros da União Africana poderão também procurar um maior acordo sobre a forma de estabelecer esta infra-estrutura do nível de autenticação e estabelecer parcerias com as CER e outras iniciativas continentais que já estão a investigar a introdução de soluções interoperacionais de identificação digital fundacionais para aceder aos serviços à distância.

A implementação do Quadro baseia-se no pressuposto de que este será adoptado e aprovado pelos Estados-membros da UA. A potencial exclusividade, os fracos mecanismos de segurança, a erosão da privacidade pessoal, a incerteza sobre o benefício do sistema de identificação digital fundacional, a falta de capacidade técnica e financeira, a seca no centro de dados em toda a África para armazenar dados sensíveis e a presença de sistemas de identificação não operacionais e de quadros legais e regulamentares desactualizados são os desafios identificados a serem mitigados.

O documento é constituído pelas seguintes secções: -

[4] União Africana, Convenção sobre Segurança Cibernética e Protecção de Dados Pessoais, vide: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

1. Um historial sobre o trabalho da União Africana que levou à criação deste documento, uma visão geral do estado dos sistemas de identificação em África e uma série de iniciativas que promovem a interoperacionalidade da identificação digital no continente;
2. Uma **introdução** à visão, objectivos, âmbito e casos de utilização potencial para a proposta de Quadro de Interoperabilidade da UA para a Identificação Digital;
3. Uma visão geral dos **elementos fundamentais que constituem o quadro**, nomeadamente os princípios orientadores para a sua concepção e implementação, o modelo seleccionado, os principais componentes da estrutura que terão de ser melhor definidos (por exemplo, regras de participação, interoperacionalidade e requisitos técnicos), bem como três potenciais opções arquitectónicas para definir um nível de autenticação da interoperacionalidade.
4. Um roteiro de alto nível elabora a abordagem faseada proposta para a definição e implementação do Quadro, bem como as acções concretas que os Estados-membros e a União Africana devem levar a cabo
5. Pressupostos de alto nível, desafios, riscos a enfrentar e mecanismos de mitigação recomendados.

O Quadro não exige a criação de um sistema unificado de identificação digital a nível continental, mas estabelece uma interoperacionalidade entre os sistemas de identificação digital fundacionais existentes nos Estados-membros da UA. que tem em consideração a soberania digital dos Estados-membros da UA, as diferenças na implantação da infra-estrutura digital, a disponibilidade de políticas e regulamentos associados, os diferentes tipos de sistemas de identificação e a vulnerabilidade das populações durante e após a implementação dos sistemas interoperacionais de identificação digital.

ACRÓNIMOS E ABREVIATURAS

ZCLCA	Zona de Comércio Livre Continental Africana
AML/CFT	Contra o Branqueamento de Capitais / Combate ao Financiamento do Terrorismo
IPA	Interface de Programação da Aplicação
CUA	União Africana
CUA	Comissão da União Africana
ERII	Equipas de Resposta a Incidentes Informáticos
RCEV	Registo Civil e Estatísticas Vitais
APD	Autoridade de Protecção de Dados
AIPD	Avaliação do impacto da protecção de dados
CAO	Comunidade da África Oriental
CEDEAO	Comunidade Económica dos Estados da África Ocidental
GIZ	Gesellschaft für Internationale Zusammenarbeit
GSMA	Associação GSM
MSE	Módulos de Segurança de Equipamentos
TIC	Tecnologias de Informação e Comunicação
CDI-ID	Credencial Digital Interoperacional de Identidade
UIT	União Internacional das Telecomunicações
CEC	Conheça o seu cliente
NDG	Nível de Garantia
QCPA	Quadro de Confiança Pan-Africano
CER	Comunidade Económica Regional
RP	Relying Party
AFAI	Aliança Fiduciária da África Inteligente
O Quadro	Quadro de Interoperacionalidade da UA para a Identificação Digital
UNECA	Comissão Económica das Nações Unidas para África
WURI	Identificação Única da África Ocidental para a Integração e Inclusão Regional

Ver Anexo I para definições de trabalho.

1. ANTECEDENTES

1.1. Contexto

Ser capaz de provar a sua identidade é essencial para a sua capacidade de aceder aos serviços e exercer os seus direitos. Tradicionalmente, a prova de identidade podia ser feita com base na familiaridade, aparência e comprovação por outros, que trabalhavam em comunidades mais pequenas e informais. À medida que as sociedades e economias se tornaram maiores, mais formalizadas e integradas, foram introduzidas credenciais físicas como documentos de identificação e passaportes para estabelecer a confiança. Contudo, à medida que os países mudam para sociedades e economias digitais, tais credenciais físicas não são muito úteis para provar a identidade através da Internet e realizar outras transacções digitais, tais como pagamentos digitais e partilha de dados pessoais. Um pré-requisito para a confiança electrónica são, portanto, as identidades digitais, representadas por identificações digitais que utilizam tecnologias e abordagens modernas para permitir às pessoas provar e verificar com segurança a sua identidade virtual.

A identificação e em particular as identificações digitais podem proporcionar uma vasta gama de benefícios para os países, tais como a boa governação, inclusão financeira, igualdade de género e o empoderamento das mulheres, e o reforço da protecção social, dos cuidados de saúde e dos resultados da educação. Para as pessoas, fornecem um instrumento para fazer valer os seus direitos e elegibilidade para os serviços e transacções. Da mesma forma, proporcionam uma plataforma para governos e empresas para racionalizar, expandir e inovar a sua prestação de serviços operacionais através da utilização da digitalização e da automatização, especialmente quando encarada como uma “pilha digital” com partilha de dados e plataformas de pagamento digital de confiança. Considerando que a Internet não tem fronteiras, as identificações digitais que são emitidas num país e reconhecidas noutros podem também ser um poderoso motor de integração social e económica, seja a nível bilateral, regional ou global.

As identificações digitais alcançam a maior segurança e impacto quando se baseiam na identidade legal dos indivíduos. A identidade legal é tipicamente gerida pelo ecossistema de identificação fundacional de um país, incluindo o registo civil, a identificação nacional e outros sistemas semelhantes. No entanto, centenas de milhões de pessoas em África ainda carecem de identificação fundacional, tal como um BI nacional ou uma certidão de nascimento.[5] É neste contexto que em Julho de 2016 a Conferência da União Africana declarou 2017-2026 como a década para o reposicionamento da CRVS em África como agenda de desenvolvimento continental, regional e nacional e instou os governos a responder com acções apropriadas.

[5] Banco Mundial, Global ID4D Dataset, vide: https://id4d.worldbank.org/global-dataset

Agenda 2063: A África que queremos, que é o quadro estratégico para o desenvolvimento socioeconómico e a transformação do continente num período de 50 anos, exigiu uma identidade jurídica para todos. A Estratégia de Transformação Digital para África (ETED) aprovada na 36ª Sessão Ordinária do Conselho Executivo da União Africana em Fevereiro de 2020 em Adis Abeba, Etiópia (EX.CL/Dec.). 1074(XXXVI) também sublinhou a importância da Identificação Digital como um elemento fundamental para a criação de um Mercado Único Digital (uma missão que é também partilhada pela Aliança Inteligente de África) em conformidade com a ZCLCA.

A Estratégia de Transformação Digital para África reconheceu igualmente que o desenvolvimento da economia e da sociedade digitais depende de importantes facilitadores, nomeadamente um forte ambiente favorável no que diz respeito à segurança cibernética e à protecção de dados.
A Convenção Malabo de 2014 sobre Segurança Cibernética e Protecção de Dados Pessoais[6] estabelece um quadro jurídico, político e regulamentar que apoia a criação de um ambiente digital seguro para a transacção digital, o comércio electrónico e a transferência de dados. Infelizmente, este quadro jurídico ainda não foi assinado e ratificado pelo número necessário de Estados-membros da UA para a sua entrada em vigor, o que limita efectivamente a sua eficácia.[7] Tal quadro jurídico não só contribuirá para a promoção da confiança no Quadro e inclusão, mas também mitigará os riscos ligados à vigilância e discriminação não autorizadas, particularmente para grupos vulneráveis ou marginalizados, bem como assegurará a responsabilização das autoridades de implementação.

1.2. Situação dos sistemas de identificação em África

Os sistemas de identificação (ID) fiáveis e inclusivos são um factor impulsionador de muitos resultados de desenvolvimento tais como a erradicação da pobreza, boa governação, migração segura e ordenada, protecção social, igualdade de género, e são um importante motor da transformação digital. Dada a necessidade fundamental de uma identificação e autenticação electrónica segura e precisa, a identificação digital e outros serviços de confiança - como as assinaturas electrónicas - representam a próxima fronteira para os países do continente. Quando activados por infra-estruturas digitais que colocam pessoas e organizações em linha, os serviços de identificação digital e de confiança podem ser alavancados por plataformas governamentais e comerciais para facilitar uma variedade de transacções digitais, incluindo pagamentos digitais. A nível de país, a identificação digital poderia funcionar como um identificador único para os sistemas centrados no cidadão, tornando viável a integração de sistemas. Em conjunto, as plataformas de identificação digital e de

[6] União Africana, Convenção sobre Segurança Cibernética e Protecção de Dados Pessoais, vide: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
[7] Desde Julho de 2021, 14 dos 55 EM assinaram a Convenção Malabo, entre os quais 8 EM a ratificaram. Para entrar em vigor, é necessária uma ratificação por pelo menos 15 Estados-membros

pagamentos fornecem os meios para avançar para uma sociedade sem dinheiro, criando ganhos de produtividade, reduzindo a corrupção e a fraude, e melhorando ainda mais a conveniência do utilizador.

Em todo o continente, existe uma vasta gama de tipos de sistemas de identificação e níveis de ligações de desenvolvimento com a prestação de serviços. Muitos outros encontram-se em níveis intermédios de desenvolvimento com lacunas de cobertura entre populações vulneráveis e capacidades digitais emergentes, enquanto outros ainda têm sistemas de identificação fundacionais inexistentes ou emergentes. Globalmente, o número de países que implementam sistemas nacionais de identificação aumentou exponencialmente durante as últimas duas décadas, impulsionado pelo desejo de melhorar a eficiência e a orientação dos pagamentos e transferências governamentais, de reforçar a integridade do sector financeiro (incluindo através do registo KYC e SIM) e o das eleições, de reforçar a segurança pública e de promover uma migração segura e ordenada. Há um impulso contínuo para reformar e modernizar a concepção do sistema e as abordagens de implementação em linha com a expansão das provas sobre boas práticas e lições aprendidas com programas de identificação bem-sucedidos.[8] Um bom exemplo é dado pelo Ruanda que conduziu uma campanha para digitalizar a sua economia e dar poder à sua classe média, conduzindo acções como a mudança para uma economia sem dinheiro, que o governo pretende alcançar através da penetração omnipresente dos telemóveis e do acesso de alta velocidade à Internet. O Ruanda aderiu à Aliança Melhor que Dinheiro, uma parceria global empenhada em passar de pagamentos em numerário para pagamentos digitais. O Ruanda já está a realizar uma maior eficiência e receitas ao eliminar custos de cobrança e outras despesas. Tornou-se igualmente um líder do conhecimento na região, e está a partilhar as melhores práticas com outros interessados em seguir um caminho semelhante (Quadro de Investimento Digital dos OSD, ITU/DIAL, 2019).

As capacidades digitais dos sistemas de identificação aumentaram muito, embora a identificação digital no contexto de transacções em linha ainda esteja na sua fase embrionária. Durante a última década, muitos países envidaram esforços para modernizar os seus sistemas de identificação, com o objectivo de criar uma plataforma digital e emitir credenciais que sustentem uma variedade de usos e serviços. Estas reformas envolvem frequentemente uma transição de sistemas baseados em papel para sistemas digitais utilizando a captação e gestão electrónica de dados, e introduzindo mecanismos de verificação e autenticação da identidade digital - por enquanto, principalmente no contexto de transacções presenciais. A maioria (85%) dos países africanos tem sistemas nacionais de identificação baseados numa base de dados electrónica, embora muitos ainda dependam de registos e

[8] Um inquérito de 2018 a funcionários governamentais africanos revelou que 60 por cento dos países africanos tencionavam lançar um sistema de identificação ou modernizar o sistema existente até ao final de 2020.

processos civis em papel, e muitos sistemas oferecem uma utilidade limitada para a prestação de serviços. Os dados biométricos são recolhidos por mais de 70% dos países africanos no momento do registo para garantir a exclusividade das identidades. Embora alguns países - tais como o Quénia, Lesoto, Nigéria, Ruanda, África do Sul - ofereçam serviços de verificação de identidade digital (a ministérios governamentais, bancos, etc.) para validar informações de identidade ou credenciais contra uma base de dados central, a autenticação para a maioria das transacções continua a depender da inspecção manual dos cartões de identificação física. As soluções de identidade digital que permitem autenticação segura para serviços e transacções em linha estão ainda na sua infância no continente, com tais serviços disponíveis apenas em alguns países (por exemplo, na África do Sul por bancos, em Cabo Verde, Seychelles para serviços de governo electrónico).

Apesar de muitas melhorias e do lançamento de novos sistemas nos últimos anos, os países africanos e os seus residentes enfrentam vários desafios no que diz respeito à identificação. Algumas das áreas fundamentais que necessitavam de reforço incluem a acessibilidade dos sistemas de identificação, a sua capacidade de apoiar eficazmente a prestação de serviços, e a implementação de salvaguardas que promovam a confiança e a privacidade dos dados.

Garantir o acesso universal dos sistemas de identificação é um desafio permanente. Estima-se que mil milhões de pessoas em todo o mundo carecem de documentos de identidade básicos - e aproximadamente metade da população reside em África.[9] África é igualmente o berço de 8 dos 10 países com as maiores disparidades de género na identificação a nível mundial e a cobertura de identificação entre adultos na África Subsariana é cerca de 10 pontos percentuais mais baixa entre as mulheres do que entre os homens.[10] Os desafios na identificação começam desde o nascimento: 100 milhões de crianças com menos de cinco anos em África não tiveram seu nascimento registado.[11] As razões para estas lacunas de cobertura são múltiplas e incluem: elevados custos directos e (particularmente) indirectos de inscrição, incluindo o custo da viagem para locais de registo frequentemente distantes; requisitos documentais e administrativos complexos para o registo; e procura limitada nos casos em que os sistemas de identificação oferecem um valor limitado em termos de facilitação do acesso aos serviços.[12]

A utilização de tecnologias modernas também aumentou a complexidade e apresenta novos riscos. Por exemplo, nem todas as soluções estão bem adaptadas às necessidades e contextos locais onde a conectividade à Internet, o acesso à

[9] ID4D Global Dataset 2018: https://id4d.worldbank.org/global-dataset
[10] https://documents1.worldbank.org/curated/en/727021583506631652/pdf/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-An-In-Depth-Look-at-the-2017-ID4D-Findex-Survey.pdf
[11] https://www.unicef.org/media/62981/file/Birth-registration-for-every-child-by-2030.pdf
[12] https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf

electricidade, ou a literacia digital entre funcionários públicos ou a população em geral podem ser limitados. O bloqueio de fornecedores é uma preocupação comum e está muitas vezes associado a custos operacionais insustentavelmente elevados, à interoperabilidade limitada do sistema de identificação e a baixos níveis de supervisão e controlo governamental e individual sobre dados de identidade. Além disso, com a crescente adopção das tecnologias digitais na identificação e autenticação, bem como com a mudança para as credenciais digitais, as pessoas com literacia digital limitada e acesso a dispositivos conectados correm o risco de ficar para trás.

À medida que os sistemas e o processamento de dados se tornam digitalizados, a necessidade de implementar salvaguardas eficazes para proteger os dados e a privacidade do indivíduo também aumentou. As salvaguardas inadequadas para a protecção de dados, privacidade, e direitos dos utilizadores - quer sejam jurídicos, institucionais, ou tecnológicos - podem deixar os sistemas de identificação vulneráveis a violações e os dados das pessoas desprotegidas. Muitos países têm ainda um longo caminho a percorrer na construção de sistemas de identificação seguros e fiáveis: de acordo com a CNUCED, apenas 28 países (50%) em África adoptaram legislação sobre protecção de dados e privacidade e 39 (70%) têm legislação sobre cibercriminalidade em vigor[13]. Mesmo onde tais quadros existem, traduzir disposições legais em controlos institucionais, operacionais e técnicos eficazes pode ser um desafio. A partir de hoje, apenas alguns países armazenam e gerem os seus dados de acordo com as melhores práticas internacionais de protecção contra roubo ou perda não intencional de dados.[14]

Os sistemas de identificação digital enfrentam os mesmos desafios que o desenvolvimento de ecossistemas digitais; estes desafios abrangem, entre outros aspectos, questões de financiamento, uma vez que os ciclos de financiamento, principalmente os baseados em dadores que são baseados em projectos e limitados no tempo, estão desligados dos ciclos de desenvolvimento tecnológico. Além disso, o planeamento em silos e a tomada de decisões entre grupos de interessados levam a oportunidades limitadas de coordenação entre os grupos de interessados; isso limita a reutilização de soluções digitais e prejudica a sua potencial aplicabilidade entre programas e sectores. As deficiências na literacia digital, nomeadamente a falta de capacidade na liderança das TIC, e na selecção, concepção, implementação, expansão e manutenção de soluções TIC, são frequentemente um problema entre governos e profissionais de desenvolvimento. Finalmente, a ausência de financiamento para a expansão de soluções de TIC é outra grande preocupação, uma vez que normalmente podem estar disponíveis fundos para financiar as fases iniciais do ciclo de vida do desenvolvimento tecnológico, mas com financiamento limitado

[13] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx
[14] https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf

disponível para a expansão a nível nacional (Quadro de Investimento Digital do ODS, ITU/DIAL, 2019).

1.3. Outras iniciativas que promovem o reconhecimento mútuo e a interoperacionalidade das identificações digitais em África

Uma série de iniciativas existentes complementares ao Quadro já promovem o reconhecimento mútuo e a interoperacionalidade de identificação digitais em África. Estes incluem, mas não estão limitados a:

1.3.1. **Estratégia de Transformação Digital para África (2020- 2030)**

A identificação digital é reconhecida como um dos cinco temas transversais da Estratégia, que também faz dez recomendações políticas e propõe acções em dois temas para garantir a inclusão, segurança, privacidade e apropriação de dados, e apoiar a interoperacionalidade e a neutralidade. Embora estas recomendações abranjam principalmente o desenvolvimento de sistemas nacionais de identificação digital, uma recomendação apela ao estabelecimento de uma "identidade digital continental interoperacional e aberta, permitindo a validação e autenticação de indivíduos", enquanto outra recomendação solicita à CUA, à UNECA e a outros parceiros que "trabalhem em conjunto sobre normas continentais e regionais, incluindo sobre protocolos de autenticação, campos de dados mínimos, protocolos de duplicação, formatos biométricos, bem como outros formatos, regulamentos-modelo, e outras normas".

1.3.2. **Iniciativa da UNECA sobre Identidade Digital**

A Comissão Económica das Nações Unidas para África (UNECA) lançou uma iniciativa sobre Identidade Digital, Comércio e Economia Digital (DITE), actuando como Centro de Excelência, que visa a harmonização de normas relacionadas, a adopção de regulamentos para salvaguardar a segurança, o aumento dos investimentos, e o desenvolvimento da capacidade e competências dos actores principais.[15] O Centro de Excelência Digital da CEA apoia o trabalho que visa estabelecer um quadro continental africano harmonizado sobre a Identificação Digital, definindo e moldando políticas e normas para a Identificação Digital, proporcionando o desenvolvimento de capacidades para os Estados-membros, Comunidades Económicas Regionais e a União Africana. A CEA produziu um livro branco sobre um quadro para a interoperacionalidade digital através do estabelecimento de um Quadro Pan-Africano de Confiança (PATF).

1.3.3. **Aliança Fiduciária da África Inteligente (SATA)**

A África inteligente é uma iniciativa dos Chefes de Estado africanos para acelerar o desenvolvimento socioeconómico em África, alavancando as TIC. Em 2020, o Benim

[15] UNECA, DITE for Africa, vide : https://www.uneca.org/dite-africahttps://www.uneca.org/dite-africa

defendeu um projecto emblemático da África Inteligente para desenvolver o Plano de Identificação Digital, apoiado por um grupo de trabalho que incluiu o Ruanda, a Tunísia, a União Africana (UA), a União Internacional de Telecomunicações (UIT), o Banco Mundial, a Rede Omidyar, a Comissão Económica das Nações Unidas para África (UNECA), a Associação GSM, o Fórum Económico Mundial, a Gesellschaft für Internationale Zusammenarbeit (GIZ) e várias empresas privadas. Foi adoptado pelo Conselho da África Inteligente, incluindo os seus 32 Estados-membros, a UA e a UIT. O Projecto em Acção[16] propõe a SATA como uma plataforma para facilitar o reconhecimento fiável da Identificação Digital entre uma série de actores através de mecanismos federados de certificação. Prevê-se a realização de projectos-piloto da SATA entre o Benim, o Ruanda, a Tunísia e outros Estados-membros da África Inteligente. A SATA servirá como uma solução ágil e adaptável para permitir a interoperacionalidade entre vários esquemas de identidade pública e privada no continente. Mais detalhes estarão disponíveis na página sata.smartafrica.org

1.3.4. **Programa de Identificação Única para a Integração e Inclusão Regional da África Ocidental (WURI)**

O WURI[17] é um programa regional que utiliza o financiamento do Banco Mundial para aumentar o acesso a serviços nos Estados-membros participantes da CEDEAO através da construção de sistemas de identificação fundacionais acessíveis a todas as pessoas no território do país - sem consideração de nacionalidade ou estatuto legal - e que foram concebidos tendo em vista a interoperacionalidade transfronteiriça para desbloquear o acesso a serviços sociais, de saúde, financeiros e outros serviços além-fronteiras. A Costa do Marfim, a Guiné e a Comissão da CEDEAO juntaram-se na primeira fase durante o ano de 2018, e o Benim, Burkina Faso, Níger e Togo juntaram-se na segunda fase durante o ano de 2020. Os princípios fundamentais do WURI incluem registo universalmente acessível e inclusivo, minimização de dados, e credenciais básicas que são fornecidas à população a custo zero.

1.3.5. **Protocolo do Mercado Comum da CEA**

Através do artigo 8º do Protocolo, os seis Estados Parceiros da EAC comprometeram-se a trabalhar progressivamente no sentido de "...um sistema normalizado comum de emissão de documentos de identificação nacionais para os seus cidadãos".[18] Isto está fortemente ligado à realização de outros objectivos do Protocolo, incluindo a livre circulação de mercadorias (artigo 6°), pessoas (artigo 7°), mão-de-obra/trabalhadores (artigo 10°), serviços (artigo 16°), e capital (artigo 24°), bem como os direitos de

[16] Smart Africa, Blueprint | Smart Africa Alliance – Digital Identity, Outubro de 2020, ver: https://smartafrica.org/knowledge/digital-id/
[17] Banco Mundial. Programa de Identificação Única para a Integração e Inclusão Regional da África Ocidental (WURI). https://projects.worldbank.org/en/projects-operations/project-detail/P161329 ; https://projects.worldbank.org/en/projects-operations/project-detail/P169594
[18] https://www.eac.int/images/doc_image_png_NnlwzXikEvuHdytNzkKNVDMScreen%20Shot%202017-06-20%20at%20153445.png

estabelecimento e residência (artigos 13° e 14°, respectivamente). No entanto, os sistemas nacionais de identificação encontram-se em diferentes fases de desenvolvimento. Todavia, no espírito da geometria variável e como iniciativa dos Projectos de Integração de Corredores Nacionais (NCIP), Quénia, Ruanda e Uganda começaram em 2014 a reconhecer os cartões de identidade nacionais respectivos como documentos de viagem válidos. No âmbito da NCIP, tem havido discussões no sentido de se desenvolverem casos de utilização adicional, tais como serviços electrónicos, embora estes ainda não se tenham materializado. Em 2018, o Banco Mundial e o secretariado da EAC realizaram um estudo sobre as opções para o reconhecimento mútuo de identificação nacionais (DNIs) na CEA que propôs quatro marcos.

1.4. Soberania Digital

Com 55 nações soberanas, África tem, portanto, 55 jurisdições legais a serem consideradas. A soberania digital descreve um espectro de diferentes conceitos técnicos e regulamentares, desde a localização física dos servidores, a construção de cabos submarinos, até às leis e práticas relativas à protecção de dados e à tributação dos mercados de dados, que permitem aos Estados tomar as suas próprias decisões sobre as escolhas tecnológicas e a sua regulamentação.

A fim de garantir a soberania dos dados**,** os Estados-membros da UA são encorajados a:

1. criar sistemas seguros de armazenamento de dados pessoais (incluindo dados sensíveis) através da concepção e criação de centros de dados nacionais que devem prever o controlo de dados pelo Estado e incluir pelo menos espaço de armazenamento e processamento dedicado exclusivamente a dados pessoais e sensíveis. Será necessário estabelecer as salvaguardas necessárias (técnicas, em particular) para assegurar que os dados utilizados no intercâmbio transfronteiriço de informações não incluam de forma alguma dados pessoais ou sensíveis cujo tratamento ou armazenamento possa colocar em risco os direitos dos indivíduos ou a soberania dos Estados membros da UA.

2. criar capacidade e infra-estruturas para o desenvolvimento de talentos e conjuntos de competências africanas para enfrentar os novos desafios e reforçar a soberania digital. Espera-se que os Estados-membros assumam a liderança no avanço das competências (incluindo competências de ciber-resiliência) de todos os cidadãos e residentes, e devem capacitar as pessoas a terem controlo sobre os seus dados pessoais.

3. estabelecer parcerias baseadas no respeito mútuo, em situações vantajosas para ambas as partes sem comprometer a soberania e a propriedade nacional e evitar interferências estrangeiras que possam afectar negativamente a

segurança nacional, os interesses económicos e a evolução digital dos Estados-membros da UA.

O Quadro será orientado pelas regras soberanas representadas pela autoridade ou autoridades de registo e emissão de identidade de cada Estado-membro da UA, e a estrutura de governação, incluindo a criação de uma instituição de coordenação continental de supervisão, será aprovada pelos Estados-membros da UA. Além disso, os mecanismos de responsabilização, incluindo o tratamento de responsabilidades em caso de má conduta, serão definidos e aprovados pelos Estados-membros da UA. O desenvolvimento da confiança continental entre Estados soberanos com esquemas de identificação digital divergentes é uma tarefa complexa mas exequível que requer a colaboração de múltiplas partes interessadas. Para alcançar a interoperacionalidade para o intercâmbio de informações de identidade jurídica nos respectivos países africanos, as semelhanças entre as regras e normas nacionais existentes devem ser reconhecidas, com base num conjunto mínimo de critérios que permitam tanto a soberania local como a confiança suficiente na abordagem um do outro.

Para este efeito, os Estados-membros da UA necessitam de reforçar e melhorar os seus quadros jurídicos as suas capacidades de execução, em particular as capacidades das autoridades de protecção de dados no controlo das transferências transfronteiriças de dados e na aplicação das leis e regulamentos relevantes em casos de violação ou utilização indevida.

O quadro proposto abraçará as tecnologias mais avançadas e respeitará as legislações e regulamentos dos países. Os governos não devem ser obrigados a utilizar tecnologias específicas. A utilização de normas e padrões abertos deve garantir uma grande diversidade de escolhas tecnológicas por parte dos Estados, facilitando ao mesmo tempo a apropriação e a interoperabilidade pelos países.

2. INTRODUÇÃO

Em 2020, os Estados membros da União Africana adoptaram a Estratégia de Transformação Digital (ETED) para África (2020-2030) com a visão de:

> *Uma sociedade e economia digital integrada e inclusiva em África que melhore a qualidade de vida dos cidadãos africanos, reforce o sector económico existente, permita a sua diversificação e desenvolvimento, e assegure a apropriação continental com África como produtor e não apenas como consumidor na economia global.*

A concretização desta ambição - bem como da ZCLCA - depende do desenvolvimento de sistemas de identificação digital inclusivos e fiáveis que permitam que todos os cidadãos africanos provem e verifiquem a sua identidade legal de forma fiável e segura ao efectuarem transacções presenciais e virtuais, e permitir aos prestadores de serviços dos sectores público e privado reconhecerem as credenciais de identidade, independentemente do local de origem em África onde tenham sido emitidas. É importante que os sistemas de identificação digital fundacionais sejam concebidos para empoderar as pessoas, especialmente as populações desfavorecidas e marginalizadas. Isto permitirá a todos participar de forma significativa na economia e sociedade digital, desbloquear o acesso aos serviços dentro dos países e além-fronteiras, promover o comércio como parte da ZCLCA, aumentar a confiança na sociedade e economia digitais, e reduzir a fraude e os custos de fazer negócios.

É importante notar que os sistemas de identificação digital fundacionais podem também sustentar o desenvolvimento de "pacotes digitais" mais amplos[19] com plataformas de pagamento digital e de partilha de dados fiáveis para criar oportunidades de inovação e uma vasta gama de transacções sem presença, sem papel e sem numerário em todo o continente. Contudo, isto também exige que os riscos relacionados com a exclusão, protecção de dados, segurança cibernética e tecnologia e o "bloqueio" de fornecedores sejam atenuados de forma abrangente. É por estas razões que a identificação digital é um dos cinco temas transversais da ETED, conferindo o mandato e o âmbito deste Quadro.

2.1. Visão, objectivos e casos de uso indicativo

A visão do Quadro de interoperacionalidade da UA para a Identificação Jurídica Digital é que todos os cidadãos africanos possam aceder com facilidade e segurança aos serviços de que necessitam, quando deles necessitam, tanto dos fornecedores do sector público como do privado, o que incentivará uma participação inclusiva e significativa na economia e sociedade digital em geral e permitirá que os serviços funcionem com maior confiança e certeza.

Para este efeito, o Quadro define requisitos comuns, normas mínimas, regras, mecanismo de governação e um alinhamento entre os quadros jurídicos e os objectivos a atingir:

1. Permitir a todos os cidadãos africanos **autenticar e verificar a sua identidade legal tanto fora do sistema como virtualmente** para aceder aos serviços dos sectores público e privado em todos os Estados-membros da UA participantes;

[19] No contexto das tecnologias digitais, um "pacote" é uma colecção de componentes ou infra-estruturas de software independentes que trabalham em conjunto para apoiar a execução de um caso de utilização.

2. Empoderar a todos os cidadãos africanos com **controlo sobre os seus dados pessoais**, incluindo a capacidade de revelar selectivamente apenas os atributos que são necessários para uma determinada transacção;
3. Reforçar a confiança e a interoperacionalidade entre os sistemas de identificação fundacional dos Estados-membros da UA.

O Quadro não exige a criação de um sistema de identificação digital continental unificado, mas fornece uma base para a interoperacionalidade entre os sistemas de identificação digital existentes nos Estados-membros da UA, que tem em consideração a soberania digital dos Estados-membros da UA, as diferenças na implantação da infra-estrutura digital, a disponibilidade de políticas e regulamentos associados, os diferentes níveis de sistemas de identificação e a vulnerabilidade das populações durante e após a implementação dos sistemas de identificação digital.
É primordial que este Quadro seja desenvolvido de acordo com as melhores práticas e normas internacionais[20] que visam proteger os dados pessoais, manter a segurança cibernética e salvaguardar os direitos das pessoas. Com a adopção da Convenção de Malabo sobre Segurança Cibernética e Protecção de Dados Pessoais e o trabalho em curso para desenvolver um quadro de política de dados continental[21], a União Africana deu um passo importante para estabelecer um ambiente digital credível para as transacções electrónicas através da adopção de um conjunto comum de regras que regem a transferência transfronteiriça de dados pessoais em todo o continente e o alinhamento dos quadros nacionais de protecção de dados e de segurança cibernética.

Um quadro continental pode facilitar o **acesso a serviços em todos os países participantes, permitindo às pessoas e empresas** verificar as credenciais e outros factos sem revelar dados pessoais. Isto inclui a possibilidade de autenticar a sua identidade ao aceder a serviços electrónicos (por exemplo, serviços governamentais) noutro país com a sua identificação digital sem a necessidade de se inscreverem nas soluções de identidade fundacional local reconhecidas pelos prestadores de serviços estrangeiros. O reconhecimento mútuo e a interoperacionalidade da identificação digital também facilitam a partilha e o consentimento de credenciais verificáveis e de dados de confiança quando se solicita serviços onde a lei exige tal verificação (por exemplo, prova de seguro, estatuto de vacinação para qualificação), permitindo às pessoas poupar tempo e reduzir a burocracia.

Pode igualmente **reforçar a integridade e acessibilidade dos pagamentos e serviços financeiros transfronteiriços em África, e criar oportunidades de**

[20] Isto inclui, entre outros aspectos, a UIT-T X.1058 | ISO/IEC 29151, os Princípios e recomendações da ONU para sistemas de estatísticas vitais, os Dez Princípios sobre Identificação para o Desenvolvimento Sustentável, normas internacionais sobre protecção de dados, o Regulamento Geral Europeu sobre Protecção de Dados e outros.
[21] União Africana, Convenção sobre Segurança Cibernética e Protecção de Dados Pessoais, vide: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

inovação. Sistemas de identificação fracos e não fiáveis, a ausência de harmonização das regras criam riscos de branqueamento de capitais/ financiamento do terrorismo (AML/CFT)[22] que introduzem barreiras às trocas transfronteiriças, aumentam os custos dos serviços (por exemplo, remessas) e dificultam a inovação. A identificação digital pode facilitar a identificação e verificação do cliente a bordo, apoiar os processos "Conheça o seu Cliente (KYC)" e ajudar na monitorização das transacções com o objectivo de detectar e comunicar transacções suspeitas. O reconhecimento mútuo não só facilitará aos migrantes o envio de dinheiro para casa, facilitando a verificação de KYC e o encargo da autenticação, como também ajudará a baixar os custos, ajudando África a aproximar-se da meta do ODS (10.c) de três por cento até 2030.

Um quadro continental pode igualmente **reforçar o comércio e o comércio electrónico, aumentando a confiança nas transacções comerciais electrónicas e facilitando a realização de negócios e o comércio em todo o continente africano.** Em 2020, o comércio intra-africano representava aproximadamente 16.6% do PIB de África.[23] A ZCLCA foi lançada em 2019 para desbloquear novas oportunidades de comércio e comércio electrónico até 2030. O reconhecimento transfronteiriço da identificação digital pode ajudar a reforçar os controlos de identidade de compradores e vendedores, especialmente no caso de bens restritos vendidos electronicamente. Pode igualmente permitir assinaturas electrónicas para transacções 100% electrónicas, sem papel, que permitem às empresas e clientes poupar tempo e aumentar a segurança, reduzindo os riscos de fraude de identidade. Também simplifica a realização de negócios além-fronteiras, permitindo às empresas gerir digitalmente a sua interacção com o governo, por exemplo declarando impostos, participando em procedimentos de aquisição, solicitando número de IVA e aplicando autorizações.

2.2. Âmbito

Para atingir estes objectivos, o Quadro definirá:

- o **tipo de informação/dados** que podem ser partilhados sob a forma de um conjunto mínimo de dados para informação de identidade fundacional;[24]
- a **forma de provar quem emitiu os dados** e que se pode confiar nos mesmos;
    - criar um processo de comunicação de fontes fiáveis e autorizadas de

[22] Os riscos de AML/CFT referem-se aos riscos de branqueamento de capitais e de combate ao financiamento do terrorismo. O GAFI recomenda aos governos que desenvolvam uma abordagem integrada de múltiplas partes interessadas para compreender as oportunidades e riscos relevantes para a identificação digital e desenvolver regulamentos e orientações para mitigar esses riscos.
[23] CNUCED , Relatório sobre o Desenvolvimento Económico em África de 2019: Made in Africa: Regras de origem para um maior comércio intra-africano, vide: https://unctad.org/press-material/facts-figures-0
[24] Embora o âmbito deste documento incida nos dados de identidade, o quadro de confiança proposto pode ser alargado pelos Estados-membros da UA para representar outras provas e realizações, tais como diplomas, qualificações profissionais, etc...

dados de identidade em cada Estado-membro da UA;
- determinar como verificar a autenticidade da reivindicação digital;

- normas e processos que descrevem a **forma como os dados são partilhados** pelos utilizadores e verificados por outros em ambiente fora do sistema e de forma electrónica.

O presente documento define as bases de um quadro de confiança e interoperacionalidade para a identificação jurídica digital em todo o continente africano. Definirá os requisitos mínimos necessários para assegurar a interoperacionalidade entre os actuais e futuros sistemas de identificação digital. O Quadro não define um sistema unificado de Identificação Digital para África e não aborda os acordos comerciais e de responsabilidade entre os Estados-membros participantes.

Muitos países africanos já possuem sistemas de identificação digital bem encaminhados e alguns introduziram capacidades de autenticação digital. **O Quadro fornece requisitos comuns para a comunicação de dados e processos de identidade fundacional que seriam interoperacionais e aceites noutros Estados-membros africanos, enquanto os Estados-membros mantêm o pleno controlo e escolha para a concepção dos seus sistemas nacionais.**

O Quadro complementará e desenvolverá, em vez de duplicar, as actividades associadas ao Protocolo ao Tratado que estabelece a Comunidade Económica Africana Relativa à Livre Circulação de Pessoas, Direito de Residência e Direito de Estabelecimento, e à Conferência dos Ministros Africanos Responsáveis pelo Registo Civil e o Programa Africano para a Melhoria Acelerada da CRVS (APAI-CRVS). A implementação do Quadro deve ser estreitamente coordenada com esta e outras iniciativas relevantes, tais como explorar a migração como um caso de utilização adicional para a identificação digital no momento apropriado e assegurar que a cobertura e a qualidade dos sistemas de CRVS sejam melhoradas como um contributo importante para os sistemas de identificação digital fundacional.

2.3. Quadro de Confiança, Privacidade de Dados, Interoperacionalidade e Normas

Os sistemas de identidade devem fomentar a confiança entre as várias partes participantes, assegurando que os direitos legais tanto dos utilizadores individuais como das agências operacionais sejam respeitados, e que a utilização ética dos sistemas de identidade seja promovida. **Para assegurar esta confiança é necessário definir um conjunto de regras que todas as partes subscrevem e observam**, um Quadro de Confiança.

Enquanto a tecnologia actua como um facilitador fundamental, o Quadro de Confiança também incide no processo e procedimento. Um quadro de confiança robusto deve definir claramente o:

- **Requisitos comerciais** (por exemplo, âmbito, serviços prestados, requisitos de participação);
- **Requisitos técnicos** (por exemplo, formatos de dados, interfaces, normas);
- **Requisitos operacionais** (por exemplo, como funcionam a prova e autenticação de identidade, apoio, comunicações); e
- **Requisitos legais** (por exemplo, níveis de serviço, responsabilidade, resolução de litígios, reconhecimento legal das transacções electrónicas dentro dos países) para o sistema de identidade.

O Quadro baseia-se **na interoperabilidade**. Para facilitar a interoperacionalidade, uma entidade deve poder confiar noutra entidade com base não só na integridade dos processos técnicos (por exemplo, prova criptográfica, etc.), mas também na proveniência dos dados a partilhar (por exemplo, os processos para a sua recolha e para a atribuição de um determinado registo a um indivíduo).

A interoperacionalidade não exige que os sistemas de identificação fundacionais sejam uniformes, apenas que certas normas comuns e abertas sejam seguidas. Ao abrigo do Quadro, cada país participante pode criar sistemas de identificação fundacionais adaptados às necessidades, tradições e legislação locais, desde que sejam seguidas certas normas que permitam a interoperacionalidade. **Norma**s Abertas estabelecem protocolos de intercâmbio universalmente compreendidos e consistentes, regimes de teste, medidas de qualidade e boas práticas relativamente à captura, armazenamento, transmissão e utilização de dados de identidade legal, bem como o formato e características das credenciais de identidade legal e protocolos de autenticação.
Ao considerar a interoperacionalidade das credenciais de identidade jurídica e autenticação em todo o continente, será importante considerar normas abertas para as reivindicações de identidade, a forma como são emitidas e a forma como a confiança é comunicada entre as entidades envolvidas no Quadro de Confiança. Estas reivindicações, que constituirão a **base da identificação digital legal**, terão frequentemente origem em fontes autorizadas, tais como agências governamentais. Deve ser igualmente definido um mecanismo de autenticação que permita aos detentores de identificação digital legal partilhar adequadamente estas reivindicações com os prestadores de serviços, assegurando que a divulgação de dados seja - binária e que quaisquer metadados sejam ocultados, e que a privacidade e os direitos dos indivíduos sejam protegidos a todo o momento.
Este quadro definirá a **forma como a confiança pode ser estabelecida nestas reivindicações verificáveis, e como funcionam os elementos e normas de governação dos dados.** A implementação técnica da solução pode ser impulsionada pelo mercado que será capaz de alavancar o quadro de confiança para desenvolver

soluções inovadoras de identificação digital fundacional. O Quadro coloca a privacidade, auditoria e protecção de dados no centro e estabelece um procedimento transparente a ser aplicável a todos os envolvidos. As Partes confiantes sobre a forma como os dados são solicitados, recolhidos, transmitidos e armazenados e segue normas bem aceites sobre o procedimento de partilha de informações/dados. A importância da atribuição de símbolos na redução das oportunidades de recolha de dados, clonagem e fraude, através da apresentação ao titular da identificação, da funcionalidade de emissão de identificações virtuais, a fim de proteger as próprias identificações reais, é um aspecto adicional que será aprofundado para reforçar a privacidade dos dados a nível nacional/continental.

3. O QUADRO

O Quadro de Interoperacionalidade da UA para a Identificação Digital propõe definir a nível continental uma abordagem harmonizada para a partilha de reivindicações de identificação digital[25] emitidas por autoridades de confiança com fornecedores de serviços, a fim de provar a sua identidade legal num ambiente virtual e não virtual. Consistirá em acordar numa **norma comum para representar as provas existentes de identidade jurídica emitidas pelos Estados-membros da UA num formato digital**.[26] A autenticidade de tais credenciais[27] seria capaz de ser verificada a fim de garantir um alto nível de confiança e segurança.
Não há restrições impostas aos sistemas nacionais de identificação fundacional como funcionam ou que tipos de credenciais utilizam para autenticar indivíduos; cada país é soberano a este respeito. A intenção do quadro é criar condições para a interoperacionalidade à escala continental com base nos sistemas existentes onde eles existem e em vez de restringir a sua utilização alargando o seu alcance.

As credenciais de identidade jurídica digital interoperacionais (IDC-ID) emitidas em conformidade com o Quadro da UA assumirão a forma de uma reivindicação verificável que será complementar aos sistemas nacionais de identificação fundacional existentes e aos projectos de cooperação regional, sem substituir os sistemas nacionais de identificação digital dos Estados-membros da UA. Os Estados-membros da UA permanecem livres para seleccionar a forma como querem emitir esta credencial digital. Pode ser armazenado num formato puramente digital numa aplicação baseada em telefones inteligentes, um servidor baseado em nuvem, um cartão inteligente ou uma ligação à representação digital pode ser estabelecida

[25] As reivindicações são uma colecção de atributos sobre uma pessoa em causa: por exemplo, nome de família, dados de nascimento
[26] O quadro actual centra-se na definição de reivindicações verificáveis para provar dados de identificação, mas poderia ser utilizado para partilhar reivindicações verificáveis sobre realizações académicas, qualificações profissionais, etc...
[27] Uma credencial é composta por uma reivindicação de identidade, metadados sobre o emissor e uma prova de autenticidade que é normalmente uma assinatura digital.

usando um código de barras de uma ou duas dimensões num documento em papel (impresso em papel, cartão plástico).

A Estrutura será baseada no desenvolvimento de sistemas de identificação interoperacionais, inclusivos e de confiança, uma vez que estes constituem a espinha dorsal de fontes de dados fiáveis sobre a identidade legal das pessoas, permitindo assim ao IDC-ID alcançar níveis mais elevados de garantia. Os Estados-membros da UA são, portanto, incentivados a reforçar os seus sistemas de identificação, bem como os *Princípios de Identificação para o Desenvolvimento Sustentável.* Podem ser consideradas soluções alternativas para obter uma IDC-ID para pessoas que estão actualmente excluídas de um sistema de identificação.
As normas para uma identificação digital legal interoperacional poderiam ser utilizadas a nível nacional ou apoiar casos de utilização transfronteiriça. Por exemplo, a norma poderia ser adoptada para:

- representam dados de identificação digital fundacionais a nível nacional sobre credenciais de identidade digital recentemente emitidas ou actualizadas; ou,
- representam dados de identificação digital fundacionais a nível continental ou das CER;
- emitidos separadamente em complemento dos sistemas de identificação digital preexistentes.

O elemento interoperacionalidade, confiança e inclusão definido como parte deste quadro constitui uma plataforma de lançamento para um quadro continental mais abrangente e uma infra-estrutura para a identificação e autenticação digital no continente.

3.1. Princípios Orientadores

Os seguintes princípios orientarão a implementação da interoperacionalidade transfronteiriça do quadro:

1. Transparência na governação e no funcionamento
2. Facilmente acessível, financeiramente e operacionalmente sustentável e amplamente utilizável,
3. Promover o respeito e defender os direitos humanos e a liberdade [28]
4. Garanta a integridade técnica, incluindo identidade exclusiva, segura, escalável e precisa
5. Garantir a soberania dos Estados-membros. garantir a soberania dos dados, nomeadamente os dados de identificação digital, pertence e permanece sob o controlo de África:
6. Ser interoperacional entre os Estados-membros da UA

[28] Segundo a Carta Africana (Banjul) sobre os Direitos Humanos e dos Povos (Adoptada a 27 de Junho de 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entrou em vigor a 21 de Outubro de 1986)

7. Utilizar normas abertas[29] e evitar o bloqueio de fornecedores e tecnologias
8. Protegem a privacidade e permitem que as pessoas controlem os seus dados pessoais, incluindo a proporcionalidade dos dados através da concepção do sistema
9. Salvaguardar a privacidade, segurança e direitos dos dados através de um quadro jurídico e regulamentar abrangente.
10. Estabelecer mandatos institucionais claros e responsabilização

Considerando que o Quadro depende de fontes autorizadas, tais como sistemas de identificação legal, a qualidade e cobertura destes sistemas, tem portanto um impacto na sua implementação. A exclusão destes sistemas e outros desafios como a fraca segurança, por exemplo, conduzirá ao mesmo em termos da capacidade de emitir e utilizar correctamente as credenciais.

Por conseguinte, os Estados-membros da UA devem cumprir as suas obrigações de garantir que todas as pessoas presentes no seu território tenham acesso à identificação legal, em conformidade com a Convenção sobre os Direitos da Criança e outros instrumentos jurídicos internacionais e regionais. Além disso, são também fortemente incentivados a aderir às normas e princípios internacionais relevantes existentes[3031] e a assegurar que as fontes autorizadas, e especialmente os seus sistemas de identificação legal, sejam inclusivas, protectoras dos dados e direitos das pessoas, e concebidas para apoiar a integração económica e social continental.

3.2. O Modelo

O Quadro irá propor uma implementação em três fases:

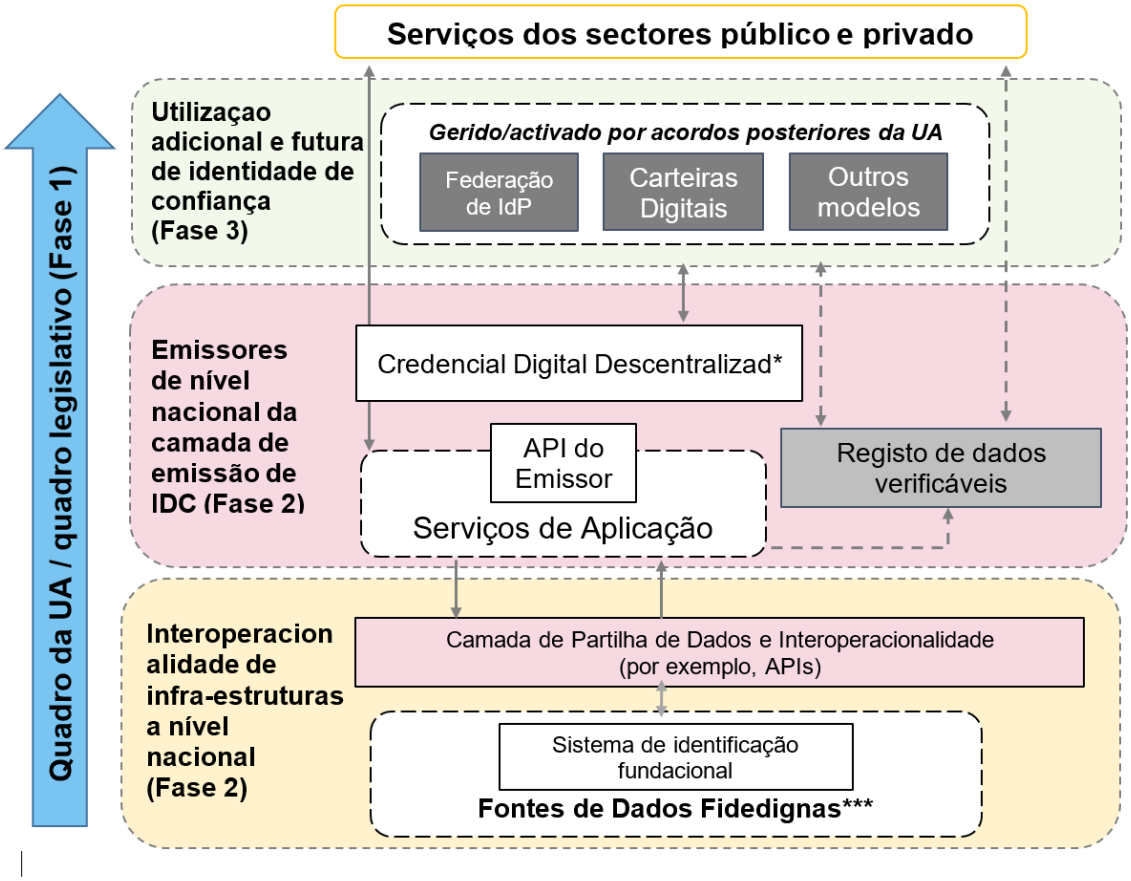
1. Aprovação do quadro da UA e apoio ao quadro legislativo favorável;
2. Implementação da estrutura e adopção de especificações técnicas para o IDC-ID;
3. A ampliação da estrutura para fornecer uma infra-estrutura que permita casos de utilização mais avançada, como a autenticação remota.

Figura 1 – Abordagem de implementação faseada do Quadro

[29] **Normas Abertas** são normas disponibilizadas ao público em geral e são desenvolvidas (ou aprovadas) e mantidas através de um processo de colaboração e de consenso. As “Normas Abertas” facilitam a interoperacionalidade e o intercâmbio de dados entre diferentes produtos ou serviços e destinam-se a uma adopção generalizada (adoptadas a partir da UIT-T).

[30] Isto inclui, entre outros aspectos, a convenção de Budapeste sobre a criminalidade cibernética, IEC, ISO, Princípios e recomendações da UIT-T da ONU para sistemas de estatísticas vitais, normas internacionais sobre protecção de dados (tais como o Regulamento Geral Europeu para a Protecção de Dados e a Convenção 108+ do Conselho da Europa), normas globais e regionais e quadros de confiança para a identificação.

[31] Tais como os Dez Princípios de Identificação para o Desenvolvimento Sustentável, que foram endossados por 30 organizações internacionais e regionais, incluindo instituições africanas como a UNECA, o BAD e a África Inteligente, bem como adotados por vários países africanos, ver: https://id4d.worldbank.org/principles, e os Princípios sobre Desenvolvimento Digital, que foram endossados por mais de 200 organizações, ver: https://digitalprinciples.org/.



O IDC-ID deve assegurar que a **autoridade emissora não tenha conhecimento dos serviços a que os indivíduos têm acesso com a sua identificação digital**, mas que a autenticidade das credenciais de identidade possa ser verificada. Isto proporciona salvaguardas em termos de protecção de dados e privacidade e mais controlo para o indivíduo sobre a forma como os seus dados são utilizados.

** Os pormenores de implementação da fase 2 serão discutidos mais aprofundadamente com os Estados-membros da UA*
** Os Estados-membros decidirão que fontes de dados fiáveis implicam os seus sistemas de Identificação Fundacional

A camada de infra-estrutura permitirá casos de utilização mais avançada e consistirá em credenciais de identidade vinculativas emitidas no formato IDC-ID para os indivíduos reais. Existem várias opções técnicas à disposição dos Estados-membros da UA para implementar esta plataforma, que poderia ser composta por uma federação de fornecedores de identidade que forneçam mecanismos de autenticação aos detentores do IDC-ID ou o desenvolvimento de soluções de carteiras de identificação digital ou quaisquer outros modelos que permitam a interoperacionalidade. Cada uma destas implementações pode oferecer **uma abordagem de minimização de dados e serviços de divulgação selectiva** para casos de uso específico, por exemplo, partilhar apenas os pontos de dados relevantes

de um cartão de identificação e relatório de crédito para obter um empréstimo, procurar benefícios sociais ou de saúde, obter pensão, candidatar-se a bolsas de estudo ou tornar anónimo o conjunto mínimo de dados do IDC-ID (nome, data de nascimento) numa prova de maioridade (+18 anos ou +21 anos ou uma resposta de sim/não).

3.2.1. **Componentes da Arquitectura**

As fontes de dados fiáveis devem cumprir as normas estabelecidas pela Estrutura da UA para a qualidade e integridade dos dados. Em muitos casos, isto seria cumprido por um sistema de identificação fundacional (cujas fontes de dados fiáveis serão decididas pelos Estados-membros) que pode fornecer uma prova de identidade jurídica.

A Figura 1 mostra a extensão do acesso aos sistemas nacionais existentes e fontes de dados de confiança através de uma camada de Partilha de Dados e Interoperacionalidade baseada em normas e protocolos que permitem a emissão de IDC de confiança. Fornecedores de serviços para verificar e recuperar dados de identidade legal ao criar credenciais de identificação digital fundacionais.

A camada de emissão da IDC representa a emissão padronizada de Credenciais de IDC com base num sistema de identificação de nível fundacional/nacional fonte de dados de confiança. Cada Emissor de Credenciais (pelo menos um por cada Estado-membro participante) terá uma série de funções essenciais (não limitadas às seguintes):

- Uma API de Emissor que permite às carteiras e outros sistemas solicitar e recuperar credenciais
- Um Registo de Dados Verificável que permite a verificação dos identificadores e a verificação da revogação das credenciais.
- Gestão de Criptografia Importante
- Visibilidade e Auditoria da utilização de credenciais para o Titular de uma credencial da IDC
- Fornecer Metadados de Credenciais juntamente com cada credencial emitida para descrever a qualidade, proveniência e nível de confiança associado à credencial emitida

3.2.2. **Nível nacional e requisitos de interoperacionalidade**

Não há nenhum requisito para que os sistemas de identificação existentes a nível nacional sejam reequipados para alcançar a interoperacionalidade a nível continental. Em vez disso, serão adoptadas normas para a interoperacionalidade dos dados, interoperacionalidade técnica através de APIs e protocolos, e representação técnica das credenciais. A emissão de credenciais, e a sua criação, é logicamente separada dos sistemas nacionais existentes, mas estaria sob o controlo de agências nacionalmente responsáveis.

A confiança técnica, sustentada por criptografia avançada, pode não exigir uma PKI continental ou outra infra-estrutura super-nacional, mas, em vez disso, resultaria da preferência e/ou capacidade dos Estados-membros da UA utilizando quer a PKI nacional (quando utilizada) quer alternativas. Cada Estado-membro da UA continuará a exercer a soberania nacional na concepção dos sistemas de identificação nacionais, incluindo a forma como esses sistemas funcionam em conjunto com o quadro da UA.

3.2.3. **Normas para a participação de fontes de dados fiáveis**

Serão estabelecidas normas no âmbito da estrutura da UA para a qualidade, segurança, fiabilidade, e nível mínimo de garantia associado a cada fonte de dados de confiança. Os sistemas dos Estados-membros devem fornecer provas de que alcançaram os requisitos mínimos de participação antes de poderem participar no Quadro da UA e emitir credenciais conformes à IDC. A natureza destas normas será determinada por acordo dos Estados-membros da UA.

3.3. Processo de confiança - o quadro fiduciário

O quadro de confiança deve descrever regras claras para a participação de entidades (por exemplo, emitentes, titulares e verificadores de identidade), o funcionamento do quadro, e os requisitos técnicos para a interoperacionalidade das credenciais de confiança.
Isto permitirá a todas as entidades confiar nas credenciais partilhadas pelos titulares de identidade com base no acordo fiduciário estabelecido pela autoridade emissora (para a credencial) e nos processos que cada entidade concordou em aderir ao abrigo do quadro fiduciário.

Prevê-se que as seguintes secções fundamentais sejam redigidas pelos Estados-membros como parte do quadro de confiança.

3.3.1. **Papéis e Responsabilidades**

Uma definição clara de cada entidade (por exemplo, um emissor de credenciais), e as responsabilidades que tem para manter a confiança, tais como a gestão segura e protegida de dados e serviços, e a comunicação de incidentes.

Os papéis fundamentais que se espera venham a ser incluídos no quadro de confiança seriam:

- As **autoridades de confiança** são fontes fidedignas de dados para a prova legal da identidade, tal como endossada pelos Estados-membros da UA.
- Os **emissores** são entidades responsáveis pela emissão da prova de identidade legal no formato digital normalizado ao abrigo do Quadro de Referência para o titular. As autoridades fidedignas podem emitir elas próprias as credenciais ou mandatar outra entidade com um conjunto de competências

mais adequado (por exemplo, agência TIC, sector privado).

- O **titular** do IDC-ID é o indivíduo que possui uma ou mais credenciais digitais. O titular pode ser mas nem sempre o sujeito dos atributos de identificação partilhados através de IDC.
- O **verificador** é uma parte de confiança (por exemplo, fornecedor de serviços públicos ou privados) que pretende verificar a reivindicação de identidade de um determinado sujeito.
- **Os fornecedores de identidade, fornecedores de credenciais e fornecedores de carteira digital** podem contribuir ainda mais para o ecossistema, fornecendo um autenticador para vincular a identidade do titular às credenciais e, portanto, permitir casos de utilização mais avançada que exijam autenticação remota.
- Poderá ser necessário um **organismo de controlo independente** a ser criado pelos Estados-membros para assegurar que as entidades participantes continuem a cumprir as regras estabelecidas pelo quadro fiduciário e definir as ferramentas e tecnologias mínimas necessárias para o cumprimento. O Organismo de Supervisão deve também ser incumbido da tarefa de aumentar a sensibilização para as competências de resiliência cibernética em todo o continente, a fim de assegurar a sustentabilidade do quadro.

3.3.2. **Regras de Participação**

As regras de participação podem incluir requisitos mínimos legais, operacionais, ou organizacionais exigidos a uma entidade de confiança autorizada que preste um serviço no âmbito do quadro fiduciário. Por exemplo, um Emissor pode ser obrigado a ter um acordo oficial para operar (de uma fonte autorizada / agência governamental).

Os serviços que aceitam o IDC-ID podem ser solicitados a confirmar a sua conformidade com os requisitos básicos de protecção de dados, privacidade e reparação (para titulares de identidade).

Pode também ser necessário um memorando de entendimento para assegurar que todas as entidades operacionais concordam com os termos do quadro de confiança.

3.3.3. **Governação**

Os mecanismos de governação a serem aprovados pelos Estados-membros da UA deverão estabelecer e manter as regras do quadro de confiança, aprovar alterações aos requisitos de interoperacionalidade, e delegar a responsabilidade pela elaboração/desenvolvimento de alterações ao quadro nos subgrupos de governação, conforme necessário.

Poderá ser necessário um organismo de controlo independente a ser criado pelos Estados-membros da UA para assegurar que as entidades participantes continuem a cumprir as regras estabelecidas pelo quadro fiduciário. Este organismo deverá

igualmente ser responsável por assegurar que todas as partes satisfaçam o cumprimento formal das normas e, caso se desviem, sejam auditadas ou levadas a prestar contas, conforme considerado necessário, por exemplo, em caso de violação de dados.

A protecção dos indivíduos deve ser primordial. O Organismo de Controlo deve ter poderes para receber e agir em caso de queixas dos Titulares da IDC-ID afectados por más práticas, violação de dados, fraude de identidade, ou outros incidentes relacionados com a identidade digital. Deve igualmente ser o ponto focal dos mecanismos de reparação, mesmo que se trate apenas de um papel de coordenação e deve actuar como um defensor dos indivíduos e dos seus direitos.

3.3.4. **Requisitos de Interoperacionalidade**

3.3.4.1. **Níveis de Garantia**

Um meio de comunicar o nível de confiança de uma credencial apresentada por um Titular a um Verificador. O Quadro deve definir as condições pelas quais cada nível pode ser alcançado com base na verificação da identidade por uma fonte autorizada, o processo de emissão, e os meios de detenção e apresentação de uma credencial.

3.3.4.2. **Conjunto de dados mínimos**

A quantidade mínima de dados relativos à identidade de um Titular, tal como consta de uma credencial de identidade, deve ser adequada para a identificação do indivíduo na maioria das transacções comuns, respeitando simultaneamente a necessidade de minimização de dados. Os atributos contidos no conjunto mínimo de dados podem ser fornecidos por diferentes entidades de confiança.

O órgão dirigente tem a liberdade de definir como os créditos adicionais (conjuntos de dados) podem ser incluídos opcionalmente no quadro fiduciário. Qualquer emissão de credenciais correspondentes deve estar sujeita às mesmas condições e regras que os emissores de credenciais de identidade fundacional. Requisitos Técnicos

3.3.4.3. **Segurança**

Devem ser definidos requisitos de segurança de base para cada entidade que presta um serviço como parte da infra-estrutura de identidade.

3.3.4.4. **Prova criptográfica**

As credenciais serão verificadas através da inclusão de uma assinatura digital criada pela autoridade emissora. A verificação da validade da assinatura actua como prova criptográfica de que o crédito feito pelo Titular que apresenta a credencial pode ser confiável. A fim de verificar uma chave pública de assinatura digital será necessária. A chave pública pode ser fornecida através de um método descentralizado ou centralizado a ser determinado como parte do quadro de confiança e dos seus requisitos técnicos.

3.3.4.5. Formato de credencial

As especificações técnicas para a criação e transmissão de credenciais devem ser definidas com base nas normas existentes, tais como as Credenciais Verificáveis W3C, quando aplicável.

- A **Credencial Digital Interoperacional para Identificação (IDC-ID)** é um conjunto de reivindicações de identidade legal (por exemplo, atributos) e relação feita por um emissor que pode ser verificada criptograficamente. Mais especificamente, inclui:

    - Metadados de credenciais sobre o tipo de credencial emitida, data de emissão, nome do emitente;
    - Informação sobre o objecto da reivindicação e a verdadeira reivindicação de identidade jurídica (por exemplo, data de nascimento).
    - Prova de autenticidade que é normalmente uma assinatura digital.

O titular de IDC-ID é capaz de gerar apresentações verificáveis de um ou mais IDC-ID da forma que a autenticidade da reclamação ainda pode ser verificada (por exemplo, divulgação selectiva)

3.4. Opções de autenticação em potencial

Várias abordagens arquitectónicas podem ser adoptadas para permitir que o titular de IDC-ID seja autenticado a um determinado nível de garantia. Todas as opções seguintes podem coexistir e ser implementadas a diferentes níveis de cooperação (por exemplo, entre actores sectoriais específicos ou a nível das CER).
Dependendo da disponibilidade de outras tecnologias com práticas de implementação comprovadas, poderão ser exploradas opções adicionais.

3.4.1. **Opção 1 - Carteiras digitais pessoais**

Esta opção consiste em fornecer a indivíduos e empresas uma carteira digital pessoal contendo uma prova verificável de atributos de identidade legal que pode ser utilizada para provar a sua identidade legal ou partilhar factos específicos com um prestador de serviços. Esta opção de arquitectura refere-se aos casos de utilização de Credenciais Verificáveis do W3C.[32]

Figura 2 – Visão geral da Opção 1 - Carteiras Digitais Pessoais

[32] W3C, Casos de Utilização de Credenciais verificáveis, vide: https://www.w3.org/TR/vc-use-cases/

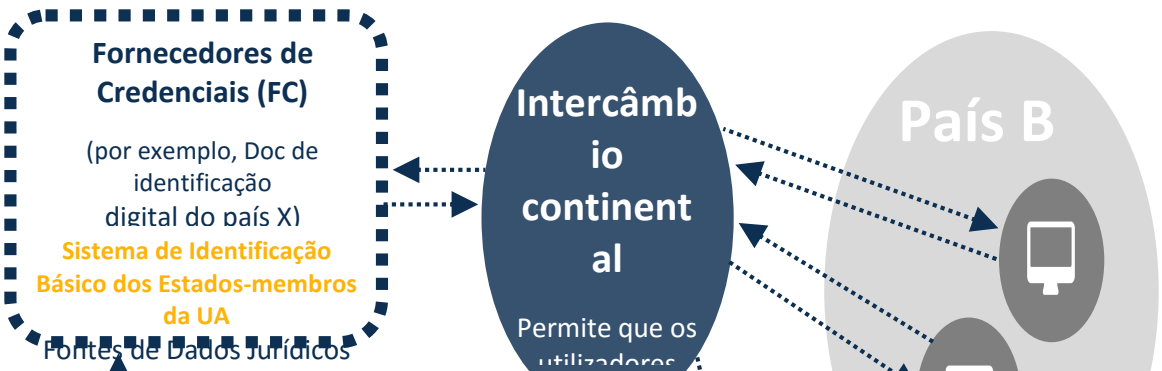
Processo de autenticação

1. O indivíduo selecciona um fornecedor de carteira de identidade para guardar o seu IDC e é necessário um processo de bordo.
2. O indivíduo recebe um IDC verificável (por exemplo, identificação, prova de morada) dos emissores autorizados e guarda-o numa **carteira digital**
3. Ao mesmo tempo da emissão, a autoridade regista uma impressão digital do **crédito numa infra-estrutura de chave pública descentralizada tendo em conta a privacidade dos cidadãos.**
4. Os indivíduos podem apresentar a um prestador de serviços (por exemplo, um seguro) uma reclamação, tal como uma **prova de morada** utilizando a sua carteira (por código QR, Bluetooth, NFC)
5. O prestador de serviços pode verificar na infra-estrutura de chave pública descentralizada que o crédito é autêntico e foi emitido por uma autoridade reconhecida.

3.4.2. **Opção 2 - Federação Continental de Identificação Digital de Fundações**

Segundo este modelo, cada residente africano poderia embarcar com um fornecedor de credenciais fundacionais a nível continental à sua escolha.

Figura 3 – Visão geral da Opção 2 – Federação Continental de Identificação Digital



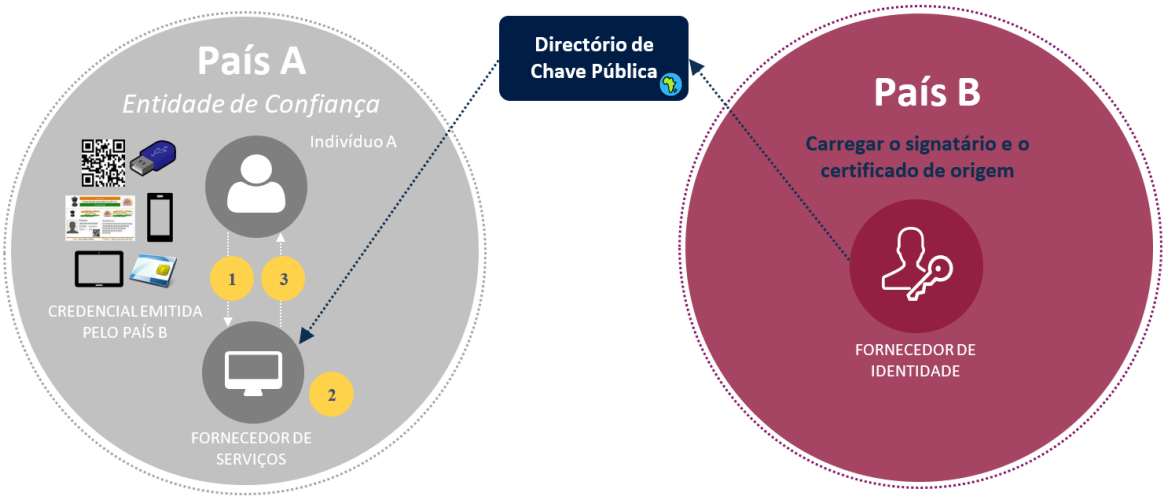
Processo de autenticação

1. **É estabelecida uma federação continental de fornecedores de credenciais de identificação fundacional**: operadores de telecomunicações, bancos, governos, etc... podem fornecer serviços de autenticação.
2. É criada uma **troca continental**, fornecendo um ponto de contacto único para todos os fornecedores de credenciais participantes e partes confiantes que queiram autenticar indivíduos.
3. Os indivíduos podem usar o seu IDC para a **bordo** do fornecedor de credenciais da sua escolha. O CP da identificação fundacional pode verificar a autenticidade do IDC.
4. Após verificação bem-sucedida, o CP emite um meio de **autenticação** para o indivíduo.
5. O indivíduo pode usar o seu meio de autenticação para aceder electronicamente **e pessoalmente aos serviços** que estão ligados ao intercâmbio continental.

3.4.3. **Opção 3 - Credenciais assinadas digitalmente**

Este modelo permite a autenticação através da verificação dos dados de identidade legal assinados digitalmente numa credencial com uma chave pública, bem como um meio adicional para partilhar a fotografia do titular.

Figura 4 – Visão geral da opção 3 - Credenciais assinadas digitalmente



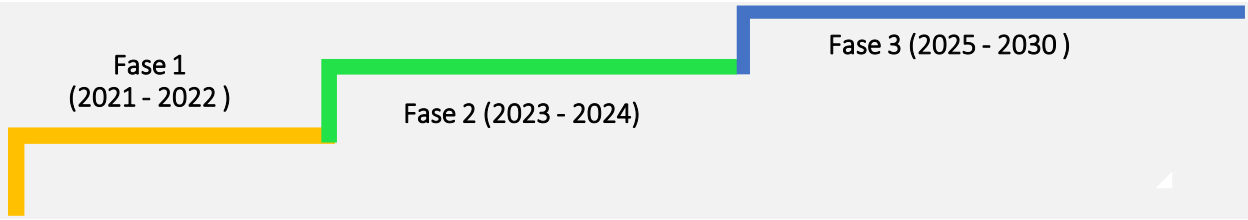
Processo de autenticação

1. Os países acordam numa **norma (por exemplo, código QR)** e fontes autorizadas assinam criptograficamente as **credenciais** (através de uma senha privada)
2. Fontes autorizadas partilham a sua chave pública num **Directório de Chaves Públicas** (PKD) cuja governação será aprovada pelos Estados-membros da UA e gerida a nível continental.
3. Os países criam um serviço separado que permite partilhar uma cópia da imagem do detentor de IDC-ID acessível através de API seguro, a fim de autenticar o detentor. Para trabalhar desconectado, é também possível que um grupo de países (por exemplo, CER) chegue a acordo sobre a emissão de uma credencial física contendo uma fotografia do titular.33
4. As fontes autorizadas dos países emitem **formulários padronizados de IDC** a indivíduos
5. É criado um **software de verificação** (app ou website) para permitir aos prestadores de serviços verificar a autenticidade e integridade da assinatura no IDC.
6. Os indivíduos podem utilizar o seu IDC para obter a sua identidade jurídica digitalmente verificada por entidades públicas ou privadas de confiança no seu país ou no estrangeiro e **aceder aos serviços.**
7. Cada Estado-membro deverá manter em armazenamento seguro tais como Módulos de Segurança de Hardware (HSMs), as chaves privadas, certificados de raiz e algoritmos de *hashing* a serem utilizados para encriptação e verificação de integridade

33 A emissão de credenciais físicas tem um custo adicional. Os Estados-membros participantes teriam de continuar a discutir o financiamento de tal solução para não criar barreiras ao acesso.

4. ROTEIRO DE ALTO NÍVEL PARA IMPLEMENTAÇÃO

Para acelerar o caminho para alcançar os ambiciosos objectivos deste Quadro, os Estados-membros da UA devem aumentar a sua colaboração para aperfeiçoar os pormenores do quadro técnico e de referência, normas e processos comuns.
A proposta é de dividir a implementação do Quadro em três fases, como mostra o diagrama abaixo:



1. Aprovação do quadro e apoio ao quadro legislativo favorável;
2. Implementação da estrutura e adopção de especificações técnicas para IDC-ID
3. A ampliação do quadro para fornecer uma infra-estrutura que permita casos de utilização mais avançada, como a autenticação remota

Para cada fase, serão planeadas oportunidades de consulta dos Estados-membros da UA, da sociedade civil e das partes interessadas do ecossistema de identidade, a fim de assegurar que o Quadro e a sua implementação se mantenham alinhados com as necessidades dos indivíduos e dos contextos locais. A documentação principal será publicada e proporcionará um período de tempo adequado para contribuições.

4.1. Fase 1: Adopção do quadro e ambiente favorável

Submissão do projecto de Quadro à 4ª sessão ordinária do CTE de Comunicação e TIC para adopção e a aprovação pelos órgãos deliberativos.

Na sequência da aprovação do presente documento, os pormenores do Quadro de Confiança serão especificados com mais detalhe e as seguintes actividades serão realizadas, nomeadamente:

- sensibilização
- estudo de viabilidade sobre o panorama actual do sistema de identificação digital em África;
- estabelecimento de um quadro de consulta para os intervenientes no ecossistema digital destinado a salvaguardar os interesses de cada interveniente
- desenvolvimento de instrumentos jurídicos e regulamentares harmonizados
- definição das regras de participação;
- criação dos mecanismos de governação e fórum para partilhar as melhores práticas ao longo de todo o processo de implementação;
- definição de disposições jurídicas que terão de ser integradas nos quadros

jurídicos nacionais dos Estados-membros da UA, a fim de implementar o Quadro, incluindo salvaguardas adequadas em matéria de segurança cibernética e protecção de dados

- ratificação da Convenção de Malabo sobre Segurança Cibernética e Protecção de Dados Pessoais;
- a adopção do quadro político continental em matéria de dados;
- nomeação de grupos de peritos pelos Estados-membros da UA para definir a interoperacionalidade e os requisitos técnicos;
- criação de estruturas institucionais independentes a nível nacional (autoridades de protecção de dados; responsável pelo controlo das autoridades de certificação; e equipas de resposta a incidentes informáticos (CIRTs) e reforço da cooperação entre instituições nacionais
- desenvolvimento de iniciativas de desenvolvimento de capacidades;
- apoio à implantação de infra-estruturas digitais, incluindo centros de dados a nível nacional, regional/continental, que sejam necessários para apoiar e sustentar a operacionalização dos sistemas de identificação digital;
- mobilização de recursos.

Para garantir o sucesso do Quadro, será definida uma série de **casos de utilização** que representam as maiores oportunidades para o continente. Um grupo de Estados-membros da UA pode ainda colaborar para testar e pilotar casos de utilização específica, juntamente com outras partes interessadas, conforme necessário.

Deve ser realizada uma avaliação dos **principais custos e benefícios** do quadro proposto e das opções de autenticação subsequente, a fim de dar maior visibilidade às necessidades de financiamento para informar os Estados-membros da UA sobre a tomada de decisões. Neste momento, espera-se que o cumprimento de uma norma harmonizada para representar informação de identidade gere custos limitados para os Estados-membros da UA, uma vez que poderia ser integrada como requisito técnico nos projectos de digitalização existentes dos seus sistemas de identificação fundacionais. Contudo, espera-se que o estabelecimento da infra-estrutura de autenticação gere custos adicionais e, dependendo dos tipos de intervenientes envolvidos, exige a definição de modelos de negócio. Para esta fase, terá de ser realizada uma avaliação de impacto detalhada a fim de assegurar que as opções de autenticação propostas se mantenham inclusivas.

Paralelamente, os Estados-membros da UA comprometem-se a: -

- elaborar e implementar quadros legais e regulamentares harmonizados que permitam criar confiança nos sistemas de identificação digital fundacional;
- Elaborar legislação harmonizada sobre dados pessoais e regulamentação de melhores práticas de protecção de dados para facilitar a harmonização entre países e para que os cidadãos possam ter mais poder, mantendo ao mesmo

tempo a soberania dos dados;

- desenvolver infra-estruturas digitais, incluindo infra-estruturas de dados (centros de dados nacionais), que constituem a base para a implementação do sistema de identificação digital
- ratificar a Convenção da UA sobre Segurança Cibernética e Protecção de Dados Pessoais (se ainda não tiver sido feita) e acelerar a sua entrada em vigor e o trabalho para acelerar a criação de autoridades de protecção de dados para a supervisão nos países participantes;
- elaborar a estratégia nacional de segurança cibernética e constituir equipas de resposta a incidentes informáticos (CIRT) para mitigar os riscos e ameaças relacionados com ataques cibernéticos, roubo de dados e tratamento incorrecto de informações sensíveis
- adoptar o quadro da Política Continental de Dados da UA. Estes devem capacitar os indivíduos e proteger a privacidade electrónica como um direito fundamental (incluir a escolha e controlo do utilizador, consentimento informado/mensurável, soberania/propriedade de dados, etc.);
- proceder ao lançamento e/ou aumento de esforços para reforçar os sistemas de identificação fundacional, para assegurar que estes sejam inclusivos e de confiança, em conformidade com normas e iniciativas relevantes, tais como o Programa Africano de Melhoria Acelerada dos Sistemas de Registo Civil e Estatísticas Vitais (APAI-CRVS) e os *Princípios de Identificação para o Desenvolvimento Sustentável.*

  Estas fases serão finalizadas com a adopção da versão completa do Quadro pelos Estados-membros da UA.

4.2. Fase 2: Implementação da estrutura e adopção de especificações técnicas para IDC-ID

A segunda fase consistirá em estabelecer o quadro de confiança e os mecanismos de governação e cooperação e fornecer a **especificação técnica** para a introdução do IDC-ID que incluirá, entre outras:

- Desenvolver normas mínimas e normas para a interoperacionalidade;
- atribuição de perfis para o conjunto mínimo de dados (formatos de dados) e metadados associados;
- Formato de apresentação (por exemplo, códigos de barras 2d, credenciais verificáveis W3C);
- Nível de Garantia (como ponto de referência para a interoperacionalidade);
- Elementos criptográficos para assinatura e encriptação de dados;
- Protocolos de verificação para casos de utilização electrónica e não electrónica.

Um grupo de EM da UA pode desenvolver uma **amostra de implementação** (aplicação ou website) para verificação básica do IDC-ID para testar a

interoperabilidade da credencial e já apoiar provas verificáveis da identidade legal. A implementação implementará a privacidade e a segurança por concepção.
Pode ser considerada a definição de **soluções alternativas para obter um IDC-ID** para pessoas que estão actualmente excluídas de qualquer sistema de ID fundacional.

Será realizado um **mapeamento de outras iniciativas em curso da União Africana** que poderão basear-se no quadro (por exemplo, Quadro de Qualificações Africano Continental)

A Fase 2 será concluída com a definição de um plano de acção claro para a definição da infra-estrutura de autenticação como parte da Fase 3.

4.3. Fase 3: Desenvolvimento da infra-estrutura para permitir a autenticação à distância

A Fase 3 começará a **implementar o quadro fiduciário** definido como parte da Fase 2:

Nesta fase, a camada que representa a emissão do IDC-ID será aumentada e expandida para implementar uma infra-estrutura que permita casos de utilização mais avançada, como a autenticação remota. Esta camada de autenticação permitirá aos indivíduos provar a sua identidade digitalmente, exercendo o controlo de um ou mais factores de autenticação (por exemplo, um código biométrico ou PIN) ligados à sua identidade legal previamente verificada, o IDC-ID. Diversas opções técnicas estão disponíveis aos Estados-membros da UA para implementar esta camada, por exemplo, uma federação de fornecedores de identidade que forneça mecanismos de autenticação aos titulares do IDC-ID, ou o desenvolvimento de soluções de carteira de identidade digital ou quaisquer outros modelos que permitam a interoperabilidade. Cada uma destas implementações pode oferecer uma abordagem de minimização de dados e serviços de divulgação selectiva para casos de uso específico, por exemplo, partilhando apenas os pontos de dados relevantes de um cartão de identificação e relatório de crédito para obter um empréstimo, procurar benefícios sociais ou de saúde, obter pensão, quando a autenticação é legalmente exigida ou anonimizar o conjunto mínimo de dados da IDC-ID (por exemplo, nome, data de nascimento) numa prova de maioridade (+18y ou +21y ou uma resposta de sim/não).

Os Estados-membros da União Africana poderão também procurar mais discussão e acordo sobre a forma de estabelecer esta infra-estrutura da camada de autenticação e estabelecer parcerias com as CER e outras iniciativas continentais que já estão a investigar a introdução de soluções interoperáveis de ID digital para aceder aos serviços à distância. De facto, os Estados Membros e as organizações poderão tirar partido da representação comum baseada em padrões de informação de identidade

num formato digital seguro e de confiança e construir serviços adicionais sobre a mesma.

Os Estados-membros da UA continuarão a colaborar para reforçar o quadro de confiança e os mecanismos de governação e cooperação, na sequência do acordo sobre as infra-estruturas adicionais que se seguirão:

- **Coordenação com outras iniciativas** destinadas a estabelecer a interoperabilidade a nível continental (por exemplo, SATA e RECs)
- **Acordo sobre a melhor opção arquitectónica** (por exemplo, federação, carteiras digitais, etc.) para desenvolver a função de autenticação remota que se basearia nas Credenciais Digitais Interoperáveis (IDC-ID).

1.	Exclusão, segurança fraca e erosão da protecção de dados pessoais	Aplicação dos Princípios definidos no quadro (3.1) e reforço dos quadros jurídicos e infra-estruturas de segurança e protecção de dados nos Estados-membros da UA.
2	Relutância dos Estados-membros da UA em adoptar e implementar o quadro	Sensibilizar para os benefícios da estrutura de interoperabilidade a nível doméstico e continental e reforçar o sistema de identificação fundacional.
3	Falta de capacidade técnica e financeira nos Estados-membros da UA	Aumentar a capacidade e promover o intercâmbio de conhecimentos entre pares entre os Estados-membros da UA, bem como considerar a relação custo-eficácia das soluções tecnológicas a serem acordadas nas Fases 2 e 3
4	Centros de dados inadequados a nível nacional/regional/continente	Construir centros de dados nacionais/regionais/nacionais e promover a sua utilização por África.

A Fase 3 será concluída com um plano de acção claro sobre a implementação da camada de autenticação de acordo com a opção arquitectónica a ser acordada entre os Estados-membros e organizações da UA.

5. SUPOSIÇÕES DE ALTO NÍVEL, DESAFIOS e Riscos

5.1. Pressupostos

Os Estados-membros adoptarão o quadro, colaborarão, comprometer-se-ão a implementar e a levar a cabo as reformas legais e regulamentares necessárias e exigidas.

5.2. Desafios gerais e propostas de mitigação de alto nível

O quadro abaixo resume os desafios gerais e os mecanismos de mitigação propostos

5.3. Riscos e propostas de mitigação

O quadro abaixo resume os riscos e os mecanismos de mitigação propostos

1	Ausência de uma definição adequada de norma comum e falta de compreensão por parte dos Estados-membros da UA e incapacidade de seguir e adoptar normas comuns	Definição de normas e comunicação das mesmas aos Estados-membros da UA durante a implementação e acompanhamento regular por um organismo pan-africano de confiança e capacitado que é apoiado e aprovado por todos os Estados-membros da mesma para garantir a adesão às normas. Discussões e workshops focalizados com as partes interessadas para assegurar uma definição clara das normas para a estratégia de implementação escolhida Avaliação de referência da estratégia de implementação baseada em padrões do Estado-membro da UA em relação a programas de identificação nacionais fundacionais similares baseados em padrões estabelecidos em todos os Estados-membros da UA
2	Baixos níveis de confiança entre as autoridades nacionais com capacidades de execução heterogéneas conduzem a uma lenta aceitação do quadro a uma grande escala continental. Além disso, os Estados-membros não estão dispostos a aceitar um organismo de supervisão supranacional, retardam a implementação do quadro de confiança.	O quadro deveria visar a harmonização e o reconhecimento mútuo como um objectivo a longo prazo, mas permanecer aberto ao desenvolvimento de soluções flexíveis e ágeis, que.
3	A solução, benefícios e opções não estão bem adaptadas ao ambiente local ou a informação é mal divulgada e as pessoas não estão a utilizar a solução levando a uma má aceitação e, em última análise, a custos elevados com poucos benefícios.	Desenvolver fortes estruturas de desenho centradas no utilizador para identificar soluções poderiam criar mecanismos de auditoria partilhados entre países dispostos a estabelecer confiança entre si, mantendo-se simultaneamente soberanos - através do reconhecimento unilateral dos certificados de confiança emitidosque sejam fáceis de utilizar e acessíveis a todos; Desenvolver fortes mecanismos de disseminação através dos Estados-membros da UA que incorporem todos os actores locais com os mesmos objectivos.
4	Ausência de Instituição Certificadora a nível continental e falta de governação inadequada os requisitos criptográficos para a assinatura digital podem revelar-se um	Criação de um quadro legal que permita o estabelecimento de uma instituição coordenadora a nível continental que seja apoiada por uma estrutura de governação equitativa que contabilize a soberania de cada Estado-membro para a implementação e gestão das assinaturas digitais, a sua emissão, revogação e substituição e actualização atempadas.

	obstáculo na criação do sistema de Interoperabilidade	Criação de uma estrutura de organização detalhada e dinâmica para permitir a governação da infra-estrutura de assinatura digital / PKI durante toda a fase de implementação e de operações.
5	Devido a dados incorrectos e incompletos, a concepção e estratégia de implementação de alguns dos componentes de interoperabilidade, como as assinaturas digitais, pode ser afectada. O atraso na partilha de dados e informações relevantes do cidadão ou residente pode também ter impacto nos prazos do projecto	Reuniões com agências governamentais para a recolha de dados relativos à implementação nas lacunas de informação, aproveitando a experiência dos peritos através da aprendizagem entre pares para encorajar a colaboração e a apropriação regional e continental. Monitorização dos prazos e marcos do projecto para evitar atrasos. É também imperativo ter um calendário de implementação detalhado e abrangente que tenha sido acordado pelos Estados-membros da UA e pelas principais partes interessadas
6	Ausência de directrizes de gestão da mudança claramente definidas para assegurar que o Quadro se mantém alinhado com as práticas, necessidades e desenvolvimento tecnológico actuais:	Implementação de um processo sólido e bem definido de gestão da mudança como parte do quadro de governação
7	Os Estados-membros decidirão sobre a tecnologia apropriada durante a fase de implementação, no entanto, se optarem pela tecnologia PKI, As agências certificadoras em África podem não chegar a um consenso em relação à gestão de PKI a nível de todo o continente. Em segundo lugar, pode não haver consensos sobre a criação de intercâmbio de assinaturas digitais	Os Estados-membros da UA criaram uma nova instituição de certificação para a gestão de PKI a nível do continente ou aprovam um mecanismo para trazer as agências existentes para uma plataforma comum.
8	Não ter o ambiente legal mínimo necessário a nível nacional e regional	Os Estados-membros da UA a acelerarem a implementação dos quadros jurídicos e regulamentares harmonizados necessários

6. ANEXO

6.1. Definições de trabalho

Atributo é uma qualidade nomeada ou característica inerente ou atribuída a alguém ou algo (adaptado de NIST 800-63:2017). Nos sistemas de identificação, os atributos comuns de identidade incluem nome, idade, sexo, local de nascimento, endereço, impressões digitais, fotografia, assinatura, número de identidade, etc.

A autenticação é o processo de estabelecer a confiança de que uma pessoa é quem afirma ser. A autenticação digital envolve geralmente uma pessoa que apresenta electronicamente um ou mais "factores" para "afirmar" a sua identidade - isto é, para provar que é a mesma pessoa a quem a identidade ou credencial foi originalmente emitida. Estes factores podem incluir algo que uma pessoa sabe (por exemplo, uma senha ou PIN), tem (por exemplo, um cartão de identificação, ficha, ou cartão SIM móvel), ou é (por exemplo, as suas impressões digitais) (adaptado de NIST 800-63:2017 e OWI 2017).

A autorização é o processo de determinação das acções que podem ser realizadas ou dos serviços acedidos com base na identidade afirmada e autenticada (Nyst et al. 2016).

Fonte autorizada é uma fonte autorizada de informação de identidade é um repositório ou sistema que contém atributos sobre um indivíduo e é considerado como sendo a fonte primária ou mais fiável para esta informação. No caso de dois ou mais sistemas não corresponderem ou terem dados contraditórios, os dados dentro da fonte de dados autorizada são considerados os mais exactos (FICAM, sem data).

Reivindicação é uma qualificação, realização, qualidade, ou informação sobre o passado de um sujeito, tal como um nome, identificação governamental, endereço de casa, ou grau universitário. (Adaptado de W3C)

O **consentimento** da pessoa em causa significa qualquer indicação livre, específica, informada e inequívoca da vontade da pessoa em causa, pela qual esta, através de uma declaração ou de uma acção afirmativa clara, manifesta a sua concordância com o tratamento dos dados pessoais que lhe dizem respeito.

Credencial é um documento, objecto ou estrutura de dados que garante a identidade de uma pessoa através de algum método de confiança e autenticação. Os tipos comuns de credenciais de identidade incluem - mas não estão limitados a - cartões de identificação, certificados, números, senhas, ou cartões SIM. No caso deste Quadro, a credencial é um crédito verificável designado por IDC-ID.

Por **responsável pelo tratamento de dados** entende-se qualquer pessoa singular ou colectiva, pública ou privada, qualquer outra organização ou associação que, sozinha ou em conjunto com outras, decida recolher e tratar dados pessoais e determine as finalidades.

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

As Autoridades de Protecção de Dados (APD) são autoridades públicas independentes que controlam e supervisionam, através de poderes de investigação e correctivos, a aplicação da lei de protecção de dados. Prestam aconselhamento especializado sobre questões de protecção de dados e tratam queixas que possam ter infringido a lei.

Por **pessoas em causa** entende-se qualquer pessoa singular que seja objecto de tratamento de dados pessoais.

A **dignidade digital** (no contexto da identificação digital) significa que a identidade humana por detrás da identificação digital tem privacidade e os seus dados são protegidos.

O **sistema de identificação digital (ID)** é um sistema de identificação que utiliza tecnologia digital durante todo o ciclo de vida da identidade, incluindo para a captura, validação, armazenamento e transferência de dados; gestão de credenciais; e verificação e autenticação de identidade (adaptado do relatório de Cooperação Público-Privada ID4D).

A i**dentidade digital** é um conjunto de atributos e/ou credenciais electronicamente capturados e armazenados que identificam de forma única uma pessoa (adaptado de Harbitz & Kentala 2013 e do relatório intitulado ID4D Technology Landscape).

A **assinatura digital** é uma operação de chave assimétrica em que a chave privada é utilizada para assinar digitalmente dados e a chave pública é utilizada para verificar a assinatura. As assinaturas digitais fornecem protecção de autenticidade, protecção de integridade e não repúdio, mas não protecção de confidencialidade (NIST 800-63:2017).

O **sistema de identificação fundamental** é um sistema de identificação criado principalmente para gerir informações de identidade para a população em geral e fornecer credenciais que servem como prova de identidade para aceder a serviços públicos e privados tais como educação, cuidados de saúde, protecção social e

serviços financeiros, etc. (adaptado de Gelb & Clark 2013a e várias publicações ID4D). Para os fins deste Quadro, os Estados-membros da UA decidirão quais as fontes de dados fiáveis que implicam os seus Sistemas de Identificação Fundacionais.

Sistemas funcionais de identificação é um sistema de identificação criado para gerir a identificação, autenticação e autorização para um determinado serviço ou transacção, tais como votação, administração fiscal, programas e transferências sociais, serviços financeiros, e muito mais. Credenciais de identidade funcionais - tais como identificação do eleitor, registos de saúde e de seguros, números de identificação fiscal, cartões de racionamento, cartas de condução, etc. - podem ser geralmente aceites como prova de identidade para fins mais amplos fora da sua intenção original, particularmente quando não existe um sistema de identificação fundacional (adaptado de Gelb & Clark 2013a e várias publicações ID4D).

A **harmonização** está a assegurar uniformidade nos sistemas através da utilização de normas mínimas para facilitar a interoperabilidade e quadros legais e de confiança (por exemplo, para níveis de garantia) para estabelecer regras e criar confiança nos respectivos sistemas.

Identificação é um acrónimo para credencial de identidade ou documento de identidade em algumas áreas.

Sistema de identificação (ID) são as bases de dados, processos, tecnologia, infra-estrutura, credenciais e quadros legais associados à captura, gestão e utilização de dados de identidade pessoal para um fim geral ou específico (adaptado dos Princípios sobre Identificação).

A **identificação** é o processo de estabelecer, determinar ou reconhecer a identidade de uma pessoa. (adaptado de ISO/IEC 24760-1:2011 e ITU-T X.1252).

A **identidade** são as coordenadas sociais relativas que distinguem um indivíduo de outro. A identidade pode mudar dependendo dos actores ou do cenário em que os indivíduos se encontram e, portanto, não é fixa nem absoluta.

O **fornecedor de identidade** é uma entidade autorizada - por exemplo, uma agência governamental ou empresa privada - que emite e gere identidades legais, credenciais e processos de autenticação ao longo do ciclo de vida da identidade (documento de Cooperação Público-Privada ID4D).

Interoperacionalidade é a capacidade das diferentes unidades funcionais - por exemplo, sistemas, bases de dados, dispositivos ou aplicações - de comunicar, executar programas, ou transferir dados de uma forma que requer que o utilizador

tenha pouco ou nenhum conhecimento dessas unidades funcionais (adaptado de ISO/IEC 2382:2015).

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

Normas Abertas são normas disponibilizadas ao público em geral e são desenvolvidas (ou aprovadas) e mantidas através de um processo de colaboração e de consenso. As “Normas Abertas” facilitam a interoperacionalidade e o intercâmbio de dados entre diferentes produtos ou serviços e destinam-se a uma adopção generalizada (adoptadas a partir da UIT-T).

Por **dados pessoais** entende-se qualquer informação relativa a uma pessoa singular identificada ou identificável através da qual essa pessoa possa ser identificada, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a factores mais específicos da sua identidade física, fisiológica, mental, económica, cultural ou social.

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

A **Avaliação de Impacto da Protecção de Dados (DPIA)** é um processo concebido para identificar os riscos decorrentes do processamento de dados pessoais e para minimizar esses riscos o mais longe e o mais cedo possível. Os DPIAs são ferramentas importantes para negar o risco, e para demonstrar o cumprimento das leis e regulamentos de protecção de dados.

Por **tratamento de dados pessoais** entende-se qualquer operação ou conjunto de operações efectuadas sobre dados pessoais, seja ou não por meios automáticos como a recolha, registo, organização, armazenamento, adaptação, alteração, recuperação, cópia de segurança, cópia de segurança, consulta, utilização,

divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, alinhamento ou combinação e bloqueio, encriptação, apagamento ou destruição de dados pessoais.

A **prova de identidade legal** é uma credencial, tal como uma certidão de nascimento, bilhete de identidade ou credencial de identidade digital, que é reconhecida como prova de identidade legal ao abrigo do direito nacional e de acordo com as normas e princípios internacionais emergentes (Grupo de Peritos em Identidade Legal das Nações Unidas Definição Operacional de Identidade Legal).

A **parte confiante (RP)** é uma entidade que depende das credenciais e mecanismos de autenticação fornecidos por um sistema de identificação, normalmente para processar uma transacção ou conceder acesso à informação ou a um sistema (adaptado de NIST 800-63:2017).

O **quadro de confiança** refere-se aos requisitos empresariais, técnicos, operacionais e legais do sistema de identidade para promover a interoperabilidade entre as várias partes participantes.

Apresentação verificável é uma apresentação inviolável (Dados derivados de uma ou mais credenciais verificáveis) codificada de tal forma que a autoria dos dados pode ser confiada após um processo de verificação criptográfica. Por exemplo, abordagens de divulgação selectiva que sintetizam os dados e não transmitem as credenciais originais verificáveis (Adaptado do W3C)

A **verificação** é definida como o processo de verificação de atributos de identidade específicos ou de determinação da autenticidade das credenciais, a fim de facilitar a autorização para um determinado serviço.

AFRICAN UNION

الاتحاد الأفريقي

UNION AFRICAINE

UNIÃO AFRICANA

P. O. Box 3243, Addis Ababa, ETHIOPIA Tel.: (251-11) 5182402 Fax: (251-11) 5.182.400

Website: www.au.int

Departamento de Infra-estruturas e Energia
Divisão da Sociedade de Informação

Projecto de Quadro Continental de Política de Dados

Setembro de 2021

Sumário Executivo

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

O objectivo do presente documento é fornecer o quadro político para os países africanos maximizarem os benefícios de uma economia baseada em dados através da criação de um ambiente político favorável aos investimentos privados e públicos necessários para apoiar a criação de valor e inovação baseada em dados. Este ambiente propício refere-se tanto à colaboração entre sectores, instituições e partes interessadas no país, um alinhamento das suas prioridades de desenvolvimento, como à harmonização das políticas em todo o continente de uma forma que proporcione a escala e o âmbito necessários para criar mercados globalmente competitivos.

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

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

Uma estratégia global de dados incluirá necessariamente a harmonização entre a concorrência, o comércio e as políticas e leis fiscais, tanto a nível nacional como regional. Este é um ecossistema de dados optimizado para África que equilibra a mobilização de receitas e a necessidade de evitar distorções nos mercados locais e no sistema fiscal global. As leis de propriedade intelectual também devem ser revistas

para esclarecer que não impedem geralmente o fluxo de dados ou a protecção de dados. Ao mesmo tempo, os governos precisam de desenvolver políticas e estratégias digitais transversais para coordenar actividades em todo o sector público e entre os sectores público e privado para cumprir os objectivos nacionais.

Embora existam múltiplas definições de dados competitivos, comum a todos é o reconhecimento de que existem muitos tipos diferentes de dados. Existem também diversas formas de classificar os dados que afectam a política e regulamentação adequadas dessa categoria, a fim de mitigar qualquer risco potencial associado ao processamento, transferência ou armazenamento dos mesmos. Uma distinção principal é a existente entre dados pessoais e dados não pessoais, sendo que a protecção de dados refere-se à garantia da privacidade das pessoas em causa. As directrizes de categorização de dados devem ser uma das primeiras acções do regulador de informações de dados, uma instituição fundamental para o desenvolvimento de um sistema nacional integrado de dados, que deve ser estabelecida em parceria com todas as partes interessadas relevantes. Essencial para o desenvolvimento de um ambiente favorável à economia de dados é assegurar a infra-estrutura digital fundamental necessária, e os recursos humanos necessários para desenvolver os dados como um bem estratégico. Deve ser dada a devida atenção ao desenvolvimento de sistemas robustos de identificação digital para a entrega de valor público e privado aos cidadãos e consumidores.

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

O quadro sublinha a importância da colaboração e dos processos políticos baseados em provas para o enquadramento da política proposta. A governação e as disposições institucionais devem atribuir papéis claros ao governo como decisor político, e reguladores independentes, ágeis e capacitados para implementar políticas e regular eficazmente a economia de dados para assegurar que a concorrência leal produza resultados positivos no bem-estar dos consumidores. A criação de reguladores de dados e informação, para promover e salvaguardar os direitos dos cidadãos e a sua participação e representação justa na economia e sociedade de dados, terá de ser uma prioridade para os países que ainda não os tenham estabelecido. A coordenação com outros reguladores para alcançar este objectivo será essencial. O ecossistema jurídico deve ser harmonizado e reequilibrado.

O acesso aos dados é um pré-requisito para a criação de valor, empreendedorismo e inovação. Quando os dados são de má qualidade ou não interoperacionais, limitam a capacidade das empresas e do sector público de se envolverem na partilha e análise que podem fornecer valor económico e social aos dados. Estas estruturas de processamento devem alinhar-se com os seguintes princípios: consentimento e legitimidade; limitações à recolha; especificação da finalidade; limitação da utilização; qualidade dos dados; salvaguardas de segurança; abertura (que inclui a comunicação de incidentes, uma correlação importante com os imperativos da segurança

cibernética e do crime cibernético); responsabilidade; e especificidade dos dados. Os modelos de segurança também precisam de ser transversais, com ênfase específica no armazenamento e processamento de dados sensíveis/proprietários na nuvem, na gestão de API e no apoio a economias de dados equitativas

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

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

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

Como o quadro sugere, existem vários processos, mecanismos e instrumentos regionais que podem e devem ser alavancados nos esforços do continente para desenvolver um quadro político de dados coesos. Estes incluem o Acordo da Zona de Comércio Livre Continental Africana (ZCLCA), que proporciona uma oportunidade para a cooperação em vários aspectos importantes do quadro político. A colaboração entre as partes interessadas nacionais e regionais é também necessária para que os países africanos se tornem mais competitivos nos fóruns de definição de políticas globais onde são estabelecidos regulamentos para a economia global de dados, e onde os estados africanos têm sido, em grande parte, “entidades responsáveis pela normalização”.

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

O Quadro apresenta um conjunto de recomendações detalhadas e acções emergentes para orientar os Estados-membros através das formulações de políticas no seu contexto interno, contexto, bem como recomendações para reforçar a cooperação entre países e promover os fluxos intra-africanos de dados. As principais

recomendações globais de alto nível estão aqui incluídas. Recomenda-se aos Estados-membros que:

- permitam, em cooperação, o fluxo de dados no continente, salvaguardando os direitos humanos, a protecção de dados, mantendo a segurança e assegurando a partilha equitativa dos benefícios;
- cooperem para criar as capacidades necessárias para aproveitar as tecnologias e serviços dependentes de dados, incluindo a capacidade de governar os dados para que estes beneficiem os países e cidadãos africanos e permitam o desenvolvimento;
- promovam uma política de dados transversal e uma regulamentação ágil para navegar na emergência de novos modelos de negócios dinâmicos orientados para os dados que possam fomentar o comércio digital intra-africano e o empreendedorismo com base em dados;
- criem quadros co-jurisdicionais para a coordenação da concorrência autónoma, do sector e dos reguladores de dados para regular eficazmente a economia da sociedade de dados, formular, implementar e rever a política de dados de uma forma dinâmica, prospectiva e experimental;
- Desenvolvam legislações nacionais sobre protecção de dados pessoais e regulamentos adequados, particularmente em torno da governação de dados e plataformas digitais, para assegurar que a confiança seja preservada no ambiente digital.
- estabeleçam ou mantenham autoridades de protecção de dados independentes, bem dotadas e eficazes , reforcem a cooperação com as APD dos membros da União Africana e desenvolvam mecanismos a nível continental para desenvolver e partilhar práticas regulamentares e apoiar o desenvolvimento institucional para assegurar um elevado nível de protecção dos dados pessoais ;
- promovam a interoperacionalidade, a partilha de dados e a capacidade de resposta à procura de dados através da definição de normas de dados abertas na produção de dados em conformidade com os princípios gerais de anonimato, privacidade, segurança e quaisquer considerações sobre dados específicos do sector para facilitar dados não pessoais e certas categorias de dados pessoais são acessíveis a investigadores, inovadores e empresários africanos;
- promovam a portabilidade dos dados para que as pessoas em causa não fiquem presas a um único fornecedor e, ao fazê-lo, promovam a concorrência, a escolha do consumidor e permitam aos trabalhadores de representação gráfica deslocarem-se entre plataformas;
- melhorem as infra-estruturas desenvolvidas de forma desigual em todo o continente, aproveitando os esforços regionais das CER existentes para apoiar uma cobertura de rede de banda larga eficiente, um fornecimento de energia fiável e infra-estruturas e sistemas (de dados) digitais fundacionais (IDE) (identidade digital (Digital ID), pagamentos interoperáveis de confiança, infra-estruturas nebulosas e de dados, e sistemas abertos de partilha de dados, para o comércio digital transfronteiriço, comércio electrónico
- estabeleçam um sistema nacional integrado de dados para permitir a criação de valor público e privado, operando com base em quadros de governação harmonizados que facilitem o fluxo de dados necessários para uma economia de dados vibrante, mas com salvaguardas suficientes para ser confiável, seguro e protegido.

- Governem o sistema nacional integrado de dados de acordo com os princípios de acesso, disponibilidade, abertura (onde o anonimato pode ser preservado), interoperabilidade, segurança, qualidade, integridade:
- integrem códigos ou directrizes de dados específicos do sector e peritos em regimes nacionais e continentais de gestão de dados;
- Os que ainda não o fizeram, que ratifiquem a Convenção da UA sobre Segurança Cibernética e Protecção de Dados Pessoais, que o façam o mais rapidamente possível, para servir de etapa fundamental para a harmonização do tratamento de dados; e
- Nas próximas negociações sobre o comércio de serviços e os protocolos de comércio electrónico, bem como os protocolos da concorrência e da propriedade intelectual, na Zona de Comércio Livre Continental Africana forneçam directrizes para promover o acesso aos dados para apoiar a inovação local, o empreendedorismo e para fins pró-competitivos.
- dar prioridade a parcerias politicamente neutras que tenham em conta a soberania individual e a propriedade nacional para evitar interferências estrangeiras que possam afectar negativamente a segurança nacional, os interesses económicos e a evolução digital dos Estados-membros da UA
- promover a investigação, desenvolvimento e inovação em várias áreas baseadas em dados, incluindo, Big Data Analytics, Artificial Intelligence, Quantum Computing, bem como Blockchain

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

- facilitem a colaboração entre as várias entidades que lidam com dados em todo o continente através do estabelecimento de um quadro de consulta no seio da comunidade do ecossistema digital para salvaguardar os interesses de cada interveniente.
- promovam e facilitem os fluxos de dados dentro e entre os Estados-membros da UA, desenvolvendo um Mecanismo de Fluxos de Dados Transfronteiriços que tenha em conta os diferentes níveis de prontidão digital, maturidade dos dados, bem como os ambientes legais e regulamentares;

- facilitem a circulação de dados através de sectores e fronteiras, desenvolvendo um Quadro Comum de Categorização e Partilha de Dados que tenha em conta os amplos tipos de dados e os níveis associados de privacidade e segurança;

- Trabalhem em estreita colaboração com as autoridades nacionais responsáveis pela protecção de dados pessoais dos membros da UA, com o apoio da Rede Africana de Autoridades (RAPDP), para estabelecer um mecanismo e órgão de coordenação que supervisiona a transferência de dados pessoais dentro do continente e assegura o cumprimento das leis e regras existentes que regem a segurança de dados e informações a nível nacional.

- Criem ou confiram poderes a um mecanismo no seio da União Africana para centralizar e conferir poderes aos compromissos regionais relativos às normas de dados.

- estabeleçam mecanismos e instituições, ou habilitem os já existentes, no âmbito da União Africana para reforçar as capacidades e prestar assistência técnica aos Estados-membros da UA para a aplicação interna deste quadro de política de dados; e

- Apoiem o desenvolvimento de infra-estruturas de dados regionais e continentais para albergar tecnologias avançadas orientadas para os dados (tais como Grandes Dados, Aprendizagem de Máquinas e Inteligência Artificial) e o necessário ambiente facilitador e mecanismo de partilha de dados para assegurar a circulação através do continente;

- Trabalhem para construir um espaço cibernético seguro e resiliente no continente que ofereça novas oportunidades económicas através do desenvolvimento de uma Estratégia de Segurança Cibernética da UA e do estabelecimento de Centros Operacionais de Segurança Cibernética para mitigar riscos e ameaças relacionadas com ciberataques, violações de dados e utilização indevida de informação sensível.

- criem um Fórum Anual de Inovação de Dados para África para sensibilizar os decisores políticos sobre o poder dos dados como um factor impulsionador de uma economia e sociedade digital , de modo a facilitar os intercâmbios entre países e permitir a partilha de conhecimentos sobre a criação de valor e inovação dos dados e as implicações da utilização dos dados na privacidade e segurança das pessoas .

- Reforcem as ligações com outras regiões e coordenar as posições comuns africanas sobre as negociações internacionais relacionadas com dados para assegurar a igualdade de oportunidades na economia digital global;

- desenvolvem um plano de implementação que tenha em consideração a soberania digital dos Estados, bem como os diferentes níveis de desenvolvimento, a vulnerabilidade das populações e a digitalização nos Estados-membros da UA, nomeadamente aspectos relacionados com a lacuna das infra-estruturas TIC e a falta de políticas e legislações em matéria de cibersegurança.

.

ÍNDICE

1. Introdução

Os dados estão no centro da transformação digital que ocorre a um ritmo e escala sem precedentes a nível mundial. A utilização de tecnologias orientadas para os dados para transformar a maioria dos aspectos da nossa vida quotidiana e do nosso trabalho em dados quantificáveis que podem ser rastreados, monitorizados, analisados e monetizados tornou-se um fenómeno tal que o termo "publicação de dados" foi criado para o descrever.

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

Alguns desses processos têm sido incrementais e alguns disruptivos, mas todos têm sido altamente irregulares. A utilização de dados é um dos principais factores para acelerar a realização da Agenda 2063 e dos Objectivos de Desenvolvimento Sustentável (ODS), sendo a ausência de bons dados um dos principais desafios para avaliar os progressos que estão a ser feitos para atingir os objectivos subjacentes. Especificamente, sistemas de dados integrados melhorados contribuem directamente para a realização de vários dos objectivos, tais como a melhoria da saúde, sistemas de identidade dos sistemas educativos, mas sem intervenção política directa, a actual distribuição desigual das oportunidades e danos resultantes da comunicação de dados entre países e dentro dos mesmos será exacerbada.

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

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

Os dados são de natureza global, o que significa que, por um lado, os regulamentos têm implicações transfronteiriças, e que, por outro lado, a precedência regulamentar é mais frequentemente estabelecida pelos países desenvolvidos ricos e intensivos em dados. A pressão do mercado é também imposta por empresas de oligopólio, nomeadamente Facebook, Apple, Microsoft, Google, e Amazon (ou FAGAM). A natureza dos dados permite a estas empresas que negoceiam em mercados digitais globais de dados aproveitarem a sua vantagem competitiva em dados e algoritmos em todo o mundo. Isto acaba por afectar a concorrência local e inibir a competitividade global dos participantes da economia de dados nacionais. Existem, portanto, questões de propriedade intelectual e acesso aos dados, comércio justo, concorrência e direitos dos consumidores que têm impacto na política de dados num contexto global e suscitam a necessidade de uma governação e colaboração globais.

Estes factores também sublinham que muito do que impulsiona o desenvolvimento da economia de dados local, tem estado fora do controlo dos intervenientes africanos, que têm sido, em grande parte, "entidades

responsáveis pela normalização na governação global. Também sublinham a necessidade de colaboração e parcerias em muitos ecossistemas de dados africanos, independentemente da maturidade digital e das dotações económicas mais amplas.

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

2. Mandato

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

Este Quadro de Política de Dados deriva da Estratégia de Transformação Digital (DTS) adoptada pela União Africana em 2020 para transformar as sociedades e economias africanas de uma forma que permita ao continente e aos seus Estados-membros aproveitarem as tecnologias digitais para a inovação local, que melhorará as oportunidades de vida, melhorará a pobreza, reduzir a desigualdade facilitando a entrega de bens e serviços.[34] A realização dos objectivos da ETED é fundamental para a concretização da Agenda 2063 da União Africana, o quadro estratégico pan-africano para a unidade, autodeterminação, liberdade, progresso e prosperidade colectiva, e dos Objectivos de Desenvolvimento Sustentável das Nações Unidas.

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

Este Quadro de Política de Dados estabelece uma visão comum, princípios, prioridades estratégicas e recomendações fundamentais para orientar os Estados-membros da União Africana no desenvolvimento dos seus sistemas e capacidades nacionais de dados, de modo a obterem valor efectivo dos dados que estão a ser gerados pelos cidadãos, entidades governamentais e indústrias. O potencial das soluções baseadas em dados para superar a maioria dos desafios de desenvolvimento de África é tornado possível pelos Estados-

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

membros que adoptam uma política de dados comum sustentada por uma abordagem de governação coerente. Além disso, o desenvolvimento de sistemas de dados integrados é fundamental para optimizar os fluxos de informação e os ganhos de produtividade da digitalização e da publicação de dados.

Este Quadro de Política de Dados visa reforçar e harmonizar os quadros de governação de dados em África e assim criar um espaço de dados partilhados e normas que regulam a intensificação da produção e utilização de dados em todo o continente. Isto é possível criando um ambiente digital seguro e digno de confiança para impulsionar o desenvolvimento de uma economia digital inclusiva e sustentável que fomente o Comércio Digital Intra-africano, em conformidade com as iniciativas de integração económica regional em curso no âmbito da ZCLCA.

Caso de utilização de dados para criação de valor
Os desertos de dados em muitos países africanos reflectem a fractura digital, uma vez que muitas pessoas não têm acesso aos serviços e sistemas utilizados para gerar os dados necessários para formar algoritmos ou para analisar para a tomada de decisões. Os conjuntos de dados gerados pelos utilizadores, tais como as actualizações das redes sociais e os registos directos de chamadas (CDR), são uma parte importante da revolução dos dados, desde que sejam recolhidos de forma responsável. Estes conjuntos de dados podem ser combinados e reestruturados com outros dados, tais como dados anónimos dos cidadãos para reflectir as experiências vividas de milhões de indivíduos e fornecer informações valiosas sobre muitas comunidades vulneráveis diferentes que podem informar a elaboração de políticas, melhorar as intervenções e estimular a actividade económica em vários casos de utilização. *Por exemplo, no Senegal foram utilizados grandes dados para mapear CDR, mobilidade e actividade económica, no Quénia foram utilizados grandes dados sobre transacções de dinheiro móvel do M-Pesa para criar produtos de crédito e poupança para subscritores e criar perfis de crédito para pequenos agricultores para empréstimos de insumos e colheitas, uma secção da economia que normalmente não consegue aceder aos mecanismos bancários formais*[35]

2.1 Visão

O Quadro de Política de Dados prevê 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 o desenvolvimento socioeconómico equitativo.

Praticamente o processo procura traduzir esta visão num quadro que, quando implementado:

- Capacitar os africanos a exercerem os seus direitos através da promoção de sistemas de dados fiáveis, seguros e seguros integrados com base em normas e práticas comuns;
- criar, coordenar e capacitar instituições de governação para regular, conforme necessário, o cenário de dados em constante mudança e aumentar o uso produtivo e inovador dos dados para fornecer soluções e criar novas oportunidades, ao mesmo tempo que mitiga riscos.
- garantir que os dados possam fluir através das fronteiras o mais livremente possível, ao mesmo tempo que se consegue uma distribuição equitativa dos benefícios e se aborda os riscos relacionados com os direitos humanos e a segurança nacional.

2.2. Âmbito e Objectivos

Tendo em conta que os dados atravessam agora todos os aspectos da nossa vida quotidiana, mas em circunstâncias muito diferentes em todo o continente, o **quadro fornece orientações baseadas em princípios** aos Estados-membros na sua apropriação da política de dados continental adequada às suas condições e propõe um instrumento ou mecanismo continental para integrar e coordenar os esforços continentais. O Quadro Africano para a Política de Dados visa **reforçar os sistemas nacionais de dados** para uma utilização eficaz dos dados, criando um ambiente favorável **que estimule a inovação, empreendedorismo para**

[35] https://www.developlocal.org/the-big-data-in-africa-report/

impulsionar o desenvolvimento de economias orientadas para o valor dos dados e que facilite a interoperabilidade dos sistemas e dos fluxos de dados transfronteiriços necessários à realização do mercado digital único africano. Harmonizado em todos os mercados africanos, isto proporciona a certeza regulamentar e a escala e âmbito conducentes aos investimentos necessários para a criação de valor público e privado com os impactos distributivos e multiplicadores não económicos associados.

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

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

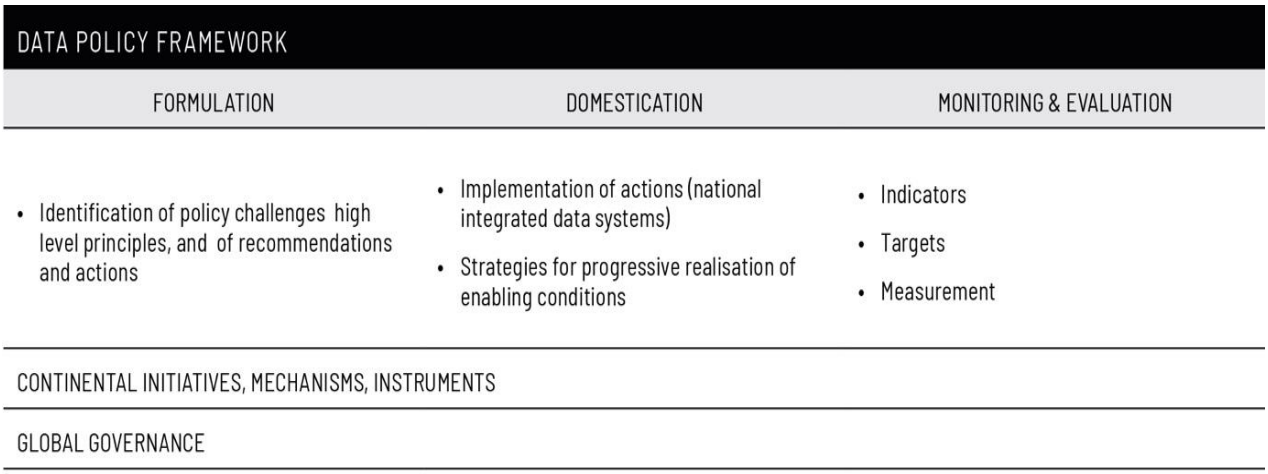
- permitir que os Estados cooperem em matéria de governação dos dados para alcançar objectivos comuns relacionados com o desenvolvimento sustentável das suas economias e sociedades;
- Informar e apoiar a domesticação da política continental por parte dos países africanos;
- garantir que os dados possam fluir através das fronteiras o mais livremente possível, promovendo simultaneamente uma distribuição equitativa dos benefícios e abordando os riscos relacionados com violações dos direitos humanos e outros interesses legítimos de Estados como o combate ao branqueamento de capitais, a evasão fiscal, os jogos virtuais, a segurança nacional,.
- promover e facilitar os fluxos de dados transfronteiriços e aumentar as oportunidades de negócio, assegurando simultaneamente um nível adequado de dados pessoais e privacidade;
- Estabelecer mecanismos de confiança colaborativos que permitam a circulação dos dados o mais livremente possível entre os Estados-membros, preservando simultaneamente a soberania dos Estados-membros e a sua capacidade de regular a economia digital
- permitir que os Estados, o sector privado, a sociedade civil e as organizações intergovernamentais coordenem os seus esforços em matéria de dados em todo o continente para realizar um mercado único digital e competir de forma mais eficaz na economia global;
- permitir a competitividade na economia global através de uma cooperação estreita e sustentável por parte dos Estados africanos, do sector privado e da sociedade civil, através de oportunidades de reestruturação para optimizar os benefícios da comunicação de dados da economia e da sociedade.
- garantir que os dados sejam utilizados de forma sustentável, que beneficie a sociedade no seu conjunto e não prejudique a privacidade, a dignidade e a segurança das pessoas;
- garantir que os dados estão amplamente disponíveis no âmbito de salvaguardas adequadas para utilização comercial e não comercial; e.
- facilitar formas inovadoras de promover benefícios públicos, utilizando os dados de novas formas que permitiriam aos dados em África compreender o valor dos dados na tomada de decisões do sector público, planeamento, e monitorização e avaliação.

Para permitir à política de dados continental cumprir os seus objectivos previstos e reflectir os interesses de todas as partes interessadas, **a formulação do quadro político é fundamentada por iniciativas e documentos anteriores**, tanto de dentro como de fora de África. Dentro das limitações do tempo disponível, o processo incluiu uma consulta pública aberta. As contribuições feitas através desta consulta virtual e de um webinar público contribuíram para o desenvolvimento do projecto de quadro político.

A CUA coordenou o desenvolvimento do Quadro Continental de Política de Dados em colaboração com organizações pan-africanas e agências e instituições especializadas da UA, nomeadamente: Comunidades Económicas Regionais, AUDA-NEPAD, Secretariado da África Inteligente, Banco Africano de Desenvolvimento, a União Africana de Telecomunicações (ATU), a Comissão Económica das Nações Unidas para África, a União Internacional das Telecomunicações (UIT), a União Internacional de

Telecomunicações, o Conselho das Nações Unidas sobre Comércio e Desenvolvimento (CNUCED), o Banco Mundial bem como outras instituições parceiras.

Além disso, um seminário de validação com peritos dos Estados-membros foi convocado pela CUA nos dias 1-2 de Setembro de 2021. Os Estados-membros da UA validaram então o projecto de estratégia com alterações para apreciação e adopção pelos Ministros da Comunicação da UA em Outubro de 2021.



3. Aumento da Economia de Dados - A necessidade de Repensar a Política

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

3.1. Dados como base para um novo contrato social e economia da inovação

Os dados em e de si mesmos têm tipicamente pouco valor. É somente através do processamento, transmissão, armazenamento e combinação que o valor é adicionado. Em termos económicos, os dados podem ser entendidos como um bem público na medida em que são inerentemente não rivais (a nível técnico, são infinitamente utilizáveis sem diminuir a capacidade de outra pessoa de os utilizar). É, naturalmente, não susceptível de exclusão, o que significa que não existem barreiras naturais para várias pessoas que utilizem os mesmos dados de uma só vez. Embora haja tentativas de tornar os dados não susceptíveis de exclusão por meio tecnológico e, às vezes, legal, não são características inerentemente dos dados. As tentativas de limitar o acesso, para fins de comercialização ou segurança, podem ser regulamentadas como não susceptíveis de exclusão. Por exemplo, os dados abertos ao abrigo de uma licença reconhecida internacionalmente ou as estatísticas públicas podem ser regulados para serem acessíveis como a radiodifusão pública gratuita, como o bem público clássico.

Os dados também não geram valor automaticamente. Em vez disso, existem diferentes utilizações de dados e diferentes métodos para medir o valor económico e social dos fluxos de dados (OCDE, 2019b). No sentido económico, é o que as empresas fazem que conduz à criação de valor, tanto internamente na empresa como externamente, através da rede de dados alargada. Teoricamente, este valor pode ser quantificado através da atribuição de valor monetário tendo em consideração várias variáveis geradoras de custos e rendimentos, tais como a forma como as organizações cobram pelos dados gerados pelos utilizadores, ou a reconciliação dos custos de gestão de dados, tais como a recolha, manutenção e publicação de dados. A valorização dos dados a partir de uma perspectiva de benefícios socioeconómicos – ou valor de dados não baseados no mercado – surge quando existem condições fundamentais ou factores que permitem que os

governos forneçam serviços públicos mais eficazes, ofereçam uma gestão ambiental eficaz, e quando os cidadãos vivem vidas mais saudáveis e economicamente seguras através da alavancagem dos dados (Banco Mundial, 2021). Exemplo de criação de valor de dados públicos inclui o uso de dados para fundamentar as necessidades de alocação de recursos para melhorar a prestação de serviços.
Estas características dos dados foram enquadradas em outros lugares como **o potencial dos dados para fornecer a base de um novo contrato social** (Banco Mundial, 2021). A formulação de orientações políticas a partir desta abordagem enfatiza a necessidade de dados abertos, normas de interoperacionalidade e iniciativas de partilha de dados para aproveitar o potencial dos dados para impulsionar o desenvolvimento; assegurar uma melhor distribuição dos benefícios dos dados; fomentar a confiança através de salvaguardas que protejam as pessoas dos danos da má utilização dos dados; criar e manter um sistema nacional integrado de dados que permita o fluxo de dados entre um vasto leque de utilizadores de uma forma que facilite a utilização e reutilização seguras dos dados.

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

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

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

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

3.2 Necessidade de um valor que crie a governação dos dados, evitando danos

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

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

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

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

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

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

Capacidade institucional interna - Atribuição de obrigações, responsabilidades e poderes aos actores institucionais a nível nacional que podem ajudar a criar um ambiente interno consistente para que as comunidades de dados (públicas e privadas) possam instituir actividades de dados.

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

Apoio político - Fornecer normas e soluções implementáveis que se concentrem na consecução de uma qualidade saudável dos dados nacionais, controlo, acesso e interoperacionalidade, processamento e protecção, e segurança como meio para o crescimento de uma economia de dados.

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

4. Contexto

4.1. Visão geral das tendências da política regional internacional e da legislação

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

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

O RGPD 2016/6 da UE é amplo, com uma definição abrangente do que são os dados pessoais. O seu vasto âmbito territorial aplica-se dentro e fora da UE, contém graves sanções para subverter o regulamento, requer uma abertura e transparência consideráveis e, acima de tudo, concede aos indivíduos direitos substanciais que podem ser aplicados contra as empresas. Esta abordagem à protecção de dados está centrada em torno de uma agenda de direitos humanos no ecossistema digital.

O Quadro de Privacidade da APEC, aplicado desde 2005 pelos Estados-membros da APEC, é constituído por um conjunto de princípios, que são criados para garantir o livre fluxo de informações em apoio do desenvolvimento económico. O quadro da APEC adopta uma abordagem diferente à protecção de dados, alinhando o mandato do quadro com a promoção do comércio e do investimento, em vez da protecção dos direitos humanos básicos como no PIBR da UE. Um importante destaque do quadro é a forma como sublinha que os regulamentos de privacidade devem ter em consideração a importância dos interesses empresariais e comerciais, para além das culturas e outras diversidades das economias dos Estados-membros.

A Parceria Trans-Pacífica Abrangente e Progressiva (CPPP) centra-se no comércio aberto e na integração regional entre os Estados-membros. O acordo permite a transferência transfronteiriça de informações por meios electrónicos, incluindo informações pessoais, quando esta actividade é "para a realização de actividades".

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

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

4.2 Política africana e contexto legislativo

De acordo com os precedentes internacionais, a maioria dos esforços na regulamentação de dados no continente tem-se concentrado na protecção de dados, com o principal objectivo de observar e salvaguardar os direitos de privacidade dos utilizadores da Internet. Embora a utilização e o processamento de dados seja uma preocupação transversal, que tem impacto numa série de áreas de política tradicionalmente em silos, não existem exemplos de leis-quadro que regulem todos os aspectos dos dados. Em vez disso, os dados foram regulamentados em cinco ramos da lei: lei de protecção de dados, lei da concorrência, lei de segurança cibernética, lei das comunicações e transacções electrónicas e lei da propriedade intelectual, que potencialmente entram em conflito nalguns casos e deixam lacunas noutros.[36]

Estima-se que **32 dos 55 países africanos tenham promulgado ou adoptado alguma forma de regulamentação com o objectivo principal de proteger dados pessoais**.[37] Regionalmente, instrumentos legislativos como o Quadro Comunitário das Leis Cibernéticas da África Oriental de 2008, a Lei Complementar de 2010 relativa à protecção de Dados Pessoais da Comunidade Económica dos Estados da África Ocidental (CEDEAO), e a lei-modelo da Comunidade de Desenvolvimento da África Austral de 2013 que harmoniza as políticas para o mercado das TIC na África Subsariana foi desenvolvida. Continuamente, a União Africana desenvolveu o primeiro quadro Pan-africano com a Convenção da União Africana sobre Segurança Cibernética e protecção de Dados Pessoais (Convenção de Malabo) em 2014, que não entrou em vigor, mas está actualmente a ser ratificada.

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

Outras iniciativas importantes no continente em matéria de política de dados

A Iniciativa de Política e Regulação para a África Digital (PRIDA) é uma iniciativa conjunta da União Africana (UA), da União Europeia (UE) e da União Internacional de Telecomunicações (UIT), que aborda várias dimensões da procura e da oferta de banda larga em África e o reforço das capacidades dos Estados-membros da UA no espaço de Governação da Internet com o objectivo de permitir que o continente africano colha os benefícios da digitalização. O projecto do PRIDA procura melhorar o nível de harmonização das TIC & Política de Telecomunicações, quadros jurídicos e regulamentares em África, reforçar a cooperação entre as Autoridades Reguladoras Nacionais de Telecomunicações (ARN) e a Associação Regional de Reguladores, bem como sensibilizar e consciencializar os decisores políticos africanos, decisores, autoridades públicas e sociedade civil para as questões transversais e para a crescente utilização das TIC em todos os sectores. A PRIDA apoia a monitorização e o desenvolvimento de mecanismos de harmonização jurídica, incluindo a protecção de dados. O objectivo geral do PRIDA é criar um ambiente político favorável e condições regulamentares que apoiem e facilitem a Transformação e Integração Digital de África.

[36] As dimensões continentais destes desafios são abordadas através da colaboração digital a nível continental.
[37] https://privacyinternational.org/long-read/3390/2020-crucial-year-fight-data-protection-africa

A África Inteligente *apoia a criação de um quadro harmonizado para políticas e regulamentação da protecção de dados em África e mecanismos de colaboração e confiança intercontinentais através do Grupo de Trabalho para a Protecção de Dados da África Inteligente. O Grupo de Trabalho irá proceder a um levantamento dos quadros jurídicos, orientações de implementação para os Estados-membros e recomendações sobre harmonização e mecanismos de colaboração entre as Autoridades de Protecção de Dados (APD). A África Inteligente está a apoiar a criação de um quadro harmonizado para as políticas e regulamentação da protecção de dados em África através do Grupo de Trabalho sobre Protecção de Dados "SMART Africa"*

4.3 Análise situacional para a economia de dados em África

A realização de uma análise situacional para todo o continente com os seus diversos sistemas jurídicos, regulamentares e políticos, e considerando o desequilíbrio do desenvolvimento económico e da prontidão digital dos países, torna-a inerentemente limitada e excessivamente generalizada. O objectivo da análise SWOT de alto nível é identificar os pontos fortes e fracos amplamente aplicáveis dos países a nível regional e identificar as potenciais oportunidades e riscos conhecidos associados aos processos globais de digitalização e publicação de dados que caracterizam o desenvolvimento da economia de dados para todos os países, mas também o que estes significam especificamente para os países africanos, dentro do seu contexto de desenvolvimento mais amplo.

PONTOS FORTES	PONTOS FRACOS
• Instrumentos de governação de dados regionais fundacionais • Comunidades Económicas Regionais (CER) para apoiar os aspectos económicos das iniciativas de política de dados • Tribunais regionais e continentais para permitir a resolução harmonizada de litígios • Centros de inovação emergentes na região para demonstrar as melhores práticas em todas as jurisdições • Pouca e menos desenvolvida concorrência, dados e leis de PI sobre os dados, com um maior potencial para uma rápida e precoce harmonização continental das leis que permitem o comércio transfronteiriço	• Conectividade e utilização de dados subaproveitada • Regime de governação de dados não harmonizado • Inconsistências no tratamento de dados nas leis de protecção de dados, concorrência e propriedade intelectual nos países • Regras de localização que limitam o fluxo transfronteiriço de informações necessárias à criação de valor local e ao estabelecimento do mercado único • Restrições de recursos na evolução e implementação de quadros de governação de dados • Infra-estrutura de dados inadequada • Insuficiência de dados governamentais abertos para satisfazer a procura de dados • Fornecimento inadequado, ou acesso a dados de qualidade • Desenvolvimento desigual das normas de dados. • Baixa penetração do Número limitado de Autoridades de Protecção de Dados (APD), muitas das quais não dispõem de recursos suficientes e/ou não dispõem de plenos poderes) • Necessidade de capacidade de segurança cibernética

OPPORTUNITIES	THREATS/RISKS
• Se forem cumpridas as condições prévias e criados ambientes facilitadores, há oportunidades para a criação de valor, tanto para os dados públicos como privados, através de melhores fluxos de informação e eficiências.	• Incapacidade de alguns países para superar os desafios de criar ambientes favoráveis necessários para a realização das oportunidades • Falha na harmonização dos quadros políticos e regulamentares para permitir economias de escala

• Utilização de dados para um melhor planeamento público e prestação de serviços e coordenação dos sectores público e privado • Com dados abertos e normas interoperacionais subjacentes ao sistema nacional integrado de dados, as barreiras à entrada no mercado podem ser reduzidas e as oportunidades para o desenvolvimento empresarial e a inovação • Esforços globais para desenvolver e harmonizar a política de dados e os quadros de governação • Esforços globais para coordenar a tributação dos serviços digitais e de dados que, em grande parte, não têm contribuído para os esforços de mobilização de recursos nacionais. • Oportunidades de trabalho emergentes para jovens com conhecimentos tecnológicos, para melhorar o empreendedorismo local, o desenvolvimento de conteúdos locais e a inovação.	e de âmbito para a criação de valor de dados e para que todos os países possam usufruir dos benefícios de um mercado digital comum. • Protecção de dados e riscos de privacidade em constante mudança • Risco de tomada de decisão automatizada discriminatória (baseada em algoritmos) resultante da invisibilidade, subrepresentação de categorias de pessoas em conjuntos de dados e deficiências de modelação de algoritmos • Concentração nos mercados globais de dados, impedindo a concorrência leal nos mercados locais • Níveis inadequados de cooperação política internacional necessários para lidar com questões de dados globais - acesso, integridade, segurança, equidade, direitos e ética.

4.4. Desafios políticos emergentes na realização de oportunidades e na atenuação de riscos

A distribuição desigual das oportunidades e riscos associados ao desenvolvimento da economia de dados correlaciona-se em grande parte com os níveis de desenvolvimento humano e económico dos países e com as desigualdades entre e dentro dos países. Estes reflectem-se nos pontos fortes e fracos acima salientados. A capacidade dos países e regiões em África para contrariar estas tendências depende da sua **capacidade de criar um ambiente propício à criação de valor orientado para os dados, que seja inclusivo e equitativo**. O objectivo do Quadro de Política de Dados é fornecer um quadro para os países superarem alguns dos desafios da formulação de políticas nesta área dinâmica e em rápida mudança através de um objectivo comum e de uma acção colectiva. Através da criação de um ambiente favorável harmonizado, os pontos fortes dos países podem ser aproveitados e os pontos fracos podem ser mitigados para o desenvolvimento de uma economia de dados continental integrada muito mais poderosa do que as suas partes individuais.

Os desafios políticos que devem ser ultrapassados para criar um ambiente propício à realização das oportunidades oferecidas pelos processos globalizados de digitalização e dataficação e para mitigar eficazmente os riscos identificados para países de todo o mundo não devem ser subestimados. Estes são actualmente objecto de vários relatórios de organizações multilaterais (CNUCED 2021, Banco Mundial 2021). Embora alguns dos desafios estejam relacionados com a criação de condições para a criação de valor orientado para os dados a nível nacional que são destacados na análise situacional acima e discutidos abaixo, a natureza internacional e transfronteiriça dos dados como bens públicos globais exige mais do que nunca uma **cooperação regional e global** para que sejam realizados a nível nacional e para mitigar os riscos associados que possam surgir da utilização de dados para além das fronteiras nacionais. Embora o quadro de política de dados forneça um quadro de alto nível para os países desenvolverem políticas nacionais, estas devem basear-se em processos consultivos nacionais que tenham em conta o contexto local, as necessidades e os dotes institucionais dos países.

Ao criar este ambiente favorável nos Estados-membros da União Africana e na região, são assinaladas as seguintes considerações resultantes da análise situacional que podem ter impacto na capacidade do país para responder às necessidades de uma nova economia de dados.

A digitalização e a publicação de dados atravessa os sectores público e privado, a economia formal e informal e as esferas social e cultural, e requer uma mudança das políticas sectoriais tradicionais. A política para a

economia e sociedade digital e de dados precisa de ser transversal para coordenar actividades em todo o sector público e entre os sectores público e privado para cumprir objectivos nacionais e regionais. Ao mesmo tempo, é importante considerar as **políticas sectoriais específicas de dados** para optimizar e salvaguardar as diversas utilizações de diferentes tipos de dados (por exemplo, dados de saúde ou dados climáticos). Para além da observação deste princípio, o desenvolvimento efectivo das várias políticas sectoriais que terão de ser desenvolvidas está para além do âmbito deste quadro de alto nível. **Uma regulamentação eficaz dos mercados globalizados cada vez mais complexos é essencial** para a espinha dorsal omnipresente e serviços sem descontinuidades necessários para que os serviços e aplicações de dados possam ser utilizados para satisfazer as diversas necessidades económicas e sociais, melhorar a concorrência e promover a inovação africana. Tal como em países de todo o mundo, os decisores políticos terão de rever e renovar os acordos institucionais para a governação da economia de dados. Os reguladores especializados, tais como reguladores de dados ou de informação, são necessários para lidar com novas questões de governação de dados, e tanto os reguladores novos como os estabelecidos terão de se empenhar em níveis elevados de coordenação nacional e regional. Para assegurar que o mercado único africano se torne operacional, a harmonização regulamentar é também essencial para a integração dos mercados, juntamente com os sistemas comuns de pagamento em linha e a facilitação do comércio transfronteiriço e a normalização dos impostos e taxas transfronteiriças. Os Estados africanos precisarão de se reunir e desenvolver posições comuns para assegurar resultados mais favoráveis em fóruns de governação global, a fim de melhor servir os interesses africanos.

A política transversal digital e de dados pode gerir a importante interacção entre concorrência, comércio e tributação numa economia de dados. Isto representa uma oportunidade para os Estados africanos coordenarem políticas sectoriais de apoio a uma florescente economia de dados. Para muitos países africanos, um risco que precisa de ser mitigado desde cedo é a tendência para a concentração do mercado e a criação desigual de riqueza devido a efeitos de rede indirectos associados a economias de escala e de gama. Os mercados digitais impulsionados por dados são propensos a "ganhar tudo". Entre outros factores, a hiper-globalização e a interdependência digital contribuem para a monopolização. Isto acaba por afectar a concorrência local e inibe a competitividade global dos ecossistemas de dados domésticos. Os desafios da concentração do mercado, da interdependência digital, e da distribuição desigual da riqueza, particularmente da erosão da base e da transferência de lucros, criam a possibilidade de incentivos que encorajam uma maior integração entre as prioridades de reforço mútuo das estratégias políticas geralmente em silos na concorrência, no comércio e nos impostos. Devido à importância crescente da governação regional e global, as comunidades económicas regionais têm um papel importante a desempenhar na implementação da política regional de dados através de leis-modelo e no apoio à criação de capacidades institucionais e humanas.

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

É necessária clareza e certeza jurídica sobre as questões de dados emergentes na transformação digital sustentável e de confiança. Um desafio global é que a natureza dos fluxos de dados e da infra-estrutura

digital, ameaça a soberania dos dados domésticos. Exercer o controlo dos dados para salvaguardar a soberania requer infra-estruturas e legislação, mas também a capacidade técnica para o fazer de uma forma que possa criar confiança. As políticas transversais proporcionam uma oportunidade de certeza em questões como a apropriação ou custódia de dados e direitos conexos, ao mesmo tempo que estabelecem um sistema abrangente de supervisão sobre o acesso e aquisição, e a análise, armazenamento e divulgação de dados tanto pessoais como não pessoais. Assegurar a protecção do consumidor, permitindo simultaneamente a inovação, é igualmente fundamental para o desenvolvimento económico e a inclusão. Além disso, porque diferentes abordagens jurídicas sectoriais servem interesses diferentes, é dada aos países a oportunidade de reinventar um sistema jurídico harmonizado que equilibre adequadamente os interesses empresariais e os direitos digitais relevantes.

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

Apesar de vários países introduzirem sistemas de identificação digital, os **sistemas de identificação digital omnipresentes e interoperacionais continuam a ser um grande desafio socioeconómico no continente.** Os sistemas de identificação digital permitem a identificação para efeitos de transacção e interacção num ecossistema de dados fiável. A identidade fundacional e funcional facilita os serviços digitais, mas a cobertura completa da identidade fundacional em particular continua a ser um desafio social e económico. Os quadros regionais emergentes sobre identidade digital estão a começar a envolver-se directamente neste desafio. Há oportunidades para que a identidade descentralizada e funcional seja incorporada nos quadros de protecção de dados. Estes podem proporcionar identidade funcional, reduzindo ao mesmo tempo os riscos associados aos dados pessoais.

SMART AFRICA - Identidade Digital

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

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

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

Os países africanos enfrentam vários desafios bem documentados e inter-relacionados no que diz respeito aos seus níveis desiguais de **prontidão digital** (União Internacional das Telecomunicações, 2019; Fórum

Económico Mundial, 2016) que têm um impacto variável na sua capacidade de responder aos desafios nacionais e globais. Estes incluem a elaboração pontual de políticas e legislação, desafios em torno da harmonização regional de políticas, falta de capacidade institucional, a concorrência ineficazmente regulada entre fornecedores de serviços, baixos níveis de cobertura, acessibilidade e qualidade da conectividade de banda larga (Gillwald & Mothobi, 2019; Hawthorne, 2020).

Apesar da adopção de cartas continentais, convenções e leis-modelo de comunidades económicas regionais que tentam harmonizar a **resposta de África aos desafios colocados pela digitalização e dataficação, a ratificação e implementação das mesmas tem sido variada**. A adopção mais ampla dos fundamentos digitais para iniciativas continentais, tais como a ZCLCA Regras normalizadas sobre fluxos transfronteiriços são um pré-requisito para a concretização dos benefícios previstos da ZCLCA. Isto pode ser feito utilizando a operacionalização do Acordo para facilitar uma melhor interoperacionalidade dos dados transfronteiriços e proporcionar uma abordagem continental harmonizada da economia digital impulsionada pelos dados. Pode ser feito de forma a apoiar os benefícios socioeconómicos do comércio digital e do comércio electrónico, assegurando ao mesmo tempo que a informação sensível permanece segura e que os regulamentos relevantes sobre protecção de dados pessoais são respeitados.

Em resposta a ondas anteriores de inovação tecnológica, económica, reguladora e social associada**, os países africanos tenderam a ser mais tomadores de normas do que criadores de normas**. As organizações multilaterais, da OCDE à Organização Mundial da Propriedade Intelectual e à Organização Mundial do Comércio, estão a reagir aos desafios da governação global de dados. Embora África e os países africanos, com algumas excepções, não tenham liderado políticas digitais globais, existe uma oportunidade para alterar esta situação. As pressões comerciais multilaterais, plurilaterais e bilaterais para permitir o fluxo de dados com poucas restrições são combinadas com pressões para a concessão de direitos de propriedade intelectual sobre dados, de modo a que os países africanos enfrentem a perspectiva de que os dados sejam explorados e apropriados. Na ausência de uma política comum e de um compromisso com padrões comuns em todo o continente, é difícil para a maioria dos países africanos escapar às correntes de uma dinâmica global em rápida mutação. Por conseguinte, é necessária uma acção coordenada por e para África para desbloquear colectivamente o enorme e transformador potencial dos dados para desenvolver uma economia digital africana inclusiva e sustentável e uma sociedade moderna.

Inovação em caso de utilização por comunidades de dados

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

5. Quadro de Política de Dados

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

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

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

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

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

5.1. Princípios Orientadores do Quadro

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

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

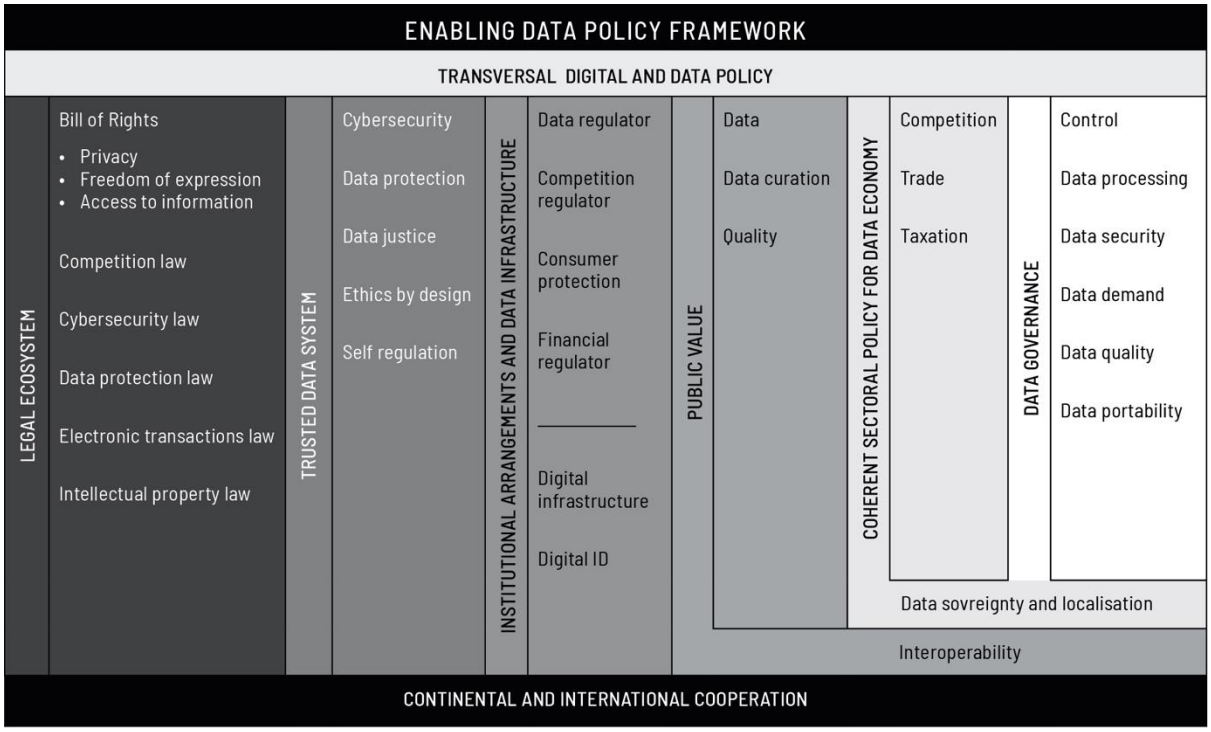
- **Cooperação**: Os Estados-membros da União Africana devem cooperar no intercâmbio de dados, reconhecendo os dados como um contributo central da economia global e a importância da interoperacionalidade dos sistemas de dados para um próspero mercado único digital africano;
- **Integração**: o Quadro promoverá os fluxos de dados intra-africanos, eliminará as barreiras jurídicas ao fluxo de dados, apenas sob reserva da segurança necessária, dos direitos humanos e da protecção de dados;
- **Equidade e inclusão:** na implementação do Quadro, os Estados-membros devem garantir que este seja inclusivo e equitativo, oferecendo oportunidades e benefícios a todos os africanos e, ao fazê-lo, procurar corrigir as desigualdades nacionais e globais, respondendo às vozes das pessoas marginalizadas pelos desenvolvimentos tecnológicos;
- **Confiança, segurança e responsabilização**: Os Estados-membros devem promover ambientes de dados dignos de confiança que sejam seguros e protegidos, responsáveis perante as pessoas em causa, e éticos e seguros por concepção;
- **Soberania**: Os Estados-membros, CUA, CER, Instituições Africanas e Organizações Internacionais devem cooperar para criar capacidade que permita aos países africanos auto-gerirem os seus dados , tirarem partido dos fluxos de dados e governarem adequadamente os dados
- **Abrangente e virado para o futuro**: o quadro permitirá a criação de um ambiente que incentive o investimento e a inovação através do desenvolvimento das infra-estruturas, da capacidade humana e da harmonização dos regulamentos e da legislação; e;
- **Integridade e justiça**: Os Estados-membros devem assegurar que a recolha, tratamento e utilização dos dados é justa e lícita, e os dados não devem ser utilizados para discriminar injustamente ou infringir os direitos dos povos.

5.2. Definição e Categorização de Dados

Não há acordo sobre como os dados são definidos, provavelmente como resultado dos muitos tipos diferentes de dados colectados e usados e seus diferentes propósitos e valores. Não há acordo sobre como os dados são definidos, provavelmente como resultado dos muitos tipos diferentes de dados que são recolhidos e utilizados, e das suas finalidades e valores variáveis. Uma melhor medição dos dados e fluxos de dados e do seu papel na produção e cadeias de valor também ajudará a apoiar a elaboração de políticas.

5.2.1 Dados pessoais e não pessoais

Embora os dados, conceptualmente, signifiquem aspectos diferentes para comunidades diferentes e dependendo do contexto, um conceito importante que está no cerne do regulamento de protecção de dados, é o de dados pessoais. A definição de tipos específicos de dados como pessoais pode ajudar as autoridades de protecção de dados a proteger os direitos das pessoas em causa de forma mais eficiente, mas existem limites a esta abordagem.



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

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

5.3. Factores impulsionadores do valor na economia de dados

O aproveitamento dos benefícios dos dados depende em grande medida de permitir quadros regulamentares e políticos que facilitem a obtenção de dados úteis; reforçar as capacidades humanas,

institucionais e técnicas para criar valor a partir dos dados; incentivar a partilha e a interoperacionalidade dos dados; e aumentar a legitimidade e a confiança pública no Estado para gerir os dados dos cidadãos de uma forma responsável. Além disso, a infra-estrutura de dados que permite um sistema de dados integrado é um recurso estratégico fundamental para os países. O ambiente criado pela interacção de elementos no ecossistema de dados e a natureza das relações e processos não lineares entre eles e dentro deles, determinam as intervenções para criar incentivos aos investimentos tecnológicos que são necessários para impulsionar o crescimento da economia de dados. Estas condições são moldadas pela estrutura do mercado, a competitividade dos serviços que dele resultam e a eficácia com que o mercado é regulado.

A economia digital abrange várias indústrias e actividades sociais, e a política de dados deve ser localizada no contexto do ecossistema digital complexo e adaptativo mais vasto. Tal como abordado, isto tem implicações para outras áreas políticas, incluindo comércio e tributação. Os Estados devem investir em capacidades de dados e activos complementares para apoiar a política m Os investimentos em inovação relacionada com dados e investigação e desenvolvimento (I&D), bem como em capacidades para harmonizar normas, competências e infra-estruturas, podem permitir aos governos desenvolver melhores políticas relacionadas com dados em todos os domínios. As questões de confiança e ética são igualmente importantes, enquanto as regulamentações baseadas em provas e consultivas devem ser consideradas prioritárias.

Recomendações:

Os Estados-membros da União Africana devem promover a investigação, desenvolvimento e inovação em várias áreas relacionadas com dados, incluindo, Grandes Análises de Dados, Inteligência Artificial, Computação Quântica, bem como Blockchain.

Todos os grupos de partes interessadas, incluindo os governos, devem criar capacidades analíticas e de gestão de dados para facilitar a utilização de dados de qualidade e de sistemas interoperacionais de confiança. Contudo, é importante lembrar que em muitos países o maior produtor e colector colectivo de dados é o Estado. Por conseguinte, muitas das observações incluídas na discussão sobre a governação dos dados a seguir apresentadas têm particular relevância para as acções dos governos.

5.3.1 Infra-estrutura de dados de base

5.3.1.1 Acesso e utilização de banda larga e dados

Definição do problema

Existem barreiras de acesso às infra-estruturas de banda larga que impedem as pessoas de aderirem à economia de dados, mesmo como utilizadores. De acordo com a Comissão de Banda Larga da UIT *, que liga África através do Relatório sobre a Banda Larga*:[38] "Cerca de 1,1 mil milhões de novos utilizadores únicos têm de estar ligados para alcançar um acesso universal, acessível e de boa qualidade à Internet de banda larga até 2030, e seriam necessários 100 mil milhões de USD adicionais estimados para alcançar este objectivo na próxima década".

Apesar disto, e de uma diversidade de limitações contextuais, África tem uma posição privilegiada para desenvolver um ecossistema de dados inovador, sendo menos prejudicada pelas infra-estruturas de dados herdadas e tendo uma utilização do espectro e níveis de congestionamento relativamente mais baixos (Saint&Garba, 2016). Enquanto a penetração da banda larga fixa na região é inferior a um por cento, a Internet móvel é mais omnipresente com um custo de

[38] https://broadbandcommission.org/Documents/working-groups/DigitalMoonshotforAfrica_Report.pdf

adopção mais baixo.[39] Por conseguinte, a evolução do ecossistema de dados de África será possibilitada principalmente pelas redes móveis de banda larga.

Recomendação

Para acelerar a domesticação da estrutura, deve haver uma implantação maciça e robusta de infra-estruturas digitais entre os membros da UA, juntamente com uma capacidade suficiente. Os Estados-membros devem dar prioridade à obtenção de uma conectividade significativa e de uma Internet a preços acessíveis, que integre mais utilizadores e impulsione a procura de serviços de infra-estruturas. Para uma utilização mais eficaz dos dados na região, é necessário resolver os défices de infra-estruturas complementares que limitam a utilidade dos dados.

Acções

Os Estados-membros terão de desenvolver políticas que:

- banir as taxas proibitivas do "direito de passagem" dos cabos de banda larga e a partilha de infra-estruturas de apoio;
- impedir práticas anticoncorrenciais decorrentes de uma posição dominante nos mercados de infra-estruturas;
- investir em Wi-Fi público e tecnologias complementares;
- adoptar técnicas inovadoras de utilização do espectro, tais como a atribuição e acesso dinâmicos ao espectro, e o aproveitamento de espaços brancos de televisão (na sua maioria espectro não utilizado, em grande parte acelerado pela migração da radiodifusão analógica para a digital) para expandir o acesso em banda larga para as zonas rurais mal servidas;
- Promover a transição e a adopção do IPv6[40], à medida que os recursos de IPv4 se tornam mais esgotados globalmente;
- investir na espinha dorsal nacional e em infra-estruturas de conectividade transfronteiriça, tais como Pontos de Intercâmbio da Internet (IXP), tanto a nível nacional como regional, para potenciar a largura de banda internacional disponível, reduzir os custos de acesso à Internet e aumentar as velocidades de acesso aos dados na região; e
- aproveitar modelos inovadores para o financiamento da infra-estrutura de dados.

5.3.1.2 Infra-estrutura de dados

Definição do problema

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

As infra-estruturas de dados fundacionais referem-se a uma vasta gama de tecnologias que facilitam a utilização intensiva de dados de qualidade, incluindo infra-estruturas duras e suaves que abordam os défices de infra-estruturas TIC "tradicionais" existentes, terão de ser feitas em paralelo com a criação de uma arquitectura para apoiar o aumento da informação de dados. Também inclui recursos de infra-estruturas tais como a Identificação Digital para permitir transacções e presença virtual seguras. Este quadro centrar-se-á em três aspectos de infra-estruturas de dados que requerem considerações políticas

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

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

que se reforçam mutuamente e também influenciam a governação dos dados: serviços na nuvem, grandes e dados e estratificação.

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

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

Serviços em nuvem

É útil para efeitos de política distinguir entre “serviços na nuvem” e “serviços baseados na nuvem”. O principal benefício oferecido pelos serviços de nuvem é a poupança de custos através de uma maior eficiência dos sistemas. Por exemplo, o sector público com recursos limitados e as pequenas, médias e microempresas (PME's) podem reduzir as despesas de capital em equipamento de TI, incluindo servidores internos, equipamento de rede, recursos de armazenamento e *software*, mudando para um modelo de serviços em nuvem baseados em serviços de utilidade pública.

A interoperacionalidade no fornecimento de nuvens é um factor crítico, pois permite flexibilidade e permite aos utilizadores alternar entre um fornecedor de nuvens e o outro. Outros benefícios da computação em nuvem incluem a redução das despesas com o consumo de energia, bem como uma menor procura de gestão e manutenção dos sistemas, transferindo a gestão dos recursos informáticos para terceiros. Consequentemente, os fundos podem ser desviados para actividades orientadas para o cliente e para uma melhor prestação de serviços públicos. No entanto, como existem certos factores que apoiam um ambiente favorável aos serviços baseados na nuvem, a adopção de novas tecnologias deve ser feita em paralelo com a abordagem dos desafios da fractura digital estrutural (capital humano, infra-estruturas, etc.). Estes processos devem reforçar-se mutuamente e ser adequados às realidades económicas dos Estados-membros.

Grandes dados

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

Platformização

A comunicação de dados criou igualmente modelos empresariais e modos de criação e extracção de valor inteiramente novos. Uma delas é a "platformisação", que facilita as transacções e o trabalho em rede, bem como a troca de informações, agregando múltiplos vendedores e compradores numa única plataforma.

Com o comércio digital e as plataformas de comércio electrónico cada vez mais subjacentes à actividade global e transfronteiriça, a integração de áreas tradicionalmente distintas de regulamentação e prioridades políticas tornou-se cada vez mais importante e entrelaçada para além das fronteiras geográficas. No entanto, políticas como a localização de dados não serão plausíveis sem os requisitos estruturais e institucionais necessários para a sua evolução e implementação efectivas, em particular a referência às capacidades digitais.[41]

Recomendações

A utilização de dados como instrumento para melhorar os interesses públicos exigirá que os Estados reforcem as infra-estruturas de dados nacionais e necessitará de um forte envolvimento das partes interessadas a nível nacional, regional e global. O desenvolvimento de quadros abrangentes de política de dados facilitadores deve ser acompanhado de estratégias de implementação sensíveis ao tempo através de diferentes mandatos internos para assegurar a responsabilização e a transparência. Os Estados-membros devem dar prioridade aos recursos para assegurar que existem incentivos para aumentar os investimentos em infra-estruturas digitais, plataformas de dados, e capacidades de *software* para aproveitar os grandes dados. Os investimentos em infra-estruturas de dados devem apoiar o contrato social digital. Os esforços do Estado para melhorar a interoperacionalidade, a qualidade e a administração pública de dados devem também complementar e melhorar, tanto quanto possível, os sistemas digitais públicos, tais como as identificações digitais, os pagamentos digitais, e os fluxos de dados abertos.

Acções

- Em vez de se concentrarem no investimento inicial significativo para substituir o equipamento de TIC obsoleto, os Estados-membros devem tirar partido das economias de escala e de gama para adoptar infra-estruturas que apoiem benefícios facilitadores oferecidos pelos serviços em nuvem e outras novas tecnologias que apoiam a criação de valor dos dados.
- As políticas fiscais, comerciais (incluindo investimento e inovação) e de concorrência devem ser coerentes, complementares e adaptadas à economia digital orientada para os dados, em particular para informar as estratégias de desenvolvimento de infra-estruturas.
- Adoptar modelos de produção de electricidade mais sustentáveis, a nível interno e em toda a região, para assegurar que a infra-estrutura digital fundacional apoie actividades de dados domésticos e transfronteiriços sustentáveis que tenham menos impactos extractivos no ambiente natural.

Governação de dados

- Criar direitos de portabilidade de dados - inclusive para dados não pessoais, para facilitar aos clientes de serviços em nuvem a troca entre provedores.
- Desenvolver normas contratuais para organizações públicas (que também podem ser utilizadas pelas PME), que protejam os seus direitos de acesso, recuperação, eliminação, etc. Os dados (incluindo dados não pessoais, novamente) que são processados por fornecedores de nuvem.
- Desenvolver obrigações de licenciamento justas, razoáveis e não discriminatórias (FRAND) para plataformas e fornecedores de nuvem que tenham acesso a conjuntos de dados que se tornem um recurso vital para entrar no mercado.

[41] Andreoni, A., & Tregenna, F. (2020). Escapar à armadilha da tecnologia de rendimento médio: Uma análise comparativa das políticas industriais na China, Brasil e África do Sul. Mudança estrutural e dinâmica económica, 54, 324-340.

5.31.3 Identificação Digital

Definição do problema

Com o continente africano a acolher a percentagem mais elevada de pessoas sem identidade legal e subsequentemente descoberta pelo registo civil e negados serviços sociais essenciais oferecidos pelos Estados, tais como cuidados de saúde, educação básica ou serviços alimentares[42]. A economia digital, contudo, oferece oportunidades para corrigir desigualdades tais como exclusões socioeconómicas e estruturais sofridas por grupos minoritários no continente.

A identificação digital (Digi-ID), como forma de expressão de dados pessoais, deve ser construída e implementada de forma coesa, em conformidade com os quadros gerais de governação de dados. A Digi-ID é facilitadora tanto para fins do sector privado como do sector público numa economia de dados, mas exige um sólido quadro de confiança para mitigar os potenciais danos, como o abuso de dados pessoais, a exclusão, ou a discriminação baseada na representação incorrecta (ou não) de dados, que podem acometer iniciativas deste tipo. Além disso, embora as parcerias público-privadas tenham o potencial de expandir a prestação de serviços estatais ao público e impulsionar a inovação sócio-empresarial, tais colaborações podem potencialmente exacerbar a desigualdade (através da má utilização dos dados) para além dos danos acima mencionados. Os quadros adoptados pelas autoridades/agências nacionais de identidade existentes devem, por conseguinte, ser revistos para reflectir estas oportunidades, riscos e danos.

Recomendações

Um sistema de identificação digital (DigiID) justo e fiável é um pré-requisito central para combinar e redireccionar dados administrativos públicos com outros tipos de dados em vários casos de utilização. As actividades de política de dados regionais devem alinhar-se com as que ocorrem no âmbito de actividades simultâneas da Digi-ID. As iniciativas de identificação digital do sector público devem permanecer orientadas por quadros de governação de dados, sejam eles fundacionais ou funcionais[43].

.3.2 Criação de sistemas de dados legítimos e fiáveis

Definição do problema

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

A confiança nas transacções de dados, dados estatísticos e tomada de decisões com base em dados deve, portanto, ser sustentada por um quadro jurídico e regulamentar transparente e sólido que simultaneamente proteja contra danos de dados e apoie estimuladores que facilitem o acesso aos dados,

[42] https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity

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

partilha de dados e alterações de dados de uma forma responsável. Um forte quadro de confiança, e a capacidade institucional para apoiar este quadro, permitirá aos governos criar valor a partir dos dados, minimizar as assimetrias de dados entre os sectores público e privado, e refrear comportamentos não competitivos nos ecossistemas de dados (Macmillan, 2020).

Neste contexto de construção de um ecossistema digital de confiança, três áreas-chave inter-relacionadas necessitam de consideração específica: segurança cibernética, criminalidade cibernética, e protecção de dados. O papel da concepção ética e da regulamentação positiva para assegurar resultados de justiça também merece destaque.

5.3.2.1 Segurança Cibernética

À medida que a tecnologia evolui e tecnologias perturbadas são adoptadas, novas ameaças e riscos indesejados são criados. Isto não só tem impacto nos bens, infra-estruturas e redes, mas também nas economias, sociedades, e pessoas, sendo os mais vulneráveis os mais afectados. Por este motivo, a utilização de tecnologias disruptivas e as normas, regras e práticas dos sectores público e privado para governar a segurança, podem ter impacto nos direitos fundamentais das pessoas de equidade, dignidade e segurança.

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

5.3.2.2 Criminalidade cibernética

O ecossistema de dados destaca tanto as oportunidades como os riscos de uma vasta rede de sistemas públicos e privados interligados. Devido à natureza transnacional da criminalidade cibernética e das operações cibernéticas, a política de segurança de dados é, na sua maioria, moldada em fóruns multilaterais globais ou regionais. Embora a participação africana nestes fóruns tenha aumentado, o envolvimento de actores africanos não estatais é ainda limitado. Além disso, um desafio político emergente é avaliar que capacidade é necessária a nível nacional para implementar convenções acordadas a nível regional e global sobre a criminalidade cibernética, e normas cibernéticas voluntárias e não vinculativas.[44]

5.3.2.3 Protecção de dados

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

Embora isto exija o desenvolvimento de instituições e leis de boa governação de dados, estas leis devem igualmente ser sensíveis aos contextos particulares em que estão a ser implementadas. Estas incluem a consideração das realidades e capacidades socioeconómicas e tecnológicas do público. Dito de forma diferente, um quadro de política de dados deve desenvolver políticas e regulamentos capazes de reconhecer as realidades das capacidades e funcionalidades de um cidadão, juntamente com os riscos que

[44] Foram observados défices na capacidade de implementação em cinco dimensões: política e estratégia de segurança cibernética; cultura e sociedade cibernética; educação, formação e competências em segurança cibernética; quadros jurídicos e regulamentares; e normas, organizações e tecnologias.

acompanham os desenvolvimentos digitais e conduzam a uma distribuição desigual de benefícios e danos (Sen, 2001; van der Spuy, 2021).

Por exemplo, com um número significativo de pessoas digitalmente e analfabetas em África, os mecanismos digitais de consentimento informado podem não ser suficientes para proteger os direitos das pessoas. Existe o risco de muitas pessoas utilizarem habitualmente meios digitais para obterem consentimento; tal como seleccionar como um botão ligado a um longo conjunto legal de termos não equivale na realidade a consentimento informado, porque a acção que se pretende constituir consentimento pode não ser um acto informado ou compreendido de todo pela pessoa que o faz. Outros meios de gestão de dados, tais como os fideicomissos de dados, que estão a surgir a nível mundial, que asseguram que os direitos das pessoas sobre os seus dados são respeitados, são discutidos a seguir. Do mesmo modo, o enquadramento dominante da governação de dados é geralmente equiparado à protecção de dados e a protecção de dados à privacidade. É amplamente entendido como um direito individual e um desafio individual. No entanto, há questões de direitos comunitários e colectivos que podem ser importantes para novos conhecimentos no tratamento de questões de interesse público.

5.3.2.4 Justiça de dados

O conceito de justiça de dados promove uma visão mais ampla do que a protecção de dados. Embora um quadro de política de dados que preserve os direitos seja essencial para salvaguardar os direitos das pessoas, as noções individualizadas de privacidade nos actuais quadros normativos de protecção de dados podem não ser suficientes para garantir uma inclusão mais equitativa numa economia de dados confiável. A justiça dos dados é um conceito que tem vindo a ganhar força em resposta à adopção exponencial de tecnologias orientadas por dados em todo o mundo, particularmente a inteligência artificial (GPAI 2021[45], Tyler 2019). Procura garantir que a crescente dependência dos dados, especialmente no que diz respeito à tomada de decisões automatizada, não perpetue as injustiças históricas e as desigualdades estruturais. Aborda a questão da equidade em resposta ao grau em que as pessoas são visíveis, representadas, sub-representadas e discriminadas como resultado da sua produção de dados digitais.

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

Recomendações

Os Estados-membros devem procurar estabelecer um ambiente de dados fiável através da segurança cibernética, da protecção de dados pessoais, do Estado de direito e de instituições capazes, reactivas e responsáveis. Devem estabelecer a confiança na governação de dados e num sistema de dados nacional, assegurando a legitimidade em todo o systemMe. Isso inclui sistemas e padrões que garantem a conformidade do sector público e privado, o próprio governo que adere às regras de protecção de dados pessoais e o governo que compartilha dados públicos.

Acções

- Salvaguardar os direitos humanos fundamentais através do Estado de Direito;

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

- Garantir que os acordos e regulamentos institucionais sejam estabelecidos apenas através de processos inclusivos, consultivos e transparentes;
- Garantir que as instituições responsáveis pela supervisão da utilização de dados, bem como os produtores de dados públicos e privados, sejam responsáveis pela utilização de dados públicos e pessoais para aqueles cujos dados são utilizados.
- Reforçar a cooperação com outras APD para assegurar uma salvaguarda suficiente, a protecção recíproca dos dados pessoais, bem como os direitos digitais individuais e colectivos em todo o continente.
- Reforçar os acordos e actividades de assistência mútua entre Estados para a investigação e acusação da criminalidade cibernética.
- Garantir que as instituições responsáveis pela supervisão do uso de dados pessoais tenham poderes de entrada e inspeção para fins de aplicação de leis e regulamentos de privacidade e proteção de dados.
- Além disso, garantir que o responsável institucional por supervisionar o uso de dados pessoais tenha os seguintes poderes corretivos em relação à correção de violação de aspectos de uso indevido e abuso de dados pessoais:
    - Emita avisos a um controlador de dados ou processador de dados que as operações de processamento pretendidas podem infringir as disposições das leis e regulamentos de proteção de dados relevantes.
    - Repreender um controlador de dados ou processador de dados quando as operações de processamento infringirem as disposições das leis e regulamentos de proteção de dados relevantes.
    - Solicite a um controlador de dados que comunique uma violação de dados pessoais aos titulares dos dados afetados.
    - Impor uma limitação temporária ou definitiva, incluindo a proibição do processamento de dados pessoais.
    - Ordenar a suspensão dos fluxos de dados para um destinatário em um terceiro país ou para uma organização internacional que não forneça proteção adequada semelhante à do país exportador de dados.
- As instituições responsáveis por supervisionar o uso de dados pessoais devem ter poderes para ajudar ou buscar indulgência do tribunal para ajudar uma pessoa que sofreu danos materiais como resultado de uma violação de seus dados pessoais para receber compensação de um controlador de dados ou processador de dados para o danos sofridos.

5.3.2.5 Ética em Dados

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

No entanto, os códigos de ética têm sido criticados como representando os pontos de vista de demografia limitada, definida na sua maioria pelas corporações e tecnólogos. Os códigos éticos podem igualmente aliviar as empresas da responsabilidade regulamentar quando utilizados como forma de auto-regulação, e podem ser insuficientes para permitir os direitos fundamentais das pessoas quando utilizam a tecnologia.

A ética, trabalhando em conjunto com a lei, permite sistemas de dados fiáveis, fornecendo o tipo de detalhes práticos e técnicos que apoiam as leis, uma vez que as leis são geralmente de aplicação mais geral do que códigos de ética específicos, mas também por vezes menos rapidamente adaptáveis às novas tecnologias. A ética opera de forma prospectiva, permitindo a concepção ética enquanto as leis tendem a ser

promulgadas e a funcionar retrospectivamente. Os códigos de conduta éticos devem incorporar os direitos digitais e apoiar o cumprimento da legislação internacional e nacional.

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

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

Recomendações

Os Estados-membros devem incentivar o desenvolvimento e a adesão a códigos de ética que respondam ao contexto africano, e que promovam os direitos digitais e humanos. Isto significa que as pessoas que trabalham com dados, independentemente do sector em que trabalham, devem respeitar os direitos e aderir a estas normas éticas. Estes códigos devem ter em conta as considerações de género no contexto africano, assegurando que reduzem os danos e a exclusão das mulheres e raparigas. É impraticável que os Estados-membros legislem no sentido de que todas as tecnologias e fornecedores de tecnologia que lidam com dados adiram a códigos éticos específicos, uma vez que muitas destas tecnologias são concebidas, construídas e operadas em outras jurisdições. Os Estados-membros devem, contudo, encorajar a adopção destes códigos de ética por eles próprios, utilizando apenas tecnologias e fornecedores de tecnologia que adiram aos códigos de conduta ética aprovados.

Para além de qualquer recurso jurídico regulamentar ou judicial disponível num país, há também a possibilidade de considerar a habilitação dos mecanismos de direitos humanos existentes a nível nacional, regional e continental para julgar a utilização de dados.

Acções

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

5.3.3 Disposições institucionais para a regulação de sistemas adaptativos complexos

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

5.3.3.1 Construir a capacidade dos organismos reguladores

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

5.3.3.2 Um afastamento dos silos regulamentares

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

SECTOR REGULATORS	TOPICS OF POTENTIAL COLLABORATION WITH THE DATA REGULATOR
Telecommunications	Availability and quality of foundational infrastructure to enable data services
Competition	Concentration, mergers and acquisitions, anti-competitive practice in digital and data markets but also pricing and market structure's effect on security
Consumer protection	Digital devices and services, e-commerce
Commerce/trade	Digital taxation, e-commerce, digital services, digital financial services
Finance	Finance blockchain, cybersecurity, financial inclusion, mobile financial services, privacy
Education	Online child protection, schools connectivity, availability of data for acquiring data skills

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

5.3.3.3 Regulador de dados

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

A Rede Africana de Reguladores da Informação fornece um exemplo de colaboração regional para estabelecer reguladores de dados nacionais, sensibilizar para novas informações e governação de dados, proporcionar governação para fluxos de dados transfronteiriços e cooperar com os reguladores a nível internacional. Faz isto para alinhar a governação, particularmente em relação à resposta proporcional e normalizada às violações de dados e direitos de violação.

Os reguladores e decisores políticos nacionais têm um papel a desempenhar na arena internacional. Intensificar a cooperação internacional sobre fluxos de dados transfronteiriços para assegurar que os requisitos de localização de dados e outras restrições ao fluxo transfronteiriço de dados não interfiram indevidamente com as comunicações transfronteiriças e os benefícios económicos e sociais que as redes globais de dados tornam possível e são minimamente restritivas do comércio, promovendo ao mesmo tempo a confiança.

Incentivar a cooperação regional e internacional em matéria de privacidade de dados e iniciativas de segurança cibernética para simplificar uma miscelânea de regras e práticas de privacidade de dados e de segurança cibernética em normas e leis regionais ou globais comuns a permitir o livre fluxo de dados e o comércio digital.

5.3.3.4 Concorrência

Como os reguladores em África esforçam-se por introduzir e aplicar a regulação da concorrência tradicional, existe o perigo de que a regulação estática da concorrência para governar sistemas dinâmicos e adaptativos possa inibir a inovação e danificar a tecnologia subjacente que permite a inovação. Por exemplo, uma regulamentação que se concentre na redução do domínio apenas na camada de aplicação da Internet poderia ter um impacto negativo e mesmo prejudicar toda a Internet e a sua infra-estrutura. Os reguladores devem estar cientes da possibilidade de sistemas globais novos e adaptáveis poderem produzir produtos e preços inovadores (como o Whatsapp) que permitam um acesso acessível e melhorem o bem-estar dos consumidores e escolha ou mesmo oportunidades de competição local nas suas plataformas, parecendo ao mesmo tempo dominantes num mercado global (Facebook).

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

5.3.3.5 Defesa do Consumidor

Como as autoridades de protecção do consumidor não são responsáveis por um sector específico, no exercício das suas funções têm geralmente confiado em outros reguladores específicos do sector. Regras claras, fortes e aplicáveis relacionadas com a gestão de dados podem proporcionar uma defesa adequada para a protecção do consumidor digital, ao mesmo tempo que criam um quadro previsível e estruturado

para a realização de actividades comerciais digitais. Protocolos e mecanismos reguladores ágeis capazes de se adaptarem a tecnologias e condições em rápida mutação podem contribuir em muito para aumentar a confiança no ecossistema digital. Estes incluem o cumprimento dos requisitos relativos ao acesso a dados não pessoais mantidos pelas plataformas digitais, a transparência de certos algoritmos essenciais utilizados pelos serviços digitais, a portabilidade dos dados essenciais das plataformas de estruturação e a interoperacionalidade e manutenção das APIS (União Internacional das Telecomunicações, 2020).

Uma forma de aumentar a transparência na utilização dos dados dos consumidores é a criação de um portal de transparência, mas isto depende de o regulador de dados ter os recursos para estabelecer, controlar e fazer cumprir as infracções. Isto proporciona às pessoas um acesso seguro a um portal onde podem ver o histórico de quando e com quem os seus dados pessoais foram partilhados, permitindo-lhes desafiar os dados partilhados ou utilizados sem o seu consentimento. Isto pode não se aplicar a certas categorias de partilha de dados de interesse público, realizada através de pseudonímia ou anonimização dos dados.

Recomendações

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

Acções

- Os membros com reguladores de dados devem avaliar se os poderes de execução existentes são suficientes.
- Os membros que criam reguladores de dados devem considerar uma série de poderes de execução e ao abordar as limitações de recursos como os reguladores de dados podem potencialmente confiar noutras agências para a execução.

5.3.4 Reequilíbrio do ecossistema jurídico

Definição do problema

Vários dos diferentes mas sobrepostos ramos do direito, tais como o direito de protecção de dados, o direito da concorrência, o direito da segurança cibernética, o direito das comunicações e transacções electrónicas, e as diferentes categorias do direito da propriedade intelectual tratam de dados. No entanto, podem entrar em conflito ou contradizer-se mutuamente. Em contraste com a protecção de dados que se aplica apenas aos dados que podem ser relacionados com um indivíduo, o regulamento da concorrência aplica-se aos dados quando o controlo dos dados tem um efeito anticoncorrencial. O controlo concentrado sobre dados, incluindo fluxos de dados e análise de dados, implica não só barreiras à entrada no mercado, mas também o interesse público A concentração de dados, fluxos de dados e sistemas de dados aumenta substancialmente a probabilidade e danos que podem ser causados por ataques cibernéticos e violações de dados, uma vez que conduz a um único ou poucos pontos de falha que podem ter consequências em grande escala. Estas preocupações não são da competência de muitas autoridades de concorrência, mas deveriam ser, uma vez que se trata de preocupações de interesse público. As autoridades de concorrência podem ser mandatadas para evitar uma centralização estrutural que aumenta os riscos de ataques cibernéticos ou de violações maciças de dados à escala da sociedade. O acesso aos dados é geralmente pró-competitivo mas pode estar em tensão com outras leis, tais como as reivindicações de propriedade intelectual sobre dados e bases de dados e privacidade e protecção de dados.

Embora seja geralmente aceite que os dados em bruto não são protegidos por qualquer direito de propriedade reconhecido, foram feitas alegações sobre os dados com base nos diferentes tipos de propriedade intelectual; direitos de autor, protecção de bases de dados *sui generis*, segredos comerciais e patentes. Nenhuma destas subvenções concede propriedade sobre dados, como tal. A protecção de bases

de dados *sui generis* é uma lei única da União Europeia, confinada à Europa. Em alguns países de direito comum, o direito de autor foi alargado a bases de dados e compilações de dados, mas mesmo estes países têm regras diferentes com alguns tribunais que alargam o direito de autor apenas para o esforço de compilação, enquanto outros exigem criatividade. Os direitos de autor destinam-se a recompensar autores humanos e a sua aplicação a bases de dados compiladas por computadores é indeterminada. As disputas entre concorrentes sobre a utilização excessiva de bases de dados padrão da indústria derivam dos direitos de autor e do direito da concorrência. Uma decisão judicial (Discovery Ltd and Others v Liberty Group Ltd ZAGPJHC 67, 2000) oferece uma solução que defende tanto a protecção de dados como a concorrência: em tais litígios, se os dados forem de natureza pessoal, são "propriedade" do sujeito dos dados e os concorrentes não podem excluir outros do acesso a esta informação. Embora a aplicação das leis de propriedade intelectual aos dados ainda esteja a ser resolvida, os direitos das pessoas sobre os seus dados pessoais devem ser tratados como mais fortes do que qualquer reivindicação de propriedade intelectual sobre esses dados, porque a protecção de dados é tão importante para a construção de economias de dados.

Os segredos comerciais podem também aplicar-se a dados em algumas circunstâncias, mas precisamente quais são as circunstâncias que não são claras.

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

As leis da criminalidade cibernética proíbem o acesso não autorizado, utilização ou alteração de dados pessoais ou sistemas de identificação. Como foi reiterado ao longo do quadro político, a segurança e a protecção são essenciais para a implementação eficaz da política e um limiar, embora não suficiente, para a construção de um sistema digno de confiança. As leis relativas à criminalidade cibernética, determinando as formas de acesso, utilização e distribuição de dados, têm o potencial de aumentar as barreiras de entrada na economia de dados. A Convenção de Malabo promulgada pela União Africana e especificamente adaptada para a região trata tanto da criminalidade cibernética como da protecção de dados. No entanto, ainda não está em vigor, na medida em que aguarda ratificação.

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

Recomendações

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

Acções

- Os contratos que pretendem renunciar aos direitos digitais, protecção de dados pessoais e que inibem a concorrência devem, como regra geral, ser inexequíveis. Isto pode ser articulado na protecção de dados e na regulamentação da concorrência, que também pode considerar, caso a caso, se os efeitos pró-concorrenciais de tais contratos compensam os efeitos anticoncorrenciais.
- As comissões nacionais de reforma legislativa ou instituições jurídicas especializadas similares devem investigar e considerar como harmonizar os diferentes ramos da legislação, regimes regulamentares e autoridades de supervisão que lidam com dados;

- Os Estados-membros devem apoiar a actualização ou adopção de quadros e regulamentos de direito da concorrência que considerem os desafios de analisar as questões de concorrência, conceber soluções e fazer cumprir os seus poderes para salvaguardar a concorrência nos mercados orientados para os dados, bem como reforçar a capacidade dos reguladores da concorrência para implementar estas regras.

- As leis de propriedade intelectual devem ser alteradas para fornecer:
    - que se os direitos de autor se aplicarem a bases de dados e compilações de dados, serão apenas aplicáveis ao trabalho de autores humanos que exibam originalidade/criatividade e que os direitos de autor se estendam apenas à selecção e disposição original dos dados numa base de dados ou compilação e não aos dados em si;
    - que qualquer direito de autor ou outro direito de propriedade intelectual, incluindo segredos comerciais que permitam o controlo de dados, não se aplica aos dados pessoais;
    - que qualquer direito de autor ou outro direito de propriedade intelectual, incluindo segredos comerciais que permitam o controlo de dados, é limitado pelas disposições da regulamentação da concorrência e direitos alternativos que oferecem protecção a inovações locais não previstas nos quadros actuais;
    - Adaptações aos regimes de DPI existentes para alavancar as próximas tecnologias de fronteira, tais como permitir a utilização de dados pela IA.

5.3.4.1 Colaboração com processos de governação regional e global

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

A regulação formal deve deixar espaço suficiente para a auto-regulação, modelos reguladores híbridos e colaborativos e mecanismos de supervisão para a aplicação da lei. A gama de ferramentas e remédios em mãos para os reguladores explorarem é ampla, desde incentivos e recompensas, passando pela indulgência, até obrigações específicas. Os instrumentos regulamentares expandiram-se para abranger caixas de areia regulamentares, quadros éticos, roteiros tecnológicos, avaliações de impacto regulamentar, investigação multifacetada e grandes simulações de dados para determinar a resposta regulamentar mais equilibrada, proporcional e justa. IA, IoT e desinformação virtual são algumas das questões complexas à espera de serem abordadas (Simpósio Global para Reguladores, 2020).

5.3.4.2 Regulamentação consultiva e baseada em provas

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

Recomendações

Ao criar disposições institucionais, os Estados-membros devem distinguir claramente entre os papéis do Estado como decisor político e regulador, que deve ser suficientemente independente do Estado e da

indústria, de modo a implementar políticas de interesse público e dos prestadores de serviços e operadores de plataformas.

As instituições reguladoras devem ser estabelecidas com base em princípios de autonomia, transparência, responsabilização para evitar a captura estatal e reguladora. Os reguladores devem realizar Avaliações de Impacto Regulamentar numa fase precoce da regulamentação para implementar as melhores abordagens que equilibrem a regulamentação e o crescimento económico. Os reguladores devem publicar o desempenho dos esforços políticos e regulamentares para melhorar as estratégias regulamentares em todos os Estados, incluindo relatórios de participação pública de regulamentos emergentes. Os reguladores devem igualmente ser autofinanciados ou financiados através de dotações parlamentares para permitir a independência financeira. As decisões regulamentares devem basear-se em bons dados e aproveitar o conhecimento do sector privado e da sociedade civil através de consulta pública. A concorrência e os reguladores sectoriais devem evitar uma regulação instrumental da concorrência, adoptando modelos de eficiência dinâmica em vez de modelos de eficiência estática.

Acções

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

5.3.5 Criar valor público

Definição do problema

Ter dados sem a capacidade humana, o controlo suficiente ou incentivos para a valorização, é muito o mesmo que não ter dados. Estas restrições aplicam-se a muitos países africanos. Há também desafios na promoção de um sector público orientado por dados. A avaliação de dados está altamente dependente de permitir quadros regulamentares e políticos que facilitem a obtenção de dados úteis, reforçando as capacidades humanas, institucionais e técnicas para criar valor a partir de dados, incentivando a partilha e interoperacionalidade de dados, e aumentando a legitimidade e a confiança pública no Estado para gerir os dados dos cidadãos de uma forma responsável. Além disso, a infra-estrutura de dados que permite um sistema de dados integrado é um recurso estratégico fundamental para os países. O ambiente criado pela interacção de elementos no ecossistema de dados e a natureza das relações e processos não lineares entre eles e dentro deles, determinam as intervenções para criar incentivos aos investimentos tecnológicos que são necessários para impulsionar o crescimento da economia de dados. Estas condições são moldadas pela estrutura do mercado, a competitividade dos serviços que dele resultam e a eficácia com que o mercado é regulado.

5.3.5.1 Capacidade do sector público

As capacidades digitais e de dados do sector público são um factor determinante para a prestação de serviços em muitas áreas prioritárias. Criar as condições para que os dados sejam optimizados no sector público para satisfazer as necessidades dos cidadãos de forma mais eficaz são condições necessárias de inclusão social e económica. Contudo, existem desigualdades multidimensionais e ineficiências políticas sobrepostas que limitam as capacidades humanas e institucionais para reforçar uma cultura de empreendedorismo digital, fomentar comunidades de inovação digital inclusivas, e promover mercados de ecossistemas de dados justos e equitativos - onde os africanos com capacidades variadas podem trabalhar com tecnologias digitais de fronteira e contribuir para o ciclo de valor dos dados ou participar em cadeias de valor de dados de uma forma mais inclusiva.

Para que um sector público orientado pelos dados se materialize, a função pública tem de ser renovada com liderança e vontade política para assegurar que os funcionários públicos a todos os níveis estejam equipados com uma compreensão básica de como os dados podem ser utilizados para melhorar a prestação de serviços e a implementação de políticas. Além disso, um sector público orientado para os dados requer uma abordagem comum e um modelo arquitectónico de infra-estrutura de dados que possa abordar a potencial integração e intercâmbio de dados e aplicações orientadas para os dados e para as plataformas.

5.3.5.2 Tratamento de dados públicos

O sector público é incumbido de gerir os principais dados de desenvolvimento económico. Isto inclui dados estatísticos e indicadores económicos utilizados para efeitos de relatórios com instituições multilaterais, e dados administrativos, tais como Identificações Digitais. Isto é frequentemente anonimizado e combinado com outros dados em vários casos de utilização que vão desde a hiper-personalização comercial, tal como a solvabilidade, até ao interesse público em subvenções sociais e gestão de catástrofes.

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

5.3.5.3 Garantir a qualidade e a relevância dos dados do sector público

Existem várias teorias ou modelos para estudar desafios de qualidade de dados. Como resultado, a definição de determinantes e relevância da qualidade dos dados de uma perspectiva técnica é informada por uma ampla variedade de cenários de aplicação, como disponibilidade de dados, tipo de dados, características do domínio e como e por que os dados são utilizados e/ou colectados, entre outros (Wang et al., 2019; Wook et al., 2021); Wook et al., 2021). Por exemplo, na investigação sobre saúde, um quadro de avaliação da qualidade dos dados consistiria em 30 ou mais indicadores de qualidade de dados, enquanto para os sensores de qualidade de dados recolhidos a partir de dispositivos IoT apenas duas dimensões podem ser consideradas (Schmidt et al., 2021; Teh et al., 2020). Além disso, o advento de grandes análises de dados, incluindo ML e capacidades técnicas para além da ciência dos dados, tais como engenharia e gestão de dados, significa que os dados são processados (limpos) e podem melhorar a qualidade dos dados recolhidos, tornando-os disponíveis para uma grande variedade de casos de utilização (Wook et al.,2021, Svolba, 2019).

Com sistemas educativos não adaptados à realidade digital e, por conseguinte, com uma má STEM e competências no domínio das TIC e digital, é limitado o talento existente para utilizar plenamente as grandes técnicas de análise de dados e a ciência dos dados para criar valor a partir de dados acumulados ou produzidos. O tratamento inadequado e a partilha de dados no sector público inibem o desenvolvimento de sistemas de dados integrados e os benefícios a eles associados.

Recomendações

- Dado o ritmo vertiginoso da digitalização, como principal guardião dos dados dos cidadãos, o sector público precisa de ser dotado de recursos adequados para potenciar os dados, de forma a salvaguardar os interesses públicos. Uma forma de o fazer é através de formação específica e de iniciativas de co-criação de conhecimentos com outras agências internacionais - instituições com poucos recursos que curam dados públicos que já albergam profissões analíticas existentes (estatísticas, economia quantitativa, investigação operacional e investigação social, etc.). Estes recursos existentes podem ser aumentados e utilizados para melhorar a criação de valor dos dados no contexto do sector público.
- Os Estados-membros devem comprometer-se com toda uma abordagem governamental à utilização de dados em várias prioridades políticas, as entidades públicas que curam vários tipos de dados devem receber mandatos claros e ser dotadas de recursos com capacidade técnica, institucional e humana. Isto pode ajudar a garantir que são responsáveis pela gestão de dados de qualidade que podem ser partilhados e reorientados de uma forma responsável para casos de utilização múltipla.
- Para promover a confiança na gestão pública de dados, os reguladores do sector e os administradores de dados públicos devem assegurar a colaboração com as partes interessadas da indústria. Dado que as avaliações da qualidade dos dados do sector privado estão frequentemente fora do controlo do sector público, os esforços de gestão de dados da indústria são mais adequados para a elaboração de leis e regulamentos que promovam a utilização de dados de alta qualidade. Isto é necessário para acomodar vários casos de utilização que requerem diferentes indicadores de avaliação da qualidade dos dados. Estas directrizes de avaliação devem ser feitas através de esforços de múltiplos intervenientes - a governação de dados deve ser considerada no contexto das realidades operacionais de vários casos de utilização de dados, em todas as indústrias.

Acções

- Os reguladores sectoriais e os administradores de dados públicos devem funcionar dentro de directrizes específicas sobre como as avaliações da qualidade dos dados devem ser implementadas, dependendo dos casos de utilização comum, algoritmos, e tipo de dados utilizados, estas directrizes podem ser informadas pelas melhores práticas globais (incluindo dados e governação da IA) mas devem ser adaptadas ao contexto dos casos de utilização de dados africanos. Devido ao intercâmbio, combinações,

armazenamento estratégico, e redireccionamento, necessários para criar valor de dados. Uma estratégia eficaz de qualidade dos dados em todo o sector público deve ser informada pelas realidades técnicas/práticas/operacionais e deve delinear os papéis, responsabilidades e mandatos das várias agências governamentais na recolha e manutenção de dados de alta qualidade, de forma a salvaguardar os cidadãos.

- Os Estados-membros precisam de participar nos esforços para estabelecer e adoptar um quadro normativo para normas e sistemas de dados harmonizados destinados a estabelecer a interoperabilidade nacional, regional e internacional. Estes podem incluir intervenções específicas de formação humana, técnica e institucional, projectos de infra-estruturas sub-regionais, e caixas de areia regulamentares das CER.
- Uma abordagem continental facilita economias de escala para incentivar o investimento privado em infra-estruturas digitais fundacionais, incluindo tecnologias baseadas na nuvem. A harmonização regional dos regulamentos para a governação de dados poderia reduzir ainda mais os custos de conformidade e reduzir a incerteza e o risco operacional para os principais investimentos em infra-estruturas relacionadas com as TIC.
- As instituições públicas que curam dados devem ser dotadas de recursos adequados a fim de contribuírem em fóruns multilaterais no que diz respeito a dados e serem administradores de acesso inclusivo e utilização responsável dos dados, guiados por normas técnicas e regulamentares, padrões e melhores práticas adequadas da indústria - que sustentam tanto as características informativas como económicas dos dados nas indústrias prioritárias.

5.3.6 Políticas sectoriais coerentes para aumentar o valor dos dados

Definição do problema

As políticas de concorrência, comércio e fiscalidade estão significativamente interligadas. As economias de dados locais competitivas, por exemplo, podem aumentar os serviços orientados por dados e a abertura comercial pode estimular o comércio digital internacional e o investimento directo estrangeiro (IDE) nas economias de dados nacionais. No entanto, isto também pode reforçar o domínio dos oligopólios globais nos ecossistemas de dados nacionais, criando tensões comerciais relacionadas com os fluxos de dados transfronteiriços. Os modelos empresariais digitais impulsionados simultaneamente pelos dados podem minar a concorrência interna e reforçar a concentração do mercado à medida que as autoridades fiscais esforçam-se por quantificar, valorizar, estabelecer e acompanhar cadeias de valor digitais devido a características como os fornecedores terceiros e a ausência de presença física como base para estabelecer a responsabilidade fiscal das empresas no sector impulsionado pelos dados.

Para os Estados-membros, a acção colectiva através de uma abordagem unificada proporcionará mais provavelmente melhores resultados que captem os contextos africanos ao abordar a concorrência, o comércio e os desafios fiscais nos mercados de dados.

5.3.6.1 Política de Concorrência

Definição do problema

As características dinâmicas dos modelos empresariais orientados para os dados criam desafios para a implementação de instrumentos tradicionais de política de concorrência, aplicação efectiva da concorrência, soluções e regulamentação das fusões nos mercados digitais. A resolução destes desafios requer intervenções preventivas no mercado e colaboração contínua com políticas complementares tais como a protecção do consumidor, comércio, industrialização e investimento.

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

5.3.6.2 Política de Comércio

Definição do problema

Os sistemas digitais já não funcionam dentro de jurisdições nacionais claramente definidas. A reforma da política comercial é necessária para orientar o crescente comércio digital e o comércio electrónico. Diferentes influências geopolíticas, dotes e capacidades institucionais e humanas no continente podem afectar as abordagens unilaterais ao comércio digital e os esforços de harmonização regional. A estratégia de dados transfronteiriços adoptada a nível interno exigirá diferentes capacidades institucionais, só poderá ser eficaz com base nas dotações existentes do ecossistema de dados, influenciará a forma como o valor dos dados será criado ou extraído dentro e entre países africanos, e determinará quem beneficiará mais do ciclo de valor dos dados a nível interno e regional.

Comércio de serviços, fluxos de dados transfronteiriços e localização

Para que o comércio digital ocorra, os dados têm de ser transferidos para além das fronteiras. Embora a acumulação de dados possa ser uma forma segura de gerir dados, o açambarcamento de dados sem meios para utilizar, trocar, ou redireccionar de uma forma segura pode também criar riscos de subutilização que podem diminuir a eficiência e diminuir outros benefícios do comércio digital. A protecção de dados nacionais e os regulamentos não afectam apenas as oportunidades de negócios locais, afectam também o comércio intra-regional e a participação na economia digital global orientada para os dados.

Enquanto os dados não pessoais são utilizados e trocados além-fronteiras, a importância dos dados gerados pelos utilizadores e dos serviços digitais como contributos em várias actividades industriais fornece um enorme campo de acção para aumentar as exportações de serviços digitais. Os serviços são igualmente contributos em muitos produtos manufacturados e em diferentes cadeias de valor de dados. Por esta razão, surgiram três regimes gerais comuns de gestão de dados estilizados para os fluxos transfronteiriços de dados pessoais, que variam em termos de abertura, intervenção necessária, e actores responsáveis. Há igualmente variações de todos os três modelos estilizados, dependendo do tipo de dados e do caso de utilização. Muitas vezes, os dados sensíveis, tais como dados pessoais, têm requisitos de dados transfronteiriços mais rigorosos do que os dados não pessoais. As regras e normas de protecção de dados também podem ser incorporadas em regulamentos sectoriais em indústrias altamente regulamentadas, como a saúde e as finanças, que exigem avaliações de qualidade e considerações éticas mais rigorosas.

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

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

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

Três abordagens estilizadas para governar os fluxos de dados transfronteiriços

CROSS-BORDER DATA GOVERNANCE REGIME	DESCRIPTION	PROS	CONS	ASSUMPTIONS
Open transfers regime	• Relatively low a priori mandatory approval requirements, and voluntary private sector industry standards inform the free movement of data (eg. USA, APEC)	• Minimal regulatory burden allows for the greatest flexibility in the movement of data • Most suitable for digital services trade and data value creation • Privacy is a consumer right	• Risk of proliferation of standards across firms and jurisdictions, without guaranteeing any minimum standard for personal data protection • Requires, technical, human, and institutional capacity to monitor private firms and exercise ex post accountability • Limited data subject rights—lack of consent for personal data use	• Interoperable data systems and infrastructure • Human, technical, and institutional capacity to create value from data • Strong preconditions (enablers) to leverage the data-driven digital economy • Data subjects with digital capabilities to provide consent
Conditional transfers regime	• Consensus base, established regulatory data safeguards and overarching regulatory guidance from data protection authorities or international agreements (e.g GDPR)	• Offers more balance between data protection and the need for openness of data transfers for value creation • Encourages establishment of domestic data processing authority (DPA) • Clear guidelines and mandatory regulatory safeguards that once met allow for the free flow of cross-border data	• Based on strong data subject rights • Certain conditions need to be fulfilled ex-ante • Can perpetuate compliance burdens and digital trade bottlenecks	• Same as above • International collaboration and geopolitical influence to enforce ex- ante conditions
Limited transfers model	• Cross-border data flows are conditional based on government approval and localization requirements for domestic storage or processing of data (e.g China, Russia).	• Based on strong national security and public data control imperatives	• Stringent regulatory approval for international data transfers and may require explicit or implied data localization and mandatory storage	• Same as above

Source: Authors own interpretation summarised from Ferracane and van der Marel (2021), WDR (2021).

Comércio electrónico

As plataformas de comércio electrónico permitem aos consumidores beneficiar de uma maior variedade de escolhas a preços mais competitivos. As estratégias para melhorar o comércio electrónico não podem ser formuladas isoladamente, uma vez que o comércio electrónico se cruza com uma multiplicidade de outras questões, incluindo a Identificação DigitaI, governação de dados, direitos aduaneiros, fluxos de dados transfronteiriços, segurança cibernética, interoperabilidade dos sistemas de pagamentos, protecção do consumidor,[46] concorrência, tributação e normas, para citar algumas. Além disso, a melhoria da adopção do comércio electrónico requer a abordagem de factores como a penetração da Internet, a fiabilidade postal, a utilização dos serviços de pagamentos (contas bancárias ou dinheiro móvel) e a segurança dos servidores da Internet.[47] Para os Estados-membros, é mais provável que a acção colectiva através de uma abordagem unificada produza melhores resultados que captem os contextos

[46] Protecção do consumidor online e devoluções de produtos, segurança do consumidor e responsabilidade do fornecedor.

[47] https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d12_en.pdf

africanos ao abordar desafios sobrepostos que afectam diferentes mandatos governamentais em fóruns multilaterais.
Os acordos comerciais, por si só, não são os instrumentos adequados de governação transfronteiriça de dados. A actual abordagem comum da utilização de acordos comerciais para regular os fluxos de dados transfronteiriços não conduziu a regras vinculativas, universais ou interoperáveis que regem a utilização de dados entre jurisdições. No entanto, no contexto da ZCLCA, uma abordagem harmonizada e coordenada para enfrentar os desafios associados à publicação de dados no mercado interno contribuirá para um melhor alinhamento com vários esforços sobrepostos de coordenação intra-regional do comércio digital e do comércio electrónico para além dos próximos protocolos comerciais de comércio electrónico[48] e serviços[49] na estratégia.

Recomendações

- Para promover ecossistemas de dados competitivos, seguros, fiáveis e acessíveis, as autoridades da concorrência precisam de encontrar formas coordenadas e eficazes de regular a concentração, preservando simultaneamente os benefícios que as empresas dominantes oferecem no contexto de diferentes necessidades de desenvolvimento em todo o continente. Isto inclui a regulamentação *ex-ante* de questões de concorrência antes que estas se intensifiquem no mercado.
- Os decisores políticos no panorama fiscal, concorrencial e comercial terão de criar capacidade humana e técnica para abordar questões emergentes para além do tradicional mandato sectorial que podem afectar os mercados impulsionados pelos dados;
- Os Estados-membros devem promover a previsibilidade e a convergência de regimes em áreas políticas complementares, de uma forma que se reforce mutuamente. Isto tem de ser feito para navegar na emergência de novos modelos de negócios dinâmicos orientados para os dados que possam fomentar o comércio digital intra-africano e o empreendedorismo com base em dados. Ao mesmo tempo, os decisores políticos devem prestar atenção às ligações de dois sentidos entre os resultados económicos e a governação dos dados e pesar cuidadosamente as contrapartidas.
- Os Estados-membros devem promover uma abordagem regional coordenada, abrangente e harmonizada dos desafios da governação global associados à economia digital global baseada em dados, como por exemplo:
    - colaboração transfronteiriça na implementação de instrumentos de política de concorrência para abordar comportamentos anticoncorrenciais em mercados digitais orientados para a informação;
    - incentivar a portabilidade dos dados através de regulamentação e outras actividades facilitadoras;
    - os esforços da Organização para a Cooperação e Desenvolvimento Económico (OCDE) para evitar a evasão fiscal em relação às empresas orientadas por dados;[50]
    - Acordos da Organização Mundial do Comércio (OMC) em matéria de serviços baseados em dados e comércio electrónico;
    - estabelecer infra-estruturas regionais coordenadas de dados fundacionais e iniciativas de desenvolvimento de sistemas de dados digitais;

[48] O protocolo de comércio eletrónico da ZCLCA é um instrumento importante para preservar o mercado africano consolidado na esfera digital, e exclui outros acordos que possam potencialmente prejudicar a agenda de liberalização e integração. Espera-se que as directrizes sejam finalizadas na Fase III das negociações da ZCLCA.
[49] A fase II da ZCLCA pretende abordar o comércio de serviços, os direitos de propriedade intelectual, o investimento e a política de concorrência
[50] https://www.oecd.org/tax/beps/

- reforço da capacidade humana, técnica e institucional para apoiar a interoperabilidade dos dados, a criação de valor, e a participação equitativa nas economias de dados;
- contribuindo para a harmonização internacional de normas técnicas, ética, governação e melhores práticas em matéria de dados, grandes análises de dados e IA.

Acções

- Os Estados-membros devem encorajar uma reforma política e regulamentar dinâmica e a experimentação (por exemplo, caixas de areia regulamentares a nível da indústria e das CER);
- Os decisores políticos devem prestar atenção às ligações de dois sentidos entre os resultados económicos e a governação dos dados e pesar cuidadosamente as contrapartidas. As diferentes entidades estatais devem esforçar-se por estabelecer quadros de partilha de dados seguros e responsáveis que facilitem a procura de dados, a interoperabilidade dos dados, os fluxos transfronteiriços de dados, as cadeias de valor de dados e os sistemas e normas de dados abertos dentro de sectores-chave prioritários, tal como atribuídos pela DTS;
- Para que a utilização de dados seja eficiente, inclusiva e inovadora, será necessária a colaboração entre instituições reguladoras em diferentes mandatos e uma regulação coordenada do mercado (em áreas políticas inter-relacionadas, tais como telecomunicações, concorrência, comércio, fiscalidade e regulação de dados);
- As autoridades de concorrência ou instituições relacionadas terão de criar capacidade humana e técnica para abordar questões de concorrência emergentes para além da concentração do mercado que possam afectar os mercados impulsionados pelos dados;
- Os instrumentos tradicionais da concorrência, tais como directrizes sobre definições de mercado, avaliação de posição dominante, práticas anticoncorrenciais (por exemplo, abuso de posição dominante, práticas coordenadas, e abuso do poder de compra), avaliação de concentrações, e teorias de danos e concepção de soluções terão de ser ajustadas para incorporar o dinamismo dos dados e as características das empresas orientadas pelos dados;
- Os signatários da ZCLCA terão de determinar de que forma o protocolo de comércio electrónico funcionará em paralelo com as leis e políticas existentes e terão de ter em conta e apoiar os objectivos dos outros protocolos, tais como o investimento, a propriedade intelectual e a política de concorrência (a negociar na Fase II).
- Reforçar a capacidade das autoridades aduaneiras de lidarem com o comércio electrónico, tais como mecanismos de desalfandegamento para a transferência de bens de baixo valor e a abordagem de tarifas personalizadas.
- Desenvolver e reforçar os mecanismos de diálogo público-privado para melhorar a elaboração de políticas relacionadas com o comércio electrónico.

5.3.6.3 Política fiscal

Definição do problema

Existe uma incongruência entre onde os lucros das plataformas globais são actualmente tributados e onde e como o valor é criado a partir de dados dentro da economia digital. Em África, a maioria dos países são principalmente mercados de dados para plataformas globais, com os utilizadores a contribuir significativamente para a geração de lucros de plataformas, sem um mecanismo plausível de captura de valor. Actualmente, o tráfego de dados em África está a crescer a uma taxa anual de 41% (CNUCED, 2019), o que implica uma maior utilização e adopção dos serviços fornecidos por plataformas digitais globais na região. Embora tenha havido compromissos contínuos por parte de instituições multilaterais, principalmente liderados pelo Quadro Inclusivo sobre Erosão de Base e Transferência de Lucros (BEPS) da

OCDE (embora não totalmente inclusivo para África com apenas 23 países participantes), não se chegou a um consenso global para as diferentes opções propostas (Pilares Um e Dois) no que diz respeito à tributação digital.

Vários países africanos, relutantes em atrasar a tributação dos serviços digitais ou não convencidos dos benefícios das reformas internacionais para os seus países já estão a implementar mecanismos unilaterais. Estes incluem impostos sobre serviços digitais e taxas de equalização baseadas em dados económicos (dados) significativos para captar parte do valor dos dados através da tributação de algumas partes da economia digital dentro das suas jurisdições. Estes mecanismos incluem também a expansão da tributação específica do sector na indústria das telecomunicações e a tributação das transacções de dinheiro móvel e a utilização de algumas aplicações de comunicação exageradas (OTTs) na região, tais como a WhatsApp, Facebook, Twitter, Skype, e Instagram. Embora estes impostos sejam impulsionados para aumentar as receitas governamentais, o impacto negativo no consumidor atrasou o acesso e a inclusão digital (devido aos custos de consumo deslocados), e restringiu o direito à liberdade de expressão dos cidadãos. Do lado da oferta, os impostos alargados sobre o sector das telecomunicações têm um impacto negativo nos lucros dos operadores residentes do sector (com as consequentes implicações negativas para os investimentos em infra-estruturas de importância crítica na região com limitações de recursos), enquanto os OTT baseados em dados são em grande parte não tributados localmente (CTO 2020, ICTD 2020, RIA 2021, (CTO, 2020)).

De uma perspectiva de soberania e benefícios fiscais, cada país tem direito a tributar os lucros das plataformas digitais globais desde que tenha uma interacção económica com os seus cidadãos e residentes (em grande parte através da venda dos seus dados pessoais). No entanto, apesar de ter milhões dos seus cidadãos e residentes como utilizadores de aplicações de dados geridas por plataformas digitais globais, os países africanos sob o actual regime de tributação internacional não têm o nexo necessário para tributar os lucros destas entidades. Embora algumas das plataformas tenham alguma forma de presença local em países africanos, estas filiais são criadas apenas como serviços de apoio administrativo e não possuem legalmente os activos destas plataformas (que são em grande parte intangíveis e actualmente não estão incluídas nas propostas da maioria das fórmulas de repartição), e portanto não recebem quaisquer receitas acumuladas sobre os activos.

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

Medidas legislativas e políticas recentes introduzidas por países africanos seleccionados, no contexto dos vários esforços multilaterais e unilaterais de tributação da economia digital, podem não ser conducentes nem à criação de um mercado único nem ao acesso a recursos internacionais para realizar bens públicos globais e satisfazer algumas das condições prévias para uma economia de dados competitiva no continente. O aproveitamento de novas fontes de receitas fiscais poderia permitir aos países africanos eliminar os impostos especiais de consumo sobre as redes sociais e os serviços de dados, reduzindo as distorções tanto para o mercado local como para o sistema fiscal global.

Recomendações

Os governos africanos precisam de aumentar as actividades económicas dentro das suas jurisdições que alavanquem os mecanismos de digitalização e publicação de dados, uma vez que o aumento da produtividade dentro deste mandato irá ampliar as capacidades para maiores receitas fiscais. Este processo exigirá o desenvolvimento de mais empresas locais baseadas em dados, no âmbito da política industrial da região (Khan & Roy, 2019).

Acções

- Os Estados-membros devem apoiar a harmonização do regime fiscal para bens e serviços digitais a nível regional, e o alinhamento a nível global, mitigariam os riscos associados ao facto de os mercados de pequenas economias de dados não serem capazes de gerar valor significativo e competir nos mercados globais para contribuir para a escala e o âmbito necessários para a criação de valor orientado pelos dados e para bases fiscais geralmente limitadas.
- Complementarmente, poderia ser criado um fundo público de dados associado pelos países membros da UA, em colaboração com o sector privado, para construir a infra-estrutura necessária à extracção destes dados de transacção, onde os dados podem ser retidos como parte de uma base de dados regional comum para além do âmbito dos fins fiscais.
- Facilitar um fundo de dados públicos exigirá que os países africanos digitalizem os seus sistemas de administração fiscal para permitir uma avaliação mais eficiente e a cobrança de impostos sobre plataformas digitais. Um sistema administrativo fiscal digital aumentará a capacidade de registo fiscal, a partilha de dados de transacções com as autoridades fiscais nacionais e a troca de informações sobre obrigações fiscais com as plataformas digitais para o cumprimento, reduzindo ao mesmo tempo os custos operacionais.
- Os Estados-membros devem aproveitar a oportunidade de coordenação da tributação dos serviços digitais para um mercado digital único para se lançarem em novas fontes de receitas fiscais que lhes permitam eliminar impostos especiais de consumo regressivos e fiscalmente contraproducentes sobre as redes sociais e os serviços de dados e, reduzir as distorções tanto no mercado local como no sistema fiscal global.

5.4. Governação de Dados

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

5.4.1 Controlo de dados

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

5.4.1.1 Soberania de Dados

O controlo de dados também pode ser entendido a nível nacional em relação à soberania dos dados (Ballell, 2019). A soberania dos dados baseia-se no conceito de Estado-nação soberano e refere-se à visão de que os dados gerados ou que passam pela infra-estrutura nacional da Internet devem ser protegidos e controlados por esse Estado ((Razzano, Gillwald, et al., 2020). No contexto digital, pode ser entendido como um subconjunto de soberania cibernética definido como a subjugação do domínio cibernético (que é global por definição) às jurisdições locais (Polatin-Rúben & Wright, 2014). Existem duas abordagens, de fraca e forte soberania de dados. A fraca soberania dos dados refere-se a iniciativas de protecção de dados lideradas pelo sector privado, com ênfase nos aspectos de direitos digitais da soberania dos dados. Comparativamente, uma forte soberania de dados favorece uma abordagem liderada pelo Estado, com ênfase na salvaguarda da segurança nacional (Polatin-Rúben & Wright, 2014).

Em geral, a transferência de dados pessoais para um outro país terceiro só é permitida sob determinadas condições, por exemplo, quando outro país terceiro tem uma lei que exige salvaguardas suficientes (incluindo privacidade e segurança) para o tratamento de dados pessoais. Os Estados exercem frequentemente a soberania dos dados para a protecção dos direitos dos seus cidadãos, por exemplo, através de regimes de protecção de dados que regulam o fluxo transfronteiriço de dados para proteger os direitos das pessoas em causa, muitas vezes através de acordos que estabelecem normas de protecção de dados e protecção recíproca dos dados trocados. Embora sejam necessárias normas jurídicas suficientes para a reciprocidade, também o é a capacidade prática dos Estados para fazer cumprir as normas mutuamente acordadas. Garantir boas práticas de gestão de dados é um passo fundamental para a realização da soberania dos dados.

5.4.1.2 Localização de dados

Definição do problema
Embora haja dados significativos e recomendações de economia digital que se relacionam com a ajuda à criação de um ecossistema de dados mais amplo, há também intervenções políticas específicas a serem prosseguidas em relação à estimulação de dados do lado da procura. Os utilizadores dos dados podem ser o sector público, empresas privadas (de diferentes dimensões), e também utilizadores individuais e cidadãos. No entanto, é necessário desenvolver a capacidade através destes perfis para estimular a procura de dados, culturas de dados e inovação. O papel da política na promoção da utilização produtiva de dados entre as partes interessadas é facilitado pelas áreas políticas anteriores, mas pode também exigir considerações mais específicas. Este é especialmente o caso dado que a realidade dos dados para muitos actores locais dentro do ecossistema de dados é de escassez de dados, e não de saturação.

Enquanto a localização de dados é frequentemente vista como uma expressão de um aspecto da soberania do Estado, a localização de dados é como uma possível opção política a localização de dados precisa de ser avaliada numa base de custo-benefício. Esta opção política pode representar um desafio prático. Embora a localização de dados seja por vezes motivada pela necessidade de proteger as pessoas em causa, a localização de dados pode ser aplicada a dados não pessoais. É por isso que é essencial que a localização de dados seja lida no contexto do controlo, a fim de salientar a importância na política da importância de apoiar mecanismos que possam facilitar o acto de soberania.

A localização de dados é um conceito que vai além da soberania dos dados. Isso envolve a construção artificial de barreiras legislativas aos fluxos de dados, como por meio de requisitos de residência de dados e armazenamento obrigatório de dados locais (Cory, 2017). Esta extremidade da política pode apresentar um desafio prático. Regras rigorosas de localização de dados que exigem o armazenamento de todos os dados localmente, e não apenas uma cópia, tornam esses dados susceptíveis a ameaças à segurança, incluindo ataques cibernéticos e vigilância estrangeira.

Recomendações

- Os Estados-membros devem dar prioridade a parcerias politicamente neutras que tenham em conta a sua soberania individual e propriedade nacional para evitar interferências estrangeiras que possam afectar negativamente a segurança nacional, os interesses económicos e os desenvolvimentos digitais dos Estados-membros da UA.
- Os Estados-membros da UA têm o direito de formular regras digitais e de dados de acordo com as suas prioridades e interesses, nomeadamente para proteger a segurança da informação do Estado e dos seus cidadãos, e para impedir que terceiros explorem injustamente os recursos e os mercados locais.
- É necessário estabelecer acordos bilaterais e multilaterais para exercer a soberania e o controlo internos, sendo necessárias vias de recurso para as infracções.
- A localização precisa ser avaliada contra possíveis danos aos direitos humanos.
- Os requisitos de localização de dados requerem especificidade de dados. As soluções de localização de dados têm sido fortemente articuladas dentro de silos de dados sectoriais (verticais) em diferentes jurisdições; por exemplo, a Nigéria instituindo certas formas de localização de dados financeiros, a

Austrália prescrevendo formas de localização de dados de saúde, etc. Esta é uma área em que a especificidade é fortemente necessária, tanto para facilitar fluxos mais amplos, na medida em que é conducente a imperativos políticos como a Zona de Comércio Livre Continental Africana, mas também para a clareza que pode ajudar a minimizar os custos para as empresas e inovadores locais e reduzir os riscos de consequências involuntárias.

- O desenvolvimento de infra-estruturas de dados deve ser explorado como um mecanismo para exercer controlo, mas deve ser contextualizado tendo em consideração os impactos ambientais, as infra-estruturas de segurança e protecção, os custos duplicados para as comunidades de dados locais, e os custos globais.
- As capacidades do sector público devem ser investidas para informar as iniciativas de controlo de dados nacionais e eficazes.
- Os direitos da pessoa em causa devem ser concebidos e prever expressamente um controlo eficaz dos dados pessoais. Os fideicomissos de dados e as diligências devem ser explorados como outra forma de controlo eficaz dos dados pessoais (e outros dados).

Acções

- As autoridades de protecção de dados (APD) necessitam de total capacitação, o que inclui a competência em matéria de soberania de dados;
- As APD são incentivadas a adoptar uma cooperação internacional e regional, tomando nota das diferentes fases de implementação e aplicação em todos os Estados-membros;
- A avaliação de riscos e o envolvimento de múltiplos intervenientes devem ser utilizados para conceber soluções de localização de dados nas políticas pelos redactores, o que inclui a participação da sociedade civil;
- A política de infra-estruturas de dados deve ser alinhada com os imperativos de controlo de dados pelos redactores de políticas, mas deve considerar a cibersegurança, a protecção de dados pessoais, os riscos ambientais e o custo;
- A administração pública e a política de investimento devem alinhar-se prioritariamente com as capacidades de controlo de dados;
- O reforço das capacidades em relação à protecção de dados, cibersegurança e governação de dados institucionais nas agências relevantes deve ser assegurado através da atribuição de políticas e bens.

Mecanismos para exercer o controlo de dados

Existem mecanismos para exercer o controlo de dados, como por meio de confiança de dados. Os fideicomissos de dados e/ou diligências são formas alternativas de soluções de governação discreta no contexto dos dados. Um depositário legal é um instrumento jurídico utilizado para gerir bens, tanto corpóreos como incorpóreos. Um depositário permite que alguém detenha bens (que não possui) em benefício dos beneficiários do depositário. A pessoa que detém os activos foi autorizada a fazê-lo e deve aos beneficiários desse fundo um dever fiduciário de agir responsavelmente na gestão dos seus activos. Esta estrutura jurídica tradicional tem sido apresentada como uma forma de gerir colecções de dados em nome de grupos e de facilitar a partilha de dados em massa em situações em que o licenciamento ou modelos de dados abertos possam não ser viáveis como meio de promover a inovação através da facilitação do acesso equitativo *(Stalla-Bourdillon et al., 2019). O Instituto de Dados Abertos define os fideicomissos de dados como fornecendo "...administração fiduciária e independente de dados" (Instituto de Dados Abertos, 2018). A adição do elemento fiduciário à definição (por oposição à sua mera definição como forma de confiança legal) foi acrescentada como sendo um elemento essencial de responsabilidade e obrigação, o que constitui uma base importante para o conceito (Instituto de Dados Abertos, 2020).* Além disso, pode incluir soluções de privacidade

por concepção na arquitectura de qualquer mecanismo concebido para facilitar a confiança, assegurando assim a privacidade em substância e processo *(Stalla-Bourdillon et al., 2019). Embora as leis de protecção de dados possam criar normas de como os dados de uma pessoa podem ou não ser processados, fora do consentimento ou recurso por violações, os mecanismos para as pessoas agirem em relação aos seus dados são limitados - assim, os fideicomissos de dados ajudam a facilitar a realização do controlo de dados. Os depositários de dados fornecem ao titular dos dados um mecanismo através do qual este pode fornecer (ou "partilhar") os seus dados, ao mesmo tempo que lhe retira a responsabilidade exclusiva de "assegurar" o cumprimento da protecção de dados por parte dos actores do sector público e privado através do estabelecimento de uma relação fiduciária.*

5.4.2 Processamento e protecção de dados

Definição do problema

Embora os princípios de controlo de dados ajudem a delinear a delimitação e as obrigações relativamente a dados pessoais e não pessoais, o tratamento de dados procura delinear as orientações políticas para o tratamento de dados pessoais, tal como discutido anteriormente. A regulamentação dos dados não pessoais é determinada pela categorização dos dados e por regimes específicos de acesso.

Estas formas de orientação são importantes como mecanismo para a realização da privacidade e protecção de dados. O processamento de dados pessoais é uma componente crítica da governação de dados e da promoção de um ambiente de confiança. A construção da confiança é entendida como uma parte necessária para a promoção de dados sólidos e de uma economia digital. Ao restringir as limitações do processo aos dados pessoais, tais limitações não precisam de impedir os fluxos de dados para o comércio digital; mas para assegurar essa falta de impedimento, são necessárias políticas de dados consistentes em toda a região baseadas em princípios partilhados, mas flexíveis (Nações Unidas, 2017).

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

Uma abordagem de privacidade por concepção pode ser adoptada ao desenvolver tecnologias e sistemas digitais através dos quais a privacidade é incorporada na tecnologia e sistemas por defeito durante o processo de concepção e desenvolvimento (Cavoukian, 2009). Por exemplo, pode reforçar a minimalidade na sua recolha de dados ou automatizar a desidentificação rígida. Significa que um produto é concebido tendo a privacidade como prioridade, juntamente com quaisquer outros fins que o sistema sirva. Esta concepção deve incorporar uma compreensão particular de como os sujeitos dos dados se envolvem com os produtos, e as suas capacidades para afirmar a sua privacidade.

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

Recomendações

- As APD devem ser estabelecidas de forma independente, financiada e eficaz. Além disso, como um método para assegurar a eficácia, as métricas de responsabilização são cruciais para ajudar uma APD a ter um alcance claro. Devem ser estabelecidos quadros legais de tratamento de dados que incluam sanções claras para garantir a conformidade. Devem abranger todos os intervenientes relevantes no processamento de dados.
- A avaliação de risco de dados pessoais deve ser obrigada na implantação do desenvolvimento de tecnologia de dados pessoais.
- Um subprincípio importante, que tem de ser accionado com quadros de processamento de dados para os intervenientes públicos e privados, é o da minimização. A minimização da recolha de dados pessoais é um dos mecanismos mais eficazes para atenuar os riscos e os danos dos dados.
- Os códigos de conduta devem ser explorados para promover dados e necessidades específicas do sector. Tais Códigos, aprovados pela APD pertinente, podem fornecer conhecimentos sectoriais e industriais especializados na gestão dos riscos e danos reais que podem estar associados ao processamento, e assegurar as melhores práticas na gestão desses danos. Pode também ajudar a considerar as excepções sectoriais que podem ser necessárias para que uma economia de dados construtiva possa prosperar, mas também contribuir para uma agenda de Desenvolvimento Sustentável mais ampla, tal como através da pronta facilitação da investigação (na área da saúde, ou outras arenas de desenvolvimento social).

Acções

- Os quadros de processamento de dados devem ser estabelecidos em parceria com todos os parceiros relevantes de múltiplas partes interessadas, mas idealmente conduzidos pela APD. Estes devem alinhar-se com os seguintes princípios: consentimento e legitimidade; limitações à recolha; especificação da finalidade; limitação da utilização; qualidade dos dados; salvaguardas de segurança; abertura (que inclui a comunicação de incidentes, uma correlação importante com os imperativos da segurança cibernética e do criminalidade cibernética); responsabilidade; e especificidade dos dados.
- As APD devem ser estabelecidas com carácter de urgência juntamente com as legislações nacionais sobre protecção de dados pessoais.

5.4.3 Acesso aos dados e interoperacionalidade

Definição do problema

O acesso e a acessibilidade aos dados são entendidos tanto em termos de formas reactivas de acesso facilitadas por leis e regulamentos, como através de formas proactivas de acesso a dados (como através de dados públicos abertos) (Open Data Charter, 2015). A acessibilidade também implica a partilha de dados entre agentes ou departamentos, um benefício importante da natureza inigualável dos dados. No entanto, isso requer interoperacionalidade entre esses diferentes agentes (Jones & Tonetti, 2020). No contexto da concorrência, os dados não são simplesmente portáveis de uma forma que possa facilitar facilmente os efeitos de escala entre empresas (Rinehart, 2020). A exigência de formas de portabilidade dos dados continua a ser uma estratégia regulamentar fundamental citada para facilitar a concorrência e o benefício dos consumidores, embora as realidades ainda não tenham sido estabelecidas como definitivamente benéficas (Mitretodis & Euper, 2019; Rinehart, 2020). Do ponto de vista da privacidade, fora de apenas mudanças de interoperacionalidade, a natureza da colecta de Grandes Dados significa que a portabilidade de dados implica a privacidade de outros usuários (Nicholas & Weinberg, 2019).

Recomendações

- Os padrões de dados abertos precisam ser priorizados na criação e manutenção de dados públicos.
- A portabilidade dos dados deve ser explorada.

- As parcerias de dados (incluindo opções como bancos de dados) devem ser priorizadas como mecanismos para o avanço da qualidade e preservação da privacidade dos dados abertos.
- Como método para tentar facilitar a especificidade, a categorização de dados pode ser um método para assegurar a coesão dentro de quadros de processamento de dados dentro de permissões de processamento, e princípios de segurança. A categorização aqui referida não é tal como as tipologias sectoriais consideradas mais amplamente, mas sim como um mecanismo específico para a realização de formas particulares de riscos que se alinham com os tipos de dados e de informação, e podem incluir categorias sensíveis (como os dados das crianças), classificações de segurança relevantes, em comparação com as formas de dados já no domínio público.
- As restrições ao processamento devem ser claramente articuladas e limitadas, a fim de não interferir com o processamento de baixo risco que pode ser cada vez mais central para a formação de IA através do processamento de dados em grande escala.

Acções

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

5.4.4 Segurança de dados

Definição do problema

A segurança dos dados inclui o conjunto de políticas, normas, regulamentos, legislações e práticas para proteger a confidencialidade, integridade e disponibilidade dos dados contra acesso não autorizado, corrupção ou roubo, ao longo de todo o ciclo de vida dos dados. Esses princípios fundamentais de segurança de dados também definem as três principais áreas de responsabilidade da segurança da informação. O conceito de segurança de dados engloba muitos aspectos, desde a segurança física do *hardware* dos centros de dados e dos dispositivos de armazenamento até aos controlos administrativos de acesso, bem como a segurança lógica das redes, do *software* e das aplicações. Também inclui procedimentos e políticas organizacionais.

A confidencialidade, integridade e disponibilidade de dados, numa perspectiva regulamentar, dependem das políticas e legislação nacionais de segurança cibernética. A segurança dos dados (incluindo confidencialidade, integridade e disponibilidade) também não depende da localização física dos servidores que albergam tais dados. É antes uma função das regras normativas - incluindo normas, políticas, regulamentos, leis e protocolos (tais como normas de dados e interfaces técnicas), e a implementação de tecnologias e medidas de segurança (tais como encriptação, firewalls e controlos de acesso) - que são implementadas por prestadores de serviços públicos ou privados na forma como armazenam, acedem, partilham e utilizam os dados.

O aumento da legislação sobre segurança de dados e as medidas técnicas podem tanto melhorar a confidencialidade, integridade e disponibilidade (segurança positiva) como prejudicar a liberdade fundamental e os direitos de privacidade, dignidade e segurança em linha (segurança negativa). Por exemplo, para proteger a segurança dos dados dos utilizadores, alguns países podem impor restrições à partilha e transferência de dados através da promulgação de legislação sobre segurança cibernética. Estas podem ser barreiras ao livre fluxo de dados. De uma perspectiva de segurança cibernética, alguns estados

podem acreditar que os dados são mais seguros se forem armazenados dentro das fronteiras nacionais. Os Estados podem erroneamente referir-se a ela como princípios de soberania de dados, enquanto estas medidas são simplesmente formas de proteccionismo de dados e localização de dados.

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

Recomendações

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

Acções

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

5.4.5 Fluxos de dados transfronteiriços

Uma questão cada vez mais importante no que se refere ao comércio internacional e regional é a transferência transfronteiras de dados pessoais e outros (Deloitte, 2017). No contexto africano, os quadros internacionais e regionais que facilitam as transacções transfronteiriças e o fluxo de dados pessoais através dos países são essenciais para a criação de mercados comuns e, em particular, para a realização da Zona de Comércio Livre Continental Africana. A transferência transfronteiriça de dados pessoais, em particular, é moldada pela abordagem de soberania de dados que um país pretende seguir, que se refere ao princípio jurídico de que a informação (geralmente em formato electrónico) é regulada ou regida pelo regime jurídico do país em que esses dados residem. Como referido, este conceito é desafiado pela realidade moderna dos movimentos de dados. As críticas à suposta narrativa de "fluxos de dados" e à extensão dos seus benefícios para os dividendos digitais no desenvolvimento devem, no entanto, ser reconhecidas, bem como o reconhecimento de que quantidades significativas de

fluxos de dados ocorrem de facto horizontalmente dentro das empresas, e não entre empresas (Conferência das Nações Unidas sobre Comércio e Desenvolvimento, 2021).

Importa também mencionar a posição comum segundo a qual a transferência de dados depende do facto de o país receptor ter ou não um nível de protecção adequado (Razzano, Calandro, et al., 2020). No entanto, o que corresponde a este nível "adequado" será frequentemente determinado pela Autoridade de Protecção de Dados de um país, ou similar. Assim, na ausência de uma lei de protecção de dados no país receptor, a transferência de dados pessoais não pode ser sujeita a regulamentação adequada, a menos que a lei de um país proíba a transferência de dados excepto para um país com um nível de protecção adequado, ou através do estabelecimento de obrigações bilaterais através de contratos entre as partes transferidoras.

A realidade é que amplas limitações à transferência transfronteiriça de dados poderiam resultar em oportunidades de negócio perdidas, e reduzir a capacidade de uma organização para negociar internacionalmente, levando a uma redução da pegada geográfica e à perda de competitividade no mercado. A regulamentação de dados que é sincronizada com os regulamentos de outras jurisdições contribui para a confiança mútua e estabelece uma base para um intercâmbio de dados de confiança, incluindo (mas não se limitando a) dados pessoais. Neste sentido, a regulamentação da protecção de dados pessoais permite e melhora a confiança e o comércio na circulação transfronteiriça de pessoas, bens e serviços (Sociedade da Informação, 2018).

Recomendações

- Os quadros de protecção de dados devem fornecer normas mínimas para os fluxos de dados transfronteiriços;
- A especificidade dos dados deve ser priorizada para evitar restrições não intencionais à partilha de dados produtivos;
- As considerações de aplicação da lei devem ser incorporadas no processo de elaboração de políticas;
- Para garantir uma resolução transfronteiras eficaz, é necessário garantir um certo grau de capacidade entre as agências.
- Os membros da União Africana devem definir rigorosamente um quadro e modalidades para regular os fluxos de dados transfronteiriços e identificar a entidade africana e as pessoas com direito a gerir este sistema.

Acções

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

5.4.6. Procura de dados

Embora haja dados significativos e recomendações de economia digital que se relacionam com a ajuda à criação de um ecossistema de dados mais amplo, há também intervenções políticas específicas a serem prosseguidas em relação à estimulação de dados do lado da procura. Os utilizadores de dados podem ser o sector público, as empresas privadas (de diferentes dimensões), bem como os utilizadores individuais e os cidadãos. No entanto, a capacidade precisa ser desenvolvida através desses perfis para estimular a demanda por dados, culturas de dados e inovação. O papel da política na promoção do uso produtivo de dados entre as partes interessadas é facilitado pelas áreas políticas anteriores, mas também pode exigir

considerações mais específicas. Isto é especialmente o caso dado que a realidade dos dados para muitos atores locais dentro do ecossistema de dados é de escassez de dados, em vez de saturação.

Recomendações

- As comunidades de dados devem ser priorizadas na política de inovação. Estas comunidades exigem incentivos e apoio à política interna, incluindo a promoção activa de centros de dados e outras formas de inovação comunitária que possam ajudar a gerar competências de dados e culturas de dados;
- A provisão regulamentar para a gestão de dados deve incluir a provisão de caixas de areia regulamentares para incentivar o desenvolvimento de dados locais.

Acções

- As comunidades de dados devem ser incorporadas nos processos de elaboração de políticas de dados pelos decisores políticos;
- As comunidades de dados devem ser atraídas para o estabelecimento de iniciativas abertas de dados governamentais por entidades responsáveis pela implementação a nível dos departamentos;
- As universidades devem ser incluídas como intervenientes políticos relevantes para ajudar a estabelecer a "base de conhecimentos" da qual a economia de dados local pode retirar conhecimentos científicos e tecnológicos suficientes.

5.4.7 Governação de Dados para Sectores e Categorias Especiais de Dados

Certas categorias de dados e certos sectores específicos, requerem uma gestão de dados adaptada que tenha em conta as questões particulares que afectam essa categoria ou sector. Categorias como dados de saúde ou dados infantis não são as mesmas que tipologias sectoriais específicas, como dados financeiros, mas ambas podem exigir um tratamento distinto. Contudo, o tratamento especial cria uma ameaça de silos de dados que tornam os dados menos utilizáveis e podem aumentar os custos de conformidade, especialmente se existirem regulamentos ou requisitos incompatíveis. O tratamento especial é por vezes necessário, mas deve estar em harmonia com a governação geral dos dados e este quadro político.

Uma recomendação fundamental de Acesso aos Dados e Interoperabilidade é que os tipos de dados que requerem consideração especial sejam identificados e claramente especificados de modo a que o acesso especial e outros requisitos em relação a esses dados se integrem com as regras gerais de dados. Conforme discutido no âmbito da Localização de Dados, tipos de dados claramente especificados são por vezes sujeitos a requisitos de localização de dados na prossecução de objectivos políticos peculiares ao tipo de dados. Nas recomendações sobre Processamento e Protecção de Dados recomenda-se que os códigos de conduta, sujeitos à aprovação da DPA nacional, possam ser utilizados para requisitos específicos do sector.

Recomendações

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

5.5. Governação Internacional e Regional

A nível transnacional e continental - particularmente para proporcionar capacidade de segurança cibernética e para responder às preocupações de protecção de dados associadas às mudanças na economia

de dados - a cooperação entre países é de importância crescente. O âmbito da cooperação necessária inclui o diálogo entre os governos, a colaboração com o sector privado e processos eficazes e integrados para investigar e processar violações transfronteiras. Uma arquitectura de confiança global que tenha em conta as limitações dos sistemas nacionais existentes ou outros sistemas fragmentados é essencial para assegurar uma economia digital e a inclusão digital (Banco Africano de Desenvolvimento de 2019).

Certas iniciativas a nível internacional e continental servem como um passo fundamental para precipitar a implementação.

Por exemplo, a União Africana e as iniciativas regionais sobre dados genéticos codificados digitalmente e dados geográficos e ambientais, respectivamente. A Comissão da União Africana assegurará a harmonia entre estas iniciativas e o trabalho em curso em matéria de política de dados[51].

Recomendações:

A União Africana com o apoio de organizações panafricanas irmãs deve:

- Facilitar a colaboração entre as várias entidades que lidam com dados em todo o continente através do estabelecimento de um quadro de consulta no seio da comunidade do ecossistema digital para salvaguardar os interesses de cada actor.
- Reforçar as ligações com outras regiões e coordenar as posições comuns africanas sobre as negociações internacionais relacionadas com dados, a fim de assegurar a igualdade de oportunidades na economia digital global.
- Apoiar o desenvolvimento de infra-estruturas de dados regionais e continentais para albergar tecnologias avançadas orientadas para os dados (tais como Grandes Dados, Aprendizagem de Máquinas e Inteligência Artificial) e o necessário ambiente facilitador e mecanismo de partilha de dados para assegurar a circulação através do continente;

5.5.1 Normas de dados continentais

Como forma de facilitar a cooperação transfronteiriça, é importante alcançar um consenso sobre normas de dados, o que é uma consideração integral para o avanço da interoperabilidade. Estas formas de consenso de vários intervenientes devem fazer referência ao trabalho realizado através da Organização Internacional de Normalização, e outras formas de consenso internacional alcançado em contextos sectoriais específicos. No entanto, embora a normalização internacional seja importante para a competitividade, é de notar que estas normas internacionais podem não ser suficientes para as necessidades da região. Isto é demonstrado, por exemplo, nos desafios linguísticos evidenciados no contexto dos dados espaciais ou geográficos (Cooper e Majeke xx).

Recomendações

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

Acções

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

51 The Regional Data Strategy for Marine and Coastal Areas Management in Western Africa promotes more sustainable management of natural resources through mutual sharing of data.

5.5.2 Portal aberto de dados e outras iniciativas

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

5.5.3 Instrumentos continentais

A vasta gama de instrumentos relevantes existentes está descrita no apêndice B. No entanto, há duas áreas específicas que precisam de ser destacadas.

Mecanismo de fluxo de dados transfronteiras

Há uma oportunidade de aproveitar este enquadramento para iniciar a colaboração no sentido de um mecanismo regional de fluxo transfronteiriço de dados, facilitado por um instrumento abrangente, como o da OCDE e da ASEAN (ver mais adiante Apêndice B).

Convenção da UA sobre Segurança Cibernética e Protecção de Dados Pessoais

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

Zona de Comércio Livre Continental Africana

A ZCLCA oferece uma oportunidade de cooperação em vários aspectos importantes do quadro político, de forma mais saliente no desenvolvimento dos acordos sobre concorrência, propriedade intelectual e investimento.

Recomendações

- Promover e facilitar os fluxos de dados dentro e entre os Estados-membros da UA através do desenvolvimento de um Mecanismo de Fluxos de Dados Transfronteiriços que tenha em conta o contexto africano, nomeadamente os diferentes níveis de prontidão digital, maturidade dos dados, bem como ambientes legais e regulamentares.
- Facilitar a circulação de dados entre sectores e entre fronteiras, desenvolvendo um Quadro Comum de Categorização e Partilha de Dados que tenha em conta os tipos alargados de dados e os seus diferentes níveis de privacidade e segurança.

- Trabalhar em estreita colaboração com as autoridades nacionais responsáveis pela protecção de dados pessoais dos Estados-membros da UA, com o apoio da Rede Africana de Autoridades (RAPDP), para estabelecer um mecanismo e órgão de coordenação que supervisiona a transferência de dados pessoais dentro do continente e assegura o cumprimento das leis e regras existentes que regem a segurança de dados e informações a nível nacional;
- Permitir a partilha de dados e uma maior interoperabilidade entre os Estados-membros da UA e outros mecanismos da UA, incluindo o Mecanismo de Cooperação Policial da União Africana (AFRIPOL).

- Trabalhar para a construção de um ciberespaço seguro e resistente no continente que ofereça novas oportunidades económicas através do desenvolvimento de uma Estratégia de Segurança

Cibernética da UA e do estabelecimento de Centros Operacionais de Segurança Cibernética para mitigar riscos e ameaças relacionadas com ciberataques, violações de dados e utilização indevida de informação sensível.

- Estabelecer mecanismos e instituições, ou conferir poderes aos existentes, no âmbito da União Africana para reforçar as capacidades e prestar assistência técnica aos Estados-membros da UA para a aplicação nacional deste quadro de política de dados.
- Recomenda-se que a negociação do capítulo de concorrência da ZCLCA estabeleça normas mínimas para garantir que os dados não pessoais de propriedade exclusiva sejam acessíveis a inovadores, empresários e outros da cadeia de valor, com o objectivo de incentivar a concorrência em todo o continente.
- Os membros da ZCLCA devem considerar a inclusão de disposições no capítulo da concorrência que conferem às autoridades da concorrência o mandato de considerarem também os efeitos da estrutura do mercado em termos de segurança e privacidade. Isto é importante para evitar a concentração de corretores de dados ou plataformas, tanto a nível nacional como regional, uma vez que isto cria o risco de um único ou poucos pontos de falha com consequências de grande alcance.
- Os membros da ZCLCA devem igualmente considerar a inclusão no capítulo da propriedade intelectual da ZCLCA de disposições que clarifiquem o estatuto dos dados relativamente à propriedade intelectual, em particular:

  - que se os direitos de autor forem alargados a bases de dados e compilações de dados que só se aplicam quando as bases de dados e compilações são criadas por autores humanos e exibem originalidade e que os direitos de autor se estendem apenas à reprodução da selecção e disposição original dos dados na base de dados e não aos dados em si;
  - que qualquer direito de autor ou outro direito de propriedade intelectual, incluindo segredos comerciais que permitam o controlo de dados, não se aplica aos dados pessoais; e
  - que qualquer direito de autor ou outro direito de propriedade intelectual, incluindo segredos comerciais que permitam o controlo de dados, é limitado pelas disposições da regulamentação da concorrência.

Acções

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

5.5.4 Instituições e associações continentais e regionais

As instituições e associações regionais criam um mecanismo central para criar uma voz regional unificada em questões de dados. Muitas associações já existem, e garantir a implementação deste quadro fala às

associações existentes é uma recomendação prioritária. Os organismos continentais e regionais são particularmente importantes devido à natureza transfronteiriça do fluxo de dados necessário para beneficiar dos dados.

Comunidades económicas e de desenvolvimento regionais

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

Juízes dos direitos humanos

O Tribunal Africano dos Direitos Humanos e dos Povos, o Tribunal de Justiça da África Oriental e o Tribunal Comunitário de Justiça da CEDEAO proporcionam fóruns e capacidade especializada para julgar disputas complexas sobre privacidade e igualdade, que são relevantes para a protecção de dados pessoais e a utilização de dados para discriminar injustamente.

O Tribunal da SADC, uma vez recapitulado, poderia também oferecer um fórum para disputas de dados, embora dentro de um mandato mais limitado. Os mecanismos continentais e regionais de adjudicação estão em melhor posição para resolver litígios transfronteiriços de dados

Rede Africana de Reguladores de Dados

Capacitar as APD e melhorar o nível de aplicação dos quadros legislativos e regulamentares a nível nacional contribuem significativamente para o gozo dos direitos digitais por parte dos indivíduos. Uma via para esta capacitação é através da promoção e apoio das associações reguladoras existentes, tais como a Rede Africana de Reguladores de Dados.

Associações de Autoridades Reguladoras das TIC

Existem associações das TIC tais como a Associação Regional de Reguladores (ARTAC, WATRA, CRASA e EACO). Podem também facilitar a colaboração e a partilha de conhecimentos à medida que são explorados instrumentos e normas transfronteiriças.

Associações Sectoriais

Associações sectoriais como o Fórum Africano de Administração Fiscal serão necessárias para ajudar a concretizar as áreas de recomendações de economia de dados em particular. Dada a importância da identidade digital na economia de dados, a Associação de Registadores Nacionais é também importante.

Fórum Africano da Concorrência

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

Recomendações

- Reforçar a cooperação regulamentar e a partilha de conhecimentos entre países e regiões africanas, através do reforço das capacidades da Rede Africana de Autoridades de Protecção de Dados e à Associação Regional de Reguladores das TIC.
- Os mecanismos de adjudicação continental e regional existentes devem ser explicitamente autorizados a lidar com questões de dados que estejam implicadas em direitos digitais e direitos de dados, e disputas transfronteiriças de dados.
- As autoridades fiscais africanas devem colaborar através do Fórum Africano de Administração Fiscal (ATAF) para desenvolver uma posição africana que represente mais eficazmente o interesse comum no processo de reformas fiscais internacionais, tais como o BEPS.

- Criar um Fórum Anual de Inovação de Dados para África para servir de plataforma para discussões entre múltiplos intervenientes, facilitar o intercâmbio entre países e sensibilizar os decisores políticos para o poder dos dados como o motor da economia digital actual.

5.6. Quadro de Implementação

5.6.1 Fases do Quadro de Implementação

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

	Actividade	Descrição	Responsabilidade de Liderança
FASE 1: ADOPÇÃO DO QUADRO			
A	Os Estados-membros adoptam um quadro		Membros
B	Concepção de Monitorização para o Quadro	Criação de um quadro de monitorização de alto nível,	CUA
C	Estabelecer ou dar poder a um mecanismo dentro da UA para centralizar os compromissos regionais sobre dados	Actividades para incluir apoio à implementação, coordenação sobre normas de dados, e outras áreas específicas enunciadas nas recomendações que requerem colaboração regional.	CUA
FASE 2: ADESÃO/APROPRIAÇÃO			
A	Avaliar o Quadro Continental	Assegurar o alinhamento com os instrumentos continentais.	CUA, CER, AUDA-NEPAD, Smart Africa
B	Envolver as Estruturas Continentais	Envolver as estruturas associadas em potenciais áreas de colaboração na implementação do quadro.	CUA
C	Avaliar o Quadro Continental	Ênfase nos princípios, explorar o alinhamento com quadros de estruturas internacionais.	CUA
D	Envolver Estruturas Internacionais		CUA, Estados-membros da UA
FASE 3: APOIO CONTINENTAL AOS ESTADOS-MEMBROS PARA SATISFAZEREM AS CONDIÇÕES PRÉVIAS			
A	Desenvolver infra-estruturas de banda larga e quadros regulamentares	Implementação de políticas mais amplas iniciada em relação ao ambiente de dados facilitador, a nível interno.	CER, AUDA-NEPAD, ATU, PAPU, SMART AFRICA
Fase 4: Enquadramento			
A	Envolvimento com várias partes interessadas	Promover o Quadro Político, envolver os intervenientes internos.	Membros, sector privado, sociedade civil,

B	Iniciar a adesão de múltiplas partes interessadas	Reflexão sobre o mapeamento das partes interessadas na Fase Dois*, garantir o alinhamento das políticas.	Membros
C	Instrumento aplicado a nível interno	Desenvolver Quadros Jurídicos e Regulamentares estabelecer um regulador de dados e um sistema de governação de dados	Membros
D	Quadro orçamental	Alocar recursos para implementação	Membros
FASE 5: COLABORAÇÃO			
A	Envolver Fóruns Internacionais de Tomada de Decisões	Envolver fóruns de elaboração de regras sobre normas e regras de dados (ver mapeamento das partes interessadas).	Estados-membros da UA
B	Monitorização da implementação dos membros		CUA, CER, AUDA-NEPAD, Smart Africa
C	Sensibilizar para o mecanismo continental centralizador de dados.	Aceitar pedidos directos de assistência	CUA, Instituições Regionais
D	Participar em actividades continentais	Participar nas actividades continentais delineadas na Secção 10.	Membros

5.6.2 Mapeamento das partes interessadas

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

DESCRIÇÃO	SUBTIPOS	FINALIDADE
INTERNACIONAL		
Nações Unidas	União Internacional das Telecomunicações, Departamento de Segurança e Protecção das Nações Unidas	Alinhamento da política de desenvolvimento
Organizações Multilaterais	Organização para a Cooperação e Desenvolvimento Económico, Banco Mundial	Alinhamento da política económica
Estruturas de Governação da Internet	Fórum de Governação da Internet, Grupo de Trabalho de Engenharia da Internet, Corporação para Atribuição de Nomes e Números na Internet	Alinhamento da política digital e da Internet
Normas internacionais	Organização Internacional de Normalização	Alinhamento da padronização dos dados
Organizações multilaterais (sectoriais)	Organização Mundial de Saúde, Organização Mundial do Comércio	Alinhamento das componentes sectoriais de política
REGIONAL		
Comunidades Económicas Regionais	CEDEAO, SADC, CAO, CEEAC, COMESA, IGAD, CEN-SAD , UMA	Alinhamento da política económica e de desenvolvimento
Estruturas de Governação da Internet	AFRINIC, IGF Africano	Alinhamento da política digital e da Internet
Comunidade Regional (regulamentar)	Rede de Autoridades Africanas de Protecção de Dados, Outras Associações Reguladoras, Fórum Africano de Administração Fiscal	Alinhamento das políticas transfronteiras
Comunidade regional (sectorial)	Banco Africano de Desenvolvimento	Alinhamento das componentes sectoriais de política
INTERNO		
Departamentos Nacionais	Telecomunicações, Justiça, Cooperação Internacional, Segurança do Estado	Alinhamento de políticas
Agências estatísticas		Capacitação
Autoridades reguladoras	Protecção de dados, Regulamento sobre TIC, Concorrência	Implementação

A nível de empresa	Comités de Governação de Dados	Capacitação, envolvimento de várias partes interessadas

Recomendações:

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

D/Statistics/Documents/facts/FactsFigures2019.pdf

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Schmidt, C. O., Struckmann, S., Enzenbach, C., Reineke, A., Stausberg, J., Damerow, S., Huebner, M., Schmidt, B., Sauerbrei, W., & Richter, A. (2021). Facilitating harmonized data quality assessments. A data quality framework for observational health research data collections with software implementations in R. BMC Medical Research

Methodology, 21(1), 63. https://doi.org/10.1186/s12874-021-01252-7

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

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

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

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

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

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

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

Wook, M., Hasbullah, N. A., Zainudin, N. M., Jabar, Z. Z. A., Ramli, S., Razali, N. A. M., & Yusop, N. M. M. (2021). Exploring big data traits and data quality dimensions for big data analytics application using partial least squares structural equation modelling. Journal of Big Data, 8(1), 49. https://doi.org/10.1186/s40537-021-00439-5

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

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

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

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

ANEXO - DEFINIÇÕES DE TRABALHO

A classificação de dados é definida como o processo de organização de dados por categorias relevantes para que possam ser utilizados e protegidos de forma mais eficiente.

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

Ecossistema de dados - para os fins aqui utilizados não só para as linguagens de programação, pacotes, algoritmos, serviços de computação em nuvem e infra-estruturas gerais que uma organização utiliza para recolher, armazenar, analisar e aproveitar dados, mas também para a cadeia de valor subjacente associada aos dados como factor de produção, a governação dos sistemas de dados e a protecção dos sujeitos dos dados.

A **minimização dos dados** é um princípio dentro dos quadros de protecção de dados, o que reforça a recolha da quantidade mínima de dados pessoais necessários para fornecer um elemento individual de um serviço ou produto.

A **publicação de dados** refere-se ao processo através do qual as interacções diárias dos seres vivos podem ser transformadas num formato de dados e colocadas em uso social e económico.

O **comércio electrónico** pode ser resumido como transacções comerciais que ocorrem através de canais electrónicos - compra e venda de bens ou serviços via Internet, e transferência de dinheiro e dados para completar as vendas - por métodos especificamente concebidos para efeitos de recepção ou colocação de encomendas.

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

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

A **identidade digital** é um conjunto de atributos e/ou credenciais electronicamente captados e armazenados que identificam de forma única uma pessoa, permitindo a distinção de um indivíduo de outro.

Capacidade digital é o termo utilizado para descrever as competências, alfabetização, normas sociais e atitudes de que indivíduos e organizações necessitam para prosperar, para viver, aprender e trabalhar numa sociedade e economia digital.

O **consentimento** da pessoa em causa significa qualquer indicação livre, específica, informada e inequívoca da vontade da pessoa em causa pela qual esta, através de uma declaração ou de uma acção afirmativa clara, manifesta a sua concordância com o tratamento dos dados pessoais que lhe dizem respeito.

Por **responsável pelo tratamento de dados** entende-se qualquer pessoa singular ou colectiva, pública ou privada, qualquer outra organização ou associação que, sozinha ou em conjunto com outras, decida recolher e tratar dados pessoais e determine as finalidades.

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

As **Autoridades de Protecção de Dados (APD)** são autoridades públicas independentes que controlam e supervisionam, através de poderes de investigação e correctivos, a aplicação da lei de protecção de dados. Prestam aconselhamento especializado sobre questões de protecção de dados e tratam queixas que possam ter infringido a lei.

Por **pessoas em causa** entende-se qualquer pessoa singular que seja objecto de tratamento de dados pessoais.

A **harmonização** assegura a uniformidade dos sistemas através da utilização de normas mínimas para facilitar a interoperabilidade e quadros jurídicos e de confiança (por exemplo, para níveis de garantia) para estabelecer regras e criar confiança nos respectivos sistemas.

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

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

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

Por **dados pessoais** entende-se qualquer informação relativa a uma pessoa singular identificada ou identificável através da qual essa pessoa possa ser identificada, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a factores mais específicos da sua identidade física, fisiológica, mental, económica, cultural ou social.

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

2022-01-20

Report of the 4th Ordinary Session of the STC on Communication and ICT (STC-CICT), 25-27 October 2021

African Union

DCMP