United Nations
Economic Commission for Africa

DRAFT

POLICY DECLARATION ON

The African contribution to the global digital compact, following the African regional review meeting

4 and 5 July 2023
Cape Town, South Africa

To order copies of *Draft policy declaration on the African contribution to the global digital compact, following the African regional review meeting*, please contact:

Publications Section
Economic Commission for Africa P.O. Box 3001
Addis Ababa, Ethiopia
Tel: +251 11 544-9900
Fax: +251 11 551-4416
E-mail: eca-info@un.org
Web: www.uneca.org

First printing October 2023

Designed and printed in Addis Ababa, Ethiopia by the ECA Printing and Publishing Unit.
ISO 14001:2015 certified. Printed on chlorine free paper

TABLE OF CONTENTS

I. Introduction

1. On the occasion of the seventy-fifth anniversary of the founding of the United Nations, marked in September 2020, the Secretary-General released a report titled "Our Common Agenda", which contains a proposal for a global digital compact to be agreed at the Summit of the Future, to be held in September 2024.[1] The aim of the Summit is to reinvigorate the global multilateral institutions for the 2030s and beyond through a technology track involving a wide range of stakeholders. It is expected that the global digital compact will "outline shared principles for an open, free and secure digital future for all". In preparation for the Summit and the proposed digital compact, the United Nations is seeking inputs from a wide range of stakeholders. The global digital compact is an opportunity to reinterpret the collective approach to the best way to respond to the constantly changing digital society and accelerate progress towards the achievement of the Sustainable Development Goals.

2. As part of that process, the Economic Commission for Africa (ECA) called for a multi-stakeholder consultation meeting to deliberate and prepare an African contribution to inform the global digital compact. The meeting was held on 4 and 5 July in Cape Town, South Africa, and gathered insight focused on African infrastructure development; digital public goods; the regulation of emerging technology, including artificial intelligence; digital trust; data protection; and human rights, among other topics. The meeting brought together experts, policymakers and stakeholders from 32 members of ECA, representing government, the private sector, civil society and academia. The present report serves as an outcome document from that meeting, and contains the key insight and inputs from the stakeholder deliberations, which were structured around the following eight thematic priorities:

   (a) Infrastructure development and access;
   (b) Digital public infrastructure;
   (c) Emerging technology: risks and opportunities for Africa;
   (d) Regulation of emerging technology;
   (e) Digital trust, data protection and human rights;
   (f) Avoiding the risk of Internet fragmentation;
   (g) Digital capacity-building;
   (h) Public goods and digital commons.

1 A/75/982.

II. Infrastructure development and access

3. Although significant progress has been made in recent years in relation to the roll-out of broadband infrastructure and Internet penetration in Africa, challenges and gaps still exist in terms of geographical coverage and Internet penetration.

4. Submarine cable systems, such as the West Africa Cable System and the Eastern Africa Submarine Cable System, have expanded connectivity to coastal regions, and national and regional broadband initiatives, including those of Kenya and Nigeria, have been implemented to improve infrastructure. Broadband infrastructure in rural and remote areas is still limited, however, leading to a significant divide between urban and rural settings in access to high-speed Internet.

5. According to the International Telecommunication Union (ITU), Internet penetration rates in Africa reached 40 per cent in 2022, compared with a global rate of 66 per cent.[2] Internet penetration rates vary significantly among countries, with some countries surpassing the continental average, while others lag behind. Such countries as Kenya, Morocco and South Africa have achieved relatively higher Internet penetration rates, owing to more extensive infrastructure development and higher urbanization rates. Many countries in Africa, however, still face low Internet penetration, in particular in rural and underserved areas. A widening usage gap is especially prevalent on the continent. The GSM Association reports that, while access to mobile broadband coverage continues to grow, reaching 83 per cent in 2021,[3] only 40 per cent of Africans are connected to the Internet.[4] The challenges that contribute to the usage gap are the high cost of Internet services, infrastructure gaps and socioeconomic factors hampering mobile internet adoption. Furthermore, ITU has reported that the gender digital divide was the highest in Africa in 2022 compared with other regions of the world, with an 11-percentage point difference in favour of men.[5]

6. Infrastructure is a key challenge, given the low level of connectivity. According to the Broadband Commission for Sustainable Development, connecting an additional 1.1 billion people online globally by 2030 and bridging the connec-

2 ITU, "Internet use", available at www.itu.int/itu-d/reports/statistics/2022/11/24/ff22-internet-use/.
3 Anne Delaporte, "New insights on mobile Internet connectivity in sub-Saharan Africa", GSM Association, 20 January 2023.
4 ITU, "Internet use".
5 ITU, "The gender digital divide", available at www.itu.int/itu-d/reports/statistics/2022/11/24/ff22-the-gender-digital-divide/.

tivity gap will cost $100 billion.6 The lack of adequate infrastructure in remote and rural areas poses a significant challenge to achieving widespread connectivity. Limited terrestrial infrastructure, such as fibre-optic networks, in remote regions makes it difficult to extend broadband services. Geographical barriers – including vast landscapes, challenging terrains and inadequate road networks – hinder the expansion of infrastructure.

7. The provision of Internet services to end users remains a significant challenge in Africa. The high cost of extending connectivity to remote areas with low population densities reduces the economic viability for service providers. A lack of community infrastructure, such as telecommunication towers and network coverage, limits Internet access for individuals and businesses.

8. Addressing the challenges and gaps in Internet infrastructure and connectivity is crucial for achieving digital inclusivity and unlocking the transformative potential of digital technology in Africa. In the context of the global digital compact, efforts towards achieving that goal shall focus on enhancing and expanding broadband connectivity, in particular in remote and underserved areas, which will involve promoting public-private partnerships, attracting investment and leveraging innovative technology to bridge the digital divide.

A. Core principles

9. All stakeholders should adhere to the following principles:

(a) Policies for national infrastructure development must address all geographical areas where social life exists, taking into consideration the specific needs and challenges of all communities, and thereby helping to ensure that connectivity is within reasonable physical reach for everyone, enabling equitable access to digital resources, opportunities and an adequate development path for the digital transformation of every community in its own way;

(b) Regulatory frameworks must be designed to accommodate a diverse range of connectivity providers, allowing for the coexistence of various economic and organizational models for the provision of Internet connectivity, and embracing community networks and small and medium-sized cooperatives as local service providers or operators;

(c) Given that many Governments in Africa lack the resources, expertise or political will to make a significant investment in digital infrastructure, the development of that infrastructure on the continent requires the participation of the private sector, which can: help to build and operate digital infrastructure, such as fibre-optic networks, data centres and mobile networks; provide the digital services – including cloud computing, e-commerce platforms and mobile financial services – that require that infrastructure, helping to improve connectivity and access to information and services, and drive economic growth; collaborate with Governments and other stakeholders to create an enabling policy environment that supports digital infrastructure development, such as

6 Broadband Commission for Sustainable Development, Connecting Africa Through Broadband: A Strategy for Doubling Connectivity by 2021 and Reaching Universal Access by 2030 (2019).

by advocating policies that promote competition, innovation and investment; and engage in public-private partnerships to share in the investment and development of digital infrastructure;

(d) Policies and regulations must allow for diversity in the types of connectivity infrastructure, and the technology and equipment that can be used to improve connectivity and bridge connectivity gaps, by giving consideration, for example, to satellite communications, television white space and innovative spectrum assignment approaches, in particular those enabling dynamic spectrum access and spectrum-sharing.

B. Recommendations

10. Stakeholders should make commitments or take action in the following ways:

(a) Consult local communities and stakeholders when devising policy and making decisions for infrastructure development;

(b) Create multilevel enabling policies and regulatory environments, not only to cater to larger national stakeholders based in capital cities, but also to accommodate local community stakeholders willing to establish their own community networks;

(c) Maintain a continuous capacity-building programme for regulators to reduce the delay between the recognition of a better practice anywhere in the world and the decision to apply that practice to address relevant issues;

(d) Facilitate innovative financing mechanisms;

(e) Improve the affordability and accessibility of Internet services, especially in underserved areas and marginalized communities, including by encouraging collaboration among Governments, telecommunication companies and other stakeholders to develop innovative strategies that reduce the cost of data and improve connectivity in remote regions;

(f) Explore alternative technology, such as community networks and shared infrastructure, to extend Internet access to underserved areas and support capacity-building for the implementation of that technology and those approaches to connectivity;

(g) Promote innovative financing mechanisms and provide financial support and investment for the development of digital infrastructure in Africa, in particular in unserved and underserved areas;

(h) Facilitate technology transfer and knowledge-sharing to enhance the African capacity to build robust and resilient digital infrastructure;

(i) Support public-private partnerships to accelerate the deployment of broadband networks and improve connectivity across the continent;

(j) Create an enabling environment that encourages private sector investment in digital infrastructure, such as through the introduction of policies that promote competition, innovation and investment, and the provision of incentives, including tax breaks and regulatory support;

(k) Prioritize investment in digital infrastructure development, including broadband connectivity and reliable electricity supplies, especially in unserved and underserved areas, and advocate policies that enhance connectivity, lower data costs and improve the quality and reliability of Internet services, bearing in mind that public-private partnerships can play a crucial role in expanding digital infrastructure and improving connectivity across the continent.

11. At the global level, stakeholders should:

(a) Address the infrastructure development data gap by carrying out infrastructure gap assessments, and by establishing international baselines and targets that are similar to targets and metrics proposed by ITU,7 such as by defining affordable Internet as pricing 1 gigabyte of mobile broadband data at 2 per cent or less of average monthly income or ensuring that entry-level broadband services in developing countries cost less than 2 per cent of monthly gross national income;

(b) Establish a global infrastructure innovation fund;

(c) Set a timeline to create a vision for the realization of the global digital compact (a 20-year timeline may be considered, with milestones to evaluate progress).

At the regional level, stakeholders should:

(a) Harmonize and standardize legislation and regulation to promote integration on the continent;

(b) Enhance affordability by promoting cross-border connectivity and pooling infrastructure procurement to eradicate duplication at all levels. Such concerted efforts, including those when African countries negotiate as one bloc, can have a significant impact on reducing costs and driving prices down;

(c) Harmonize institutional procedures to enable their interoperability and integration;

(d) Seek inward-looking solutions at the regional level, and build local manufacturing capacity (devices and other technology can be manufactured in Africa).

12. At the national level, stakeholders should:

(a) Reform the regulatory framework to allow private sector stakeholders to enter the market and dismantle monopolies, issuing licences to those that want to provide a service;

(b) Innovate and find creative solutions, including by:

7 For information on the targets, see ITU, “New UN targets chart path to universal meaningful connectivity”, 19 April 2022.

(i) Diversifying the types of connectivity infrastructure, technology and economic models – considering satellite Internet, spectrum sharing, community networks and cooperatives – that can be used to improve connectivity and bridge connectivity gaps;

(ii) Encouraging the creation of smart villages and Internet presence points in white areas using universal access funds efficiently, wherever available;

(iii) Improving digital literacy in sparsely populated areas;

(iv) Incentivizing private sector investment through favourable taxation systems;

(c) Use market and public interest mechanisms, with the appropriate incentives, to attract a wide range of market-driven and community-based parties to make innovative offers to address the infrastructure connectivity gaps in unserved and underserved areas, noting the widespread failure of universal service, and access funds to achieve their mission;

(d) Leverage taxation models, such as the model proposed by the Organisation for Economic Cooperation and Development on universal taxation levels for global companies;8

(e) Promote demand-driven decision-making to prioritize community needs;

(f) Separate infrastructure management from service management by establishing companies that are responsible for managing telecommunications infrastructure and opening their capital to the private sector;

(g) Reform the regulators of telecommunications to make them facilitators of the digital society, with a view to enabling them to engage complementary infrastructure or sectors – such as energy, finance, taxation, education and health – that are needed for a digital economy to thrive;

(h) Enact key legislation, focus on enforcement, encourage the adoption of laws that incentivize private sector investment and review taxation regimes – including, for example, the introduction of zero-rate terminals in rural areas.

8 For further information on the proposal, see Organisation for Economic Co-operation and Development, "International community strikes a ground-breaking tax deal for the digital age", 8 October 2021.

III. Digital public infrastructure

13. Digital public infrastructure refers to the solutions and systems that facilitate the efficient delivery of vital functions and services across society, encompassing the public and private domains in the digital environment.[9] Digital public infrastructure serves as a crucial driver for deep and sustainable transformation that aligns with international environmental agreements, such as the Paris Agreement and the 2030 Agenda for Sustainable Development. Those agreements present significant opportunities to enhance the quality of life for billions of people around the globe.

A. Core principles

14. All stakeholders should adhere to the following principles:

(a) Computer technology can streamline data collection, registration and storage, making the system of civil registration and vital statistics more efficient, and reducing manual paperwork and administrative burdens;

(b) Digital technology enables real-time data capture, reducing the risk of errors and improving the accuracy of vital statistics, leading to more reliable demographic data for policymaking, planning and resource allocation;

(c) Digital systems for civil registration and vital statistics can improve accessibility among remote and marginalized populations, and leveraging mobile devices and Internet connectivity can help to reach individuals in rural or underserved areas, ensuring their inclusion;

(d) Computer technology enables data interoperability among different government systems – such as civil registration, health, education and social services – which facilitates data-sharing and integration, leading to a more comprehensive understanding of population dynamics and the better coordination of services;

(e) All infrastructure development and innovation should consider emergencies and the sudden onset of disasters that could result in the loss of data, and include remedial measures.

9 For further information on digital public infrastructure, see Digital Public Goods Alliance GovStack Community of Practice, "GovStack definitions: understanding the relationship between digital public infrastructure, building blocks and digital public goods", May 2022.

B. Recommendations

15. Digital public infrastructure presents opportunities – such as electronic civil registration and vital statistics systems, digital identity platforms and e-government services – but it is important to understand the risks and address the challenges associated with the digital divide, the interoperability of systems, data privacy, the availability of technological infrastructure, collaboration and capacity-building, to ensure the inclusive and secure implementation of digital platforms.

16. Stakeholders should make commitments or take action in the following ways:

(f) Ensure equitable access and address the digital divide to avoid leaving populations behind, given that access to computer technology and Internet connectivity is not uniform across Africa, and that there is a risk that existing inequalities could be exacerbated;

(g) Introduce robust data protection measures to safeguard privacy and prevent unauthorized access or misuse of data, given that digital public infrastructure, including e-government systems, involve the collection and storage of sensitive personal information;

(h) Invest in infrastructure development to support reliable and sustainable technological solutions and prevent inadequate technological infrastructure – including power supplies, network coverage and information technology capacity – from presenting challenges to the successful implementation of digital systems;

(i) Build the capacity of the individuals who work with digital public infrastructure and ensure their digital literacy, given that the effective use of computer technology requires a skilled workforce with knowledge of digital systems and data management;

(j) Support service delivery by a variety of providers in order to prevent monopolies, while being mindful of the dangers of the private provision of public digital infrastructure;

(k) Build on demonstrated progress, such as fast payments and data-sharing;

(l) Mitigate weaponization and risks, and ensure the trustworthiness of cross-border data flows, by sharing regional digital public infrastructure and its associated resources.

IV. Emerging technology: risks and opportunities for Africa

17. New and emerging technologies – such as artificial intelligence, the Internet of things, the blockchain, quantum computing and robotics – are causing exponential changes globally. By 2030, products and services powered by artificial intelligence could contribute up to $15.7 trillion to the global economy, of which $1.2 trillion will come from Africa, Oceania and some Asian markets.[10] Generative artificial intelligence is transforming industries by analysing and modelling data effectively in ways that benefit human interaction with digital systems, leading to increased productivity and innovation. Generative artificial intelligence has garnered significant attention from investors, including venture capital firms and technology leaders. In 2022, such firms invested over $2 billion in that field,[11] with major players such as Microsoft and Google – which have a $10 billion stake in OpenAI and a $300 million stake in Anthropic, respectively – making substantial investments.[12,13] By 2025, data generated by artificial intelligence is expected to account for 10 per cent of all data produced,[14] which presents significant opportunities for sub-Saharan Africa, considering that the combined gross domestic product of that region in 2019 was $1.8 trillion.[15] The successful implementation of emerging technology presents a world of possibilities. Given the tremendous potential that the opportunity presents, it is appropriate to consider whether the existing technological infrastructure can enable Africa to capitalize on it, and whether the continent is ready.

A. Core principles

18. By working with a multitude of stakeholders, emerging technology can be designed with trust, inclusivity and affordability. Regulators should create an enabling environment – encompassing governance institutions, policies and laws – for an effective roll-out of emerging technology, taking into account the following core principles:

10 PricewaterhouseCoopers, Sizing the Prize: What's the Real Value of AI for Your Business and How Can You Capitalise? (2017).
11 Cristina Criddle and Tim Bradshaw, "Investors seek to profit from groundbreaking 'generative AI' start-ups", Financial Times, 9 December 2022.
12 Dina Bass, "Microsoft invests $10 billion in ChatGPT maker OpenAI", Bloomberg, 23 January 2023.
13 Hayden Field, "Ex-OpenAI execs raise $450 million for Anthropic, a rival A.I. venture backed by Google", CNBC, 23 May 2023.
14 Gartner, "Gartner identifies the top strategic technology trends for 2022", 18 October 2021.
15 World Bank Group, GDP (current US$) – sub-Saharan Africa. Available at https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=ZG (accessed on 13 September 2023).

(a) Appropriate policies, regulatory measures and a sectoral code of conduct should be introduced, including the creation of frameworks for data protection and sectoral regulation that are the basis for rules governing the transparency, liability, accountability and justification of artificial intelligence and redress for decision-making by artificial intelligence;

(b) International standards, cooperation and best practice should be promoted and adopted, with the aim of reducing risks, such as the identification of individuals through data, data selection bias, discrimination by artificial intelligence models and asymmetry in data aggregation;

(c) Safety and security challenges of complex artificial intelligence systems must be addressed, given their critical threat to fostering trust in artificial intelligence and big data for development;

(d) Collaboration should be sought with universities and other institutions working in artificial intelligence, and with the public and private sectors at the national, regional and international levels, to build capacity;

(e) Public and private stakeholders should work together to develop common resources, databases, platforms and tools that are open, use privacy as a safeguard and encourage development;

(f) Innovative regulatory instruments that offer flexibility, such as regulatory sandboxes and public policy laboratories, should be deployed, and Governments should establish cross-functional teams across ministries and tiers of government;

(g) Implementation and enforcement mechanisms for emerging technology, regulations and strategies should be strengthened through the coordination of various public and private sector stakeholders, tackling such issues as privacy of personal data and information security;

(h) Artificial intelligence for development should be ethical and trustworthy, fair and unbiased, transparent and explainable, responsible, accountable, robust and reliable.

B. Recommendations

19. Stakeholders should make commitments or take action in the following ways:

(a) Adapt the approach to regulation. Current regulatory models can be adaptive and innovative, given that they tend to rely on trial and error, and the co-design of standards and regulations. The feedback loops of adaptive regulation are much shorter than those of hard-law requirements, including statutes and treaties. Regulators can, therefore, use various soft-law tools and instruments – such as crowdsourcing, policy laboratories, codes of conduct and regulatory sandboxes – in the emerging technology governance process;

(b) Facilitate regulatory sandboxes, which can be safe spaces for testing innovative services and products without complying with regulations. The sandbox approach helps regulators to:

(i) Understand new technology better and collaborate with industry to establish rules for managing services, products and business models that stem from emerging technology;

(ii) Lower the cost and regulatory barriers for testing disruptive, innovative technology without negatively affecting consumers;

(iii) Create regulations for emerging technology on the basis of foreseeable outcomes.

Unlike input-based and traditional regulatory models, outcome-based and evidence-based regulations prescribe the achievement of measurable, desirable and specific results. They require objectives or outcomes, and do not depict the way the outcomes should be achieved. Outcome-based regulations can ensure positive results with the governance process, developing regulations or guidelines that regulators are trying to encourage;

(a) Create emerging technology regulations on the basis of possible risks. Risk-weighted regulation can be vital for start-up business models or businesses for which emerging technology is central, and for making digital products and services more effective. Through advanced analytics tools, such as artificial intelligence, data analysis can detect new trends and patterns, which is necessary for making products safer and more accurate, personalized and effective;

(b) Improve collaborative regulation – such as international coordination, self-regulation and coregulation – for the benefit of various parties, not only firms and regulators. Agencies from across the globe can collaborate and foster innovation to protect consumers from potential fraud and safety concerns;

(c) Enhance capacity-building in generative artificial intelligence systems, and raise awareness among stakeholders of the capabilities and limitations of generative artificial intelligence;

(d) Establish guidelines and protocols for the use of generative artificial intelligence, including by identifying appropriate use cases and setting limits on the types of content that can be generated. Generative artificial intelligence systems may be used to produce content that infringes on the intellectual property rights of others;

(e) Support the implementation of safeguards, such as by implementing appropriate oversight and review processes, to prevent generative artificial intelligence systems from being used for nefarious or malicious purposes;

(f) Monitor and evaluate the performance of generative artificial intelligence systems to ensure that they function as intended, and that any potential risks are adequately managed.

V. Regulation of emerging technology: artificial intelligence

20. Emerging technologies, including artificial intelligence, are aimed at developing machines and systems that can carry out tasks considered to require human intelligence, with limited or no human intervention. Such systems increasingly embody human dimensions and result in electro-mechanical devices that replace human beings. Predictability and transparency are, therefore, always a concern. Security, accountability and compliance must also always be questioned.

21. As artificial intelligence continues to transform society, the ways in which its evolution affects society should be a priority consideration for regulation. As the impact of emerging technology on society is considered, the interaction of artificial intelligence, risks and regulation should also be given attention.

22. The principles that respond to the questions of how and when to regulate emerging technology – including artificial intelligence, machine learning and the Internet of things – should, therefore, be a priority area when diversifying applications to foster the economic development of the continent. The principles can lay a foundation for the way in which regulation is viewed in the rapidly changing world of technological development, and provide guidelines for overcoming the challenges associated with regulatory technology in Africa.

A. Core principles

23. By working with key stakeholders from the private sector, the not-for-profit sector and academia, regulators can ensure that they help to create an environment in which emerging technology is built with consumer safety, privacy and security in mind, and that digital products and services are as inclusive and affordable as they are innovative. Regulators should create an enabling environment – encompassing governance institutions, policies and laws – for an effective roll-out of emerging technologies.

24. Stakeholders should adhere to the following principles:

(a) Appropriate policies and regulatory measures – including the establishment of frameworks for data protection and sectoral regulation, and the promotion and adoption of international standards and international cooperation – should be prioritized;

(b) Regulators should ensure that adequate levels of data privacy, security and handling are in place – for example, by regulating against the use of data without consent, and by reducing the risk of identification of individuals through data, data selection bias and the resulting discrimination by artificial intelligence models and asymmetry in data aggregation;

(c) Safety and security challenges of complex artificial intelligence systems must be addressed, given their critical threat to fostering trust in artificial intelligence and big data for development;

(d) Public sector expertise in artificial intelligence and data must be developed, with leadership in relevant government institutions, through collaboration with universities and other institutions working in artificial intelligence, and with regional and international organizations;

(e) Rules governing the transparency, liability, accountability and justification of artificial intelligence and redress for decision-making by artificial intelligence should be created;

(f) Regulations should be innovative and agile through the deployment of public-private partnerships, in which public and private stakeholders work together to develop common resources, databases, platforms and tools that are open, use privacy as a safeguard, and encourage development. Innovative regulatory instruments that offer flexibility, such as regulatory sandboxes and public policy laboratories, should be deployed, and Governments should establish cross-functional teams across ministries and tiers of government;

(g) Implementation and enforcement mechanisms for emerging technology, regulations and strategies should be strengthened through the coordination of various public and private sector stakeholders, tackling such issues as privacy of personal data and information security;

(h) Emerging technology, such as artificial intelligence for development, must be ethical and trustworthy, fair and unbiased, transparent and explainable, responsible and accountable, robust and reliable, compliant with privacy standards, safe and secure, diverse and inclusive, and human- centred.

B. Recommendations

25. Stakeholders should make commitments or take action in line with chapter IV, section B, subparagraphs 20 (a) to (c) of the present report.

VI. Digital trust, data protection and human rights

26. The African Digital Transformation Strategy has highlighted the need for greater capacity to detect and mitigate digital threats and attacks. According to the Strategy, African governments have a fundamental responsibility to create an enabling environment, with policies and regulations that promote digital transformation across foundation pillars and cross-cutting themes, including cybersecurity. Addressing digital trust and security is the foundation for digital transformation in any society.

27. The relationship between human rights and digital technology is complex. Digital technology has transformed the avenues for promoting human rights, but the transborder nature of the Internet presents significant legislative and judicial challenges for existing legal and institutional human rights frameworks.

28. Although digital trust, data protection and human rights must be prioritized and the emerging legal and regulatory issues related to data protection and personal privacy must be addressed, there is a need to balance the interests of business and government in collecting, using and sharing personal data. Transparency and accountability are central to the promotion of human rights in the digital era, and therefore they are the guiding principles in the duty to promote and protect digital trust, data protection and human rights in general.

A. Core principles

29. Stakeholders should adhere to the following principles:

(a) Data subjects have rights to access, rectify, erase, restrict and port their personal data, and the right to object to certain processing;

(b) Personal data should be processed legally, fairly and transparently, and individuals should be informed about data usage;

(c) Personal data should be collected for specific, legitimate purposes, and incompatible processing should be avoided;

(d) Only necessary personal data should be collected and retained, and excessive or unnecessary collection should be avoided;

(e) Accuracy of personal data should be ensured and inaccurate information should be rectified or erased;

(f) Identifiable personal data should be kept only for as long as necessary, and should be securely deleted or anonymized when no longer needed;

(g) Personal data should be processed securely to prevent their unauthorized processing, loss, destruction or damage;

(h) Organizations should be responsible for complying with general data protection principles, similar to those that are embedded in the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and implement measures to demonstrate compliance;

(i) Personal data should be processed on lawful grounds, such as consent, contractual necessity, legal obligation, vital interest, public task or legitimate interest;

(j) Freely given, specific, informed and unambiguous consent should be obtained, and consent can be withdrawn;

(k) Civic education and best practices for preserving privacy and enabling trust in data handling should be central to the democratization of data literacy for greater equity;

(l) Resources should be allocated for open and responsive data systems for equitable benefit;[16]

(m) Data stewardship rights of indigenous people should be safeguarded;

(n) Resolution 38/7, on the promotion, protection and enjoyment of human rights on the Internet, adopted by the Human Rights Council on 5 July 2018,[17] and the norms, rules and principles for the responsible behaviour of States, as contained in the report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,[18] should be recognized.

B. Recommendations

30. To enhance data governance and privacy in Africa, stakeholders can take action and make commitments inspired by state-of-the-art practices from around the world, and help to align the continent with the best policies and practices relating to data governance and privacy. Stakeholders should make commitments or take action in the following ways:

(a) Advocate the development and implementation of comprehensive data protection legislation at the national level, aligned with global best practices, such as the General Data Protection Regulation of the European Union;

16 For further information, see World Bank Group, World Development Report 2021: Data for Better Lives (Washington, D.C., World Bank, 2021).
17 A/HRC/RES/38/7.
18 A/76/135.

(b) Adopt the concept of privacy by design and default, conducting a data protection impact assessment prior to implementing any technology project involving the collection or processing of personal data, and embedding privacy and data protection prior to building;

(c) Facilitate cross-border data flows, while ensuring the adequate protection of personal data by adhering to minimum standards;

(d) Raise awareness of data governance, privacy rights and best practices among individuals, organizations and government agencies, and conduct public awareness campaigns and educational programmes to inform individuals about their rights and responsibilities in relation to data privacy;

(e) Evaluate the implications of data localization requirements on privacy, innovation and economic growth, and develop a balanced approach that considers data sovereignty and the benefits of crossborder data flows;

(f) Foster collaboration among governments, private sector entities, civil society organizations and academia to develop and share best practices in data governance and privacy, and establish multistakeholder forums.

VII. Avoiding the risk of Internet fragmentation

31. As emphasized at the World Summit on the Information Society, it is crucial to uphold a unified, open and global Internet.

32. Internet fragmentation refers to the potential division or splintering of the global Internet into separate and disconnected networks, which has the potential to limit access to information, hamper cross-border flows and regional collaboration, and affect overall connectivity.

33. Considering the Internet as a network of networks, its fragmentation could occur in various scenarios and at various levels. It is crucial to acknowledge that governance can take place at multiple levels within that interconnected system.

34. Fragmentation at the technical level is the hindrance at the underlying infrastructure level that impedes the seamless interoperability and exchange of data packets among interconnected systems. An example of such fragmentation is the introduction of protocols that are incompatible with existing protocols, resulting in a lack of interoperability.

35. Fragmentation at the governance level is the introduction and implementation of policies and actions that constrain or prevent certain uses of the Internet to create, distribute or access information resources freely. Fragmentation at the governance level includes such practices as content censorship, data localization, geolocalization and geoblocking, and the implementation of cybersovereignty policies and laws that promote the creation and maintenance of walled gardens on the Internet. Those measures contribute to fragmentation by restricting access to information and limiting the free flow of data across borders, which, in the African context, worsens the digital divide among the privileged and the underserved.

36. Fragmentation at the process level refers to the fragmented efforts within various intergovernmental Internet governance processes at the regional and global levels, including the Internet Engineering Task Force, the World Summit on the Information Society, the Internet Governance Forum and the global digital compact. Such fragmentation highlights the need for cooperation and collaboration across the various processes to ensure a more cohesive and unified approach.

37. It is important to expand the definition of Internet fragmentation to encompass not only the technical level of the Internet, but also the content and transaction level, which is focused on the substantial exchange of information, including the content, data and transactions taking place within the network. That broader perspective helps to provide a more comprehensive understanding of the various dimensions of Internet fragmentation.

38. Cooperation and collaboration are essential to achieving an unfragmented Internet. The Tunis Agenda for the Information Society, which was adopted in 2005 at the World Summit on the Information Society, includes an emphasis on the importance of maintaining a single, open and global Internet, effectively calling for efforts to avoid the fragmentation of the Internet. In order to cater to the diverse requirements of stakeholders, with the goal of advancing digital cooperation, key actions associated with the report of the Secretary-General on the road map for digital cooperation, have been suggested, including the creation of a more effective architecture for digital cooperation. Deliberations are ongoing about the various possible models for that architecture proposed by the High-level Panel on Digital Cooperation.19

A. Core principles

39. Stakeholders should adhere to the following principles:

(a) It is important to promote a secure, stable and interconnected Internet that upholds the values of open societies and safeguards fundamental human rights and freedoms;

(b) Concerted efforts must be made to bridge the digital divide through affordable, safe and reliable Internet using adequate and up-to-date infrastructure to ensure connectivity for all;

(c) Sufficiently training African stakeholders in a manner that enables decisions to be implemented on the continent, through capacity-building and access to technical work that can spark further innovation, and ensures equitable empowerment;

(d) Realistic, executable and enabling regulation, relevant to the African context and the African agenda, should be developed;

(e) Involvement of multiple stakeholders can be encouraged by demonstrating the value of such involvement and by requiring States to adopt that approach;

(f) Regional and global cooperation, including the use of more platforms, helps to improve engagement at the continental level and results in a united voice globally;

(g) Interoperability with existing Internet standards should be ensured when contributing to existing standards and developing new standards, either through evolution or revolution.

19 For more information on digital cooperation, see www.un.org/en/content/digital-cooperation-roadmap/ and the report of the Secretary-General on the road map for digital cooperation: implementation of the recommendations for the High-level Panel on Digital Cooperation (A/74/821).

B. Recommendations

40. Stakeholders should make commitments or take action in the following ways:

(h) Stakeholders – especially policymakers at all governance levels and those from regional blocs and international organizations, such as the United Nations – must ensure and safeguard the interoperability of the global Internet;

(i) National Governments and policymakers must understand the entirety of the Internet environment, which can be achieved through national, regional and global Internet governance forums;

(j) To avoid the risk of Internet fragmentation, the achievement of the shared goal of a truly global and open Internet is vital and aligns with the eight key actions associated with the report of the Secretary-General on the road map for digital cooperation;

(k) Managers of universal access obligation funds should consider capacity-building when budgeting, to ensure that education and skills are harnessed broadly among rural and remote communities;

(l) Threats to the neutrality of the Internet and Internet shutdowns in certain areas of Africa must be prevented, given that marginalization eventually leads to Internet fragmentation. Organizations such as ECA have an important role to play in spearheading that work on the continent.

41. At the technical level, stakeholders should:

(a) Respect existing protocols and processes while ensuring greater African representation in the development of technical standards;

(b) Strengthen African technical organizations, such as the African Network Information Centre;

(c) Address other forms of fragmentation that affect the technical level;

(d) Ensure the effective communication, in a manner that is easily understandable and accessible to other stakeholders, of findings and developments concerning the management and coordination of various aspects of the Internet.

42. At the governance level, stakeholders should:

(a) Promote the harmonization of rules and regulations at the regional and continental levels;

(b) Enhance African participation and understanding of Internet governance processes, ensuring that African needs are effectively represented;

(c) Strengthen African governance organizations, such as African secretariats and national and regional initiatives of the Internet Governance Forum;

(d) Recognize the impact of external forces, such as affordability, local content, digital literacy and walled gardens;

(e) Address regulations that may inadvertently lead to fragmentation, such as limitations on service provision by big technology companies to communities, censorship and Internet shutdowns;

(f) Emphasize multi-stakeholder involvement in all relevant processes;

(g) Develop appropriate guidelines and policies to manage emerging issues proactively;

(h) Ensure that governance models are inclusive and diverse, and meaningfully engage stakeholders in that process;

(i) Establish trust frameworks for Internet governance at various levels of Internet management;

(j) Develop shared norms and normative frameworks that foster trust among stakeholders, and promote the advancement of an open, free and secure Internet.

43. The recommendations are intended to mitigate the risk of Internet fragmentation and promote a more inclusive, open and globally connected Internet environment. Placing users and human rights at the forefront of the discussion necessitates adopting a broader perspective, going beyond the effectiveness of technical infrastructure in connecting devices and ensuring consistent functionality.

VIII. Digital capacity-building

44. The development of digital skills and education in Africa faces several pressing challenges and gaps. Addressing the challenges and implementing potential solutions are vital for fostering a digitally empowered population and workforce, and promoting inclusive digital development. The overall digital divide among urban and rural areas and socioeconomic groups – which affects low-income communities and marginalized groups, including women and girls – creates a complex set of problems when tackling issues of access, digital skills and education.

45. Additionally, traditional education systems often do not adequately address the evolving demands of the digital age, leading to a gap between education and industry requirements. Addressing digital capacity-building across all sectors is, therefore, a priority for Africa.

A. Core principles

46. Stakeholders should adhere to the following principles:

(a) It is critical to address the digital divide, ensuring access for all and recognizing that one size does not fit all, and that digital initiatives must be tailored to specific contexts;

(b) The lack of digital and literacy skills, especially among educators, is a critical problem to address, and therefore advocacy is needed for digital skills education to start in primary schools, acknowledging the diverse needs of marginalized communities, women and girls;

(c) Technology-enabled curricula and training programmes involving the active participation of the learner are essential;

(d) Recognition should be given to the challenges associated with partnership approaches and the need for sector-specific engagements, emphasizing the importance of financing that is aligned with sector needs and the benefits of strategic, context-specific partnerships and the harmonization of policies;

(e) Coordinated efforts to bridge the digital divide across the continent should be advocated, the sharing of open resources and lessons learned should be encouraged, and the importance of regulatory recognition for digital education and certification should be discussed;

(f) Innovation hubs and policies that support innovation and capacity-building should be promoted, ensuring skills are responsive to economic demands and

fostering industry partnerships. The need for digital infrastructure, including Internet connectivity in schools, should be highlighted, and private sector involvement and engagement should be encouraged, potentially through incentives;

(g) African barriers – such as insufficient digital infrastructure, energy problems, limited access and resource availability – should be identified. The leveraging of existing strategies – such as the Pan African Initiative for Digital Transformation of TVET20 and Skills Development Systems in Africa of the United Nations Educational, Scientific and Cultural Organization – should be discussed;

(h) The importance of understanding and leveraging technology for ease of life and progress, and encouraging the development of indigenous systems, should be acknowledged.

B. Recommendations

47. African Governments and all key stakeholders should aim to ensure that everyone has affordable and meaningful connectivity, and strengthen digital capacity-building by providing support for financing, key infrastructure development, technology transfer and training of personnel, to ensure that Africa has the resources needed to participate in the digital economy. It is essential to foster public-private partnerships, in which stakeholders work together to develop and implement digital capacity-building initiatives that are tailored to local needs and priorities, and build resilience to shocks and crises. Inclusivity and accessibility must be promoted in the exploration of viable strategies to bridge the digital divide on the continent.

48. Stakeholders should make commitments or take action in the following ways:

(a) Establish a coordinated, multi-stakeholder framework – including development partners, African Governments, the private sector and civil society organizations – to align efforts and achieve synergies, and conduct a regional comprehensive review of capacity-building policies, strategies and frameworks for digital skills, taking into consideration the African context and digital environment;

(b) Identify and build institutional capacity to ensure a holistic and coordinated approach across policies, programmes, education levels, industry sectors, languages and geographies. Current skills and capacity gaps should be mapped to monitor, plan and anticipate future needs to ensure that the supply of and demand for skills are matched. That exercise can help with the design or alignment of curricula and capacity-building programmes for the development of digital skills, addressing early-stage education, technical and vocational education and training, skills development systems, the formal education system and the day-to-day use of digital skills. A measurement framework for digital skills should be developed and fiscal incentives for education solutions should be offered;

20 Technical and vocational education and training.

(c) Resources should be mobilized and allocated to implement policies recommended to develop training and capacity-building programmes for digital skills, ensuring equality of access and using specific measures to close the digital divide associated with gender, geographical location, socioeconomic status or disability;

(d) Centres of excellence or digital innovation hubs should be established to promote digital entrepreneurship and increase the participation of academia and the research and development sector;

(e) An online knowledge-sharing platform should be developed to foster regional collaboration, improve the availability of resources, share best practices and provide lessons.

IX. Public goods and digital commons

49. After several decades of private interests dominating the evolving forms of data governance, the role of public regulation of digital public goods – such as the Internet, data, cybersecurity, spectrum and spectrum platforms – has emerged as a priority. The current challenges to ensuring the provision of global digital public goods lie in the increasing complexity and adaptiveness of the global communications system and the changing ways in which global governance responds to that system. An approach to global governance that is based on digital public goods is necessary for those goods to serve the common interest at the national level.

50. Although the term "public good" is commonly used interchangeably with "public interest" or to mean something that is good for the public, in economic terms, public goods – such as air, forests, water and defence – are distinguished from private goods by the rationale for their regulation. A public good is inherently non-rivalrous in consumption – it can be used infinitely without any impact on the ability of another person to use it. Private goods are excludable, but public goods are naturally non-excludable, meaning that there are no natural barriers to their use. Free-to-air public broadcasting is often cited as an example of a public good: the use of free-to-air radio or television by one person does not detract from its use by another person, assuming there is no interference with the signal or congestion. It is also non-excludable given that, unlike for encrypted subscription services, no one can be prevented from using a free-to-air service.

51. Public goods are typically expected to be funded by a general contribution. The challenges of mobilizing public resources to provide public goods, however, have begun to focus attention on the provision of public goods through some form of exclusion, thereby allowing the market to play a much greater role in their delivery. Such an approach effectively renders most public goods impure, given that they are made excludable – often through regulation or for the purposes of commercialization, monetization and profit – at the expense of public service obligations or access. Although debates over public and private provision have been polarized, in practice, State and non-State stakeholders regulate the capacity of one another to provide, access and distribute public goods, often in ways that compromise the idea of public goods. Democratic regulation can, however, uphold public interest by excluding some stakeholders

or practices that serve only private interests and, conversely, can promote some stakeholders and practices that align with the societal value of having inclusive public goods. The importance of that form of public interest regulation, which recognizes that public goods should be universally accessible, is at the heart of the creation of commons, digital public infrastructure, data lakes and open data systems.

A. Core principles

52. Stakeholders should adhere to the following principles:

(a) Global digital products and services are common goods that must be made available to all;

(b) Understanding the Internet, data, cybersecurity and spectrum as a global public good depends on Africa and other regions acquiring the relevant national and global governance capacity;

(c) Over the past three decades, operationalizing access to public goods has entailed private delivery, which still requires public regulation, including at the global level, of governance;

(d) Existing policy divides in the regulation of emerging technologies among the global South and the global North should be addressed;

(e) Representatives of African economies should participate more in global governance negotiations and processes, including concerning the ability to access the legitimate taxation of revenues of global platforms that do not have physical presence in their jurisdictions.

B. Recommendations

53. Stakeholders should make commitments or take action in the following ways:

(a) Establish more effective and shared measures, such as better global resource mobilization through digital taxes or other solidarity mechanisms, to ensure the universal and meaningful availability of digital public goods;

(b) Use public interest policy and regulation to ensure equitable access to public infrastructure, even if the infrastructure is provided privately, so that otherwise common infrastructure does not serve only a small or elite segment of the population. The commercial valuation of resources necessary to deliver public goods, such as digital and data infrastructure, should be balanced with a demand-side approach to enable the creation of commons, allowing those who are unable to afford commercial services to access spectrum through unlicensed spectrum or data through data lakes or alternative forms of data stewardship.

X. Conclusion

54. The consultation on the African contribution to the global digital compact has highlighted key areas of focus to foster a more equitable and inclusive digital development on the continent. Various stakeholders have identified critical challenges and potential solutions in such areas as infrastructure development and access; digital public infrastructure; the prospects of emerging technology and its regulation; digital trust, data protection and human rights; tackling the risk of Internet fragmentation; digital capacity-building; and public goods and digital commons.

55. Africa faces the tasks of expanding and strengthening its digital infrastructure, bridging the digital divide and skills gap, and fostering an environment that is conducive to digital innovation and growth. The importance of digital inclusion – with a particular emphasis on gender equality, the need to avoid Internet fragmentation and the importance of harnessing emerging technologies through appropriate regulation – has been underscored.

56. Collaboration with the international community, including the United Nations system and global corporations, has emerged as a crucial element in addressing those challenges. By partnering with African stakeholders, the international community can support the continent in various ways, including through financial investment, knowledge transfer, capacity-building, mentorship and public-private partnerships.

57. It is essential to prioritize equity, accessibility, empowerment, education, capacity-building, collaboration and partnerships throughout the journey towards digital inclusion and gender equality in Africa. By embracing those concepts and working collectively, African stakeholders and their partners can build a more inclusive, resilient and prosperous digital future for Africa, where every individual, community and country can harness the transformative power of digital technology for sustainable development and mutual prosperity.

Annex

Participants in the Africa Regional Review Meeting on Africa's Contributions Towards the Global Digital Compact, held on 4 and 5 July in Cape Town, South Africa

Name	Country	Title or organization
Blaise Fundji Azitemina	Democratic Republic of the Congo	Adviser to the Minister's Office, Ministry of Posts, Telecommunications and New Information and Communications Technology
Ferdinand Manirakiza	Burundi	Permanent Secretary, Ministry of Communication, Information and Communications Technology and Media
Mourad Melliti	Tunisia	General Telecommunication Engineer, Ministry of Communication Technologies
Francois Joseph Nnemete Beyeme	Cameroon	Director of Telecommunications Regulation, Ministry of Posts and Telecommunications
Mino Harivelo Ramaroson	Madagascar	Adviser to the Minister, Ministry of Development and Digital Transformation
Attoumani Mohamed Karim	Comoros	Telecommunications Engineer, Ministry of Posts, Telecommunications and the Digital Economy
Njalakangwa Phumaphi	Botswana	Deputy Manager, e-services, Ministry of Communications, Knowledge and Technology
Aissata Chanoussi Moustapha	Niger	Information Systems Security Director, National Agency for the Information Society
Siaka Kangoute	Côte d'Ivoire	Director Coordinator of Priority Projects, Ministry of Communication and Digital Economy
Fode Youla	Guinea	Telecommunications Adviser, Ministry of Posts and Telecommunications
Emmanuel Mikiela	Gabon	Digital Economy Administrative and Logistics Manager
Annie Mwelwa Munsaka	Zambia	Ministry of Technology and Science
Fanta Sombie	Burkina Faso	Technical Advisor, Ministry of Digital Transition, Posts and Electronic Communications
Johanna Nalimanguluke Nashipili	Namibia	Chief Development Planner, Directorate of Information and Communications Technology Development Division, Information Technology Infrastructure Development, Ministry of Information and Communication
Amine Adoum Bakhit	Chad	Technical Adviser, Ministry of Telecommunications and Digital Economy
Eric Armel Ndoumba	Congo	Telecommunications Adviser to the Minister
Mawaki Chango	Togo	ECA consultant, DigiLexis Consulting

Name	Country	Title or organization
Massani Koroney	Niger	Member of Parliament
Amadou Bah	Gambia	President, Gambia Cybersecurity Alliance
Thomas Senaji	Kenya	ECA consultant
Yai Jorjoh Ndure Tambedou	Gambia	Chief Executive Officer, Insist Global and UNESCO consultant on technical and vocational education and training
Mani Abdou	Niger	Member of Parliament and President of the Economic Community of West African States parliamentary forum on the harmonization of laws for the development of information and communications technology in West Africa
Aicha Jeridi Chebbi	Tunisia	Internet governance and digital policy expert
Barnabas Charakupa	Zimbabwe	Ministry of Information and Communications Technology and Postal Service
Massamba Badiane	Senegal	Head of the Office of Security and Digital Trust, Ministry of Telecommunications
Chamsoudini Mzaouiyani	Comoros	General Director, National Agency for Digital Development
Violet Nyambura	Kenya	ECA consultant on electronic civil registration and vital statistics
Neema Kichiki Lugangira	United Republic of Tanzania	Member of Parliament and President of the African Parliamentary Network on Internet Governance
Muriuki Mureithi	Kenya	Chief Executive Officer, Summit Strategies
Gebreala Abraham Gebri	Ethiopia	Policy adviser for the Ethiopian national identity programme
Emmanuel Ofori	Ghana	Head of Policy, Planning, Budgeting, Monitoring and Evaluation, Ministry of Communications and Digitalization
Viguier Carmen Nguembi	Congo	Legal Adviser to the Minister
Sisay Fekadu Wolde	Ethiopia	Network and development and operations engineer, Ethiopian national identity programme
Rosalio Sandra Kaluwa	Malawi	Chief Information and Communications Technology Officer
Godffrey Maina Mwangi	Kenya	Member of Parliament
Sorene Assefa	South Africa	ECA consultant and cybersecurity expert
Zanyiwe Asare	South Africa	Internet Governance Forum Steering Committee, Africa Youth Internet Governance Forum Secretariat
Linda Anyango Bonyo	Kenya	ECA digital centre consultant
Nolwando Maoto	South Africa	Chief Data and Analytics Officer, Rand Merchant Bank

Name	Country	Title or organization
Lerato Seema	South Africa	Executive Manager, Regulation and Compliance, .za Domain Name Authority
Tsholofelo Mokone	South Africa	Coordinator, Internet Governance, .za Domain Name Authority
Molehe Wesi	South Africa	Chief Executive Officer, .za Domain Name Authority
Tony Parry	South Africa	Chief Executive Officer, Institute of Information Technology Professionals South Africa
Palesa Legoze	South Africa	Chairperson, .za Domain Name Authority
Raesibe Josephine Phihlela	South Africa	Resident Coordinator's Office
Sinovuyo Ndadlana	South Africa	United Nations Development Programme
Fayaz King	United States of America	Office of the Secretary-General's Envoy on Technology
Alison Gilward	South Africa	Executive Director, Research Information and Communications Technology Africa
Mike Silber	South Africa	Group Chief Regulatory Officer, Liquid Telecom
Palesa Natasha Mothapo	South Africa	University of Stellenbosch
Godfrey Kyama	South Africa	ECA consultant
Zara Schroeder	South Africa	Research Information and Communications Technology Africa
Mike Mojapelo	South Africa	Executive, Broadband Infraco
Jim Paterson	South Africa	Director, Multilateral Affairs, Department of Communications
Alfred Mmoto	South Africa	Department of Communications and Digital Technologies
Trevor Rammithwa	South Africa	National Electronic Media Institute of South Africa
Nokwanda Madondo	South Africa	Post Bank
Buntu Manitshana	South Africa	State Information Technology Agency
P Sitmole	South Africa	Association of Comms and Technology
Ayodele Odusola	South Africa	United Nations Development Programme South Africa