



General Assembly

Distr.: General
23 December 2022

Original: English

Human Rights Council

Fifty-second session

27 February–31 March 2023

Agenda item 3

Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

International financial obligations, digital systems and human rights

Report of the Independent Expert on the effects of foreign debt and other related international financial obligations of States on the full enjoyment of all human rights, particularly economic, social and cultural rights, Attiya Waris

Summary

In the present report, the Independent Expert on the effects of foreign debt and other related international financial obligations of States on the full enjoyment of all human rights, particularly economic, social and cultural rights, focuses on the implications of the digital economy on the enjoyment of human rights. Technological innovations in the economic sphere have the potential to impact people's daily lives in both positive and negative ways. In order to fully reap the benefits of this technological progress while minimizing the potential for harm, the development and deployment of new technologies forming a part of the digital economy must be rooted in human rights.

In her report, the Independent Expert reflects on issues such as the lack of transparency of cross-border financial transactions, the difficulty of prosecuting cases involving illicit financial flows in the digital world and taxing digital platforms or companies, as well as the lack of access to technological resources in developing countries and increasing socioeconomic inequalities. The report also focuses on new digital lending practices, digital financial services, cryptocurrencies, blockchains, non-fungible tokens and encryption systems, among others.

To address these challenges, the Independent Expert calls for the application of the rights and principles related to privacy, access to information, participation, accountability, transparency and fiscal legitimacy, as well as for international cooperation and assistance, to the development and deployment of digital technologies in the economy.



I. Introduction

1. Individuals, institutions and States have a diverse and varied experience of digital systems. In some scenarios, almost all the activities related to the different facets of an individual's life involve an element of digital technology. The use, speed, manner of operation, capacity and pace of operation and growth of digital technologies affects every single person, entity and State across the world. The continuing evolution of this technology has resulted in a context where tax, trade and financial laws, regulations, guidelines and norms are unable to keep pace.

2. The fast-growing digital economy has implications for human rights, the economy and the international financial architecture and how it is regulated in the context of prevailing and deepening multidimensional inequalities. Digital systems, including digital tax systems, rely heavily on processing personal data for the digital economy.¹ Protection laws on data must be formulated in line with the right to privacy of individuals. Presently, States are grappling with whether to consider data protection as entitled to separate regulation or whether to assign the role to existing financial regulators.² In this report the Independent Expert explores the key areas of financial transactions – their creation, movement, storage, use review and analysis – and how approaches to these transactions should apply a human rights lens.

3. It is estimated that the digital economy is worth \$11.5 trillion globally. It is equivalent to 15.5 per cent of global gross domestic product and it has grown two-and-a-half-times faster than the global gross domestic product over the past 15 years, almost doubling in size since 2000.³ In 2020, globally, 62 per cent of men were using the Internet, compared with only 57 per cent of women.⁴ The share of Internet users in urban areas is twice as high as in rural areas, and 71 per cent of the world's younger population aged 15–24 is using the Internet, compared with 57 per cent of all other age groups. Even though new technologies are spreading rapidly around the world, an estimated 37 per cent of the population – or 2.9 billion people – have still never used the Internet.⁵

4. In the context of foreign debt, illicit financial flows and international financial obligations and their impact on human rights, there are a host of specific dimensions and concerns related to the digital economy. Concerning the magnitude of money flows, with digital advances remittances (which are one of the largest and most stable sources of foreign exchange, especially in developing countries) have been a growing source of revenue in many countries around the world, through regulated and unregulated methods of digitally connected transfers.⁶ Mobile money providers through their everyday transactions are leveraging the system, as are all others operating within economies engaging in cross-border transactions.⁷ In a digital world, the issue of remittances, when linked and pooled together with other issues in development finance – such as lack of access to sufficient condition-free, debt-free liquidity, chronic under provision of official development assistance and volatile private capital flows – contributes towards financial systems with information flows that can be either supportive of or undermine the realization of human rights.⁸

5. The use of data and its analysis through artificial intelligence in the digital economy is transforming business models, facilitating new and targeted products and services.⁹ The State-business nexus has increasingly come to the attention of various stakeholder groups, raising concerns of a lack of human rights protection when States have outsourced to, or

¹ Deloitte Malta, “What Is Digital Economy?”, 2022.

² Submission from Afronomicslaw, p. 5. Submissions from States and other stakeholders in response to the call for input by the Independent Expert are available from <https://www.ohchr.org/en/calls-for-input/2022/international-financial-obligations-digital-systems-and-human-rights>.

³ See https://www.huawei.com/minisite/gci/en/digital-spillover/files/gci_digital_spillover.pdf.

⁴ See World Bank, “Digital Development: Overview”, 6 October 2022.

⁵ Ibid.

⁶ See [A/HRC/49/47](#).

⁷ Ibid.

⁸ Ibid.

⁹ See Deloitte Malta, “What Is Digital Economy?”.

contracted technology companies for, public services. For example, for the delivery of social services, public authorities are reportedly increasingly relying on technological systems developed by private actors.¹⁰ Furthermore, the Special Rapporteur on extreme poverty and human rights identified the dangerous implications of the lack of regulation of big tech firms from a human right perspective. They have increasingly taken up a leading role in designing, constructing and operating parts of the public and welfare services delivered to the vulnerable and marginalized.¹¹ Even as States engage with the same digital systems to deliver public services and disseminate information to the vulnerable, State processes at lower tiers of governance, in particular, are unable to keep up with these rapid developments.¹² There are examples of system errors and failures in digitized eligibility assessment and in payment and disbursement of social benefits, which has resulted in difficulties in accessing and enjoying the right to social security.¹³

6. In developing more robust, fiscally legitimate systems, greater transparency is a commonly agreed public good. Yet, too often, public access to public finance contracts is limited and bilateral agreements remain inaccessible. Unequal access to information and general opacity is a particularly difficult problem when digital systems are used, especially since data is held either in private institutions based in high-income countries or by high-income countries themselves.

7. Three elements of fiscal legitimacy – responsibility, transparency and accountability – will be the focus of the investigation of the Independent Expert into the limits on financial information that countries and the public are able to access in order to generate revenue that can promote the realization of human rights.¹⁴ Lack of access to data remains an impediment to the monitoring and control of these financial information transfers. Control of these transfers would result in two financially related achievements in all countries: (a) curbing illicit financial flows, which will promote the progressive realization of human rights; and (b) improving the State’s ability to regulate and collect tax revenue. Thus, the State will be in a position to better finance its activities, including those related to human rights, resulting in their progressive realization, and also to improve its understanding of relevant challenges, opportunities and risks.¹⁵ However, this should take place in an ecosystem that is fiscally legitimate and allows for stakeholders to access information.

8. The Independent Expert, through consultations and multi-stakeholder engagement, has set out potential areas and actors States could engage with and regulate in order to improve protections and advance the human rights of their populations.¹⁶ The report by the Independent Expert will focus on the need for cross-border cooperation on the use of digital technologies in matters of finance and the impacts on the realization of human rights, including the maximum available resources needed to realize economic, social and cultural rights.¹⁷

II. Digital systems in the context of human rights

9. The role of data flows in facilitating trade is undeniable, especially in facilitating global trade in goods and services. Consequently, the impact of the growing importance of data flows has led countries to adopt national data policies. This role is likely to increase with

¹⁰ A/HRC/50/56, para. 26.

¹¹ See A/74/493, para. 72.

¹² In South Africa, for example, the South African Security Agency has distributed social grants through a private company (Cash Paymaster Services), which registered beneficiaries by collecting their biometric information (fingerprints and, originally, voice recordings). The beneficiaries were issued MasterCard debit cards with biometric functionality and a linked bank account. See Ray Mahlaka, “Post Office Set to Take Over Cash Payments from CPS”, Moneyweb, 4 June 2018.

¹³ A/74/493, para. 23.

¹⁴ A/HRC/49/47, paras. 26 and 38–42.

¹⁵ Ibid., para. 62.

¹⁶ Ibid., paras. 30 and 36–37.

¹⁷ Ibid., para. 60.

the expansion of data-intensive technologies such as autonomous driving, machine learning, artificial intelligence and the Internet of things.¹⁸

10. In a recent report by the United Nations Conference on Trade and Development (UNCTAD) the crucial role data and cross-border data flows play in economic and social development is emphasized. It is also pointed out, with regard to the central issue of cross-border data flows, that data are both economic and non-economic in nature, with implications for privacy, human rights and security.¹⁹

11. Similarly, data policies adopted by countries have important implications for trade. Data localization and data sovereignty, for example, have an impact on trade flows in goods and services. On certain websites and for certain web applications, it is a prerequisite to provide user information in order to purchase the goods and services being offered on these platforms. Regulations around privacy and personal data protection therefore have an important connection to trade. However, while cross-border data flows are strongly linked to trade, the rationale for regulating cross-border data flows primarily in trade agreements remains weak at best.²⁰

12. While much global data in commercial transactions is being produced, stored and exchanged, a huge share of these data is not directly related to the transactions themselves, but to other aspects of human life, and there are challenges facing the distinction between different types of transactions. As such data are produced, collected, stored and transferred, these processes impact issues related to privacy, personal data, social relations and security, among others, and treating these issues exclusively through a trade lens is too narrow an approach. Moreover, this also applies to data products, which can be regulated through the services trade regime, implying that trade regulations in relation to data may need to take place in a broader context.²¹

III. Digital systems and international financial obligations

A. Illicit financial flows

13. Participation, accountability and transparency are critical to enhance the effective use of information and public resources for investment in human rights. Greater transparency is a commonly agreed public good for guiding financial policymaking. Yet, too often, public access to public finance contracts is minimal and bilateral agreements remain inaccessible.²² Transparency around debt swaps, service obligations and restructuring, especially with private creditors and bondholders, is not always available. Technical mechanisms on digital financial technologies need administrative, legal and regulatory frameworks so that countries can benefit from different sources of finance. Mechanisms providing access to timely information on financial matters allow decision-makers to be held to account.²³

14. In an earlier report, the Independent Expert highlights the implications of tax-related illicit financial flows on human rights.²⁴ The report also discusses the role that secrecy jurisdictions have in perpetuating the erosion of resources from countries, in particular developing countries, to jurisdictions which offer low or no taxes and provide sophisticated financial structures to facilitate tax abuse. The report states that banks and other financial service providers offering these services have been used by the very wealthy to transfer resources from countries where income is generated to no or low-tax jurisdictions. The

¹⁸ United Nations Conference on Trade and Development, *Digital Economy Report 2021 – Cross-Border Data Flows and Development: For Whom the Data Flow* (New York, 2021), p. 143.

¹⁹ *2022 eCommerce Week Outcome Report: Data and Digitalization for Development*, p. 4.

²⁰ UNCTAD, *Digital Economy Report 2021*, p. 144.

²¹ *Ibid.*

²² [A/HRC/49/47](#), paras. 57–58.

²³ *Ibid.*

²⁴ See [A/HRC/31/61](#).

question that arises from the discussion in the report is thus, what is the effect of such illicit financial flows on human rights?²⁵

15. The answer to the above question is twofold. First, such practices have exacerbated inequality by widening the income and wealth gap, thus hindering the ability of the State to fulfil not only its minimum core obligations but also the progressive realization of human rights. Second, these illicit flows directly and indirectly facilitate a cyclical dependence on borrowing.²⁶ The opaqueness of cross-border financial transactions that facilitate the erosion of resources is a major reason for the increasing wealth gap. In her report, the Independent Expert suggests that secrecy jurisdictions provide a habitat for these transactions and, in that sense, the wealthy who can afford such services get wealthier while the disadvantaged populations remain at the periphery.

16. Among the challenges developing countries face in tracing the amount of resources eroded through the schemes identified above are technological hindrances owing to digitalization. The lack of technological resources in low- and middle-income countries make it challenging to trace offshore and dubious transactions. Technological systems are being used in diverse ways to obfuscate the transparency of financial transactions, enabling illicit financial flows out of developing countries, which has a negative influence on debt sustainability in these countries.²⁷

17. The fast-growing role of information and communication technologies also requires close attention in the context of illicit financial flows.²⁸ Criminals – including transnational organized crime groups – increasingly use digital avenues to facilitate illicit cross-border trade and associated financial flows. At the same time, big data analytics, machine learning and neural network programming could potentially provide an array of tools and methods to better predict illicit behaviour and measure illicit financial flows more accurately.²⁹ Those abusing the processes are beneficiaries of technological advancement and these activities not only hinder development at the State level, but also have negative repercussions on individuals, who are plunged deeper into poverty.

18. Financial transparency is not a single-country endeavour. Several African countries, like Algeria, Ghana, Uganda and Zimbabwe, are not members of the Inclusive Framework on Base Erosion and Profit Shifting of the Organization for Economic Cooperation and Development (OECD) and the Group of 20 and are thus systematically underrepresented in global decision-making spaces on digital tax issues.

B. Digital systems and the lending industry

19. Big data is one of the frontiers for the linkage between tax, data and technology. Illicit financial flows thrive on technological advancements in secrecy jurisdictions. Compared with the private sector, the lesser uptake of digital tools in fighting illicit financial outflows from developing countries increases the income and wealth gaps.

20. As identified in the report on private debt and human rights, new digital lending practices via mobile applications is an important contributory factor in the overall rise of private debt and overindebtedness among households.³⁰ The fast-evolving digital lending industry increasingly (and aggressively) facilitates credit through digital means, including

²⁵ Ibid, paras. 21–36.

²⁶ Ibid, para. 35.

²⁷ Peter Chowla and Tatiana Falcao, “Illicit Financial Flows: Concepts and Scope” draft Financing for Development Working Paper, Inter-Agency Task Force on Financing for Development, 5 December 2016.

²⁸ United Nations, General Assembly, “International Cooperation to Combat Illicit Financial Flows and Strengthen Good Practices on Assets Returns”, 16 May 2019, available from <https://www.un.org/pga/73/event/international-cooperation-to-combat-illicit-financial-flows-and-strengthen-good-practices-on-asset-returns/>.

²⁹ Ibid.

³⁰ [A/HRC/43/45](#), para. 69; and [A/74/493](#), para. 25.

mobile applications, leading to overborrowing.³¹ At the same time, the digital lending practices are highly unregulated in comparison with the more traditional forms of credit.³² It is observed in the report that often mobile lenders leverage the data received from users of their services to update their systems and come up with more products targeting borrowers.³³

21. The digital lending industry also capitalizes on the digital infrastructure provided to States to distribute welfare benefits and social grants (e.g., in the form of electronic payment cards or debit cards). This is then used to influence the recipients to purchase commercial financial products or to impose user fees for late payments, which may contribute to growing private debt among low-income groups, leading to overindebtedness.³⁴ This includes not only analysing data that is directly related to the purpose of granting credit. Complex algorithm-based applications evaluate the social media activities of millions of people to assess their behaviour and preferences with a view to inferring their creditworthiness. The use of such practices can affect individuals beyond economic considerations and privacy.³⁵

22. The private information of borrowers in the lenders' possession is not available to regulators. Thus, regulating the amounts of profit that these lenders make against the repayment rates paid by the borrower may be challenging in some instances and does not stop lenders from selling their customers' data. Inadequate regulation of financial practices of private lenders and banks and abuse of digitally stored information results in higher levels of private debt among low-income groups. This facilitates inequality, and might potentially breach the right to privacy. Furthermore, low-income and socially marginalized groups are likely to depend on informal sources of borrowing that are not subject to compliance codes and regulations.³⁶ While one of the impacts of illicit financial flows is lesser public investment in public goods and services, like health and education, it also means that more individuals and households rely on commercial borrowing to pay for necessities that are not financed by the State.

23. Digital systems have implications for the enjoyment of human rights, as indicated above. New innovations have the potential to exacerbate or alleviate the net effects of digitalization on developing economies. To fully reap the benefits of the technological progress under way while minimizing the potential for harm, the development and deployment of new technologies need to be rooted in human rights

IV. Global financial architecture on digital systems

A. Remittances

24. Blockchain and other distributed ledger technologies now play an important role in the world of archives and document management, due to their ability to guarantee the authenticity, reliability, traceability and use of electronic documents. Although envisaged, these technologies should not, however, lead to the creation of a monumental archival resource, and be excessive or disproportionate, without any natural or legal person having a specific responsibility for its creation and maintenance. This is the case of the blockchain "accounting book" produced by the use of some cryptocurrencies. This decentralized archive, with no regulators, offers unquestionable guarantees of immediacy and anonymity in transactions and is a very attractive channel for sending remittances from immigrants to their countries of origin. States must keep records of electronic commerce companies and have a

³¹ [A/HRC/43/45](#), paras. 68–69. See also Milford Bateman, Maren Duvendack and Nicholas Loubere, "Is Fin-Tech the New Panacea for Poverty Alleviation and Local Development? Contesting Suri and Jack's M-Pesa Findings Published in *Science*", *Review of African Political Economy*, vol. 46, No. 161 (2019).

³² [A/HRC/43/45](#), paras. 68–69.

³³ [A/HRC/43/45](#), para. 63.

³⁴ [A/74/493](#), para. 25.

³⁵ [A/HRC/43/45](#), para. 68.

³⁶ [A/HRC/43/45](#), para. 16.

digital file that makes it possible to establish the volume and the number of operations in the field of digital economy.³⁷

B. Digital goods and services

1. Digital payment systems and financial inclusion

25. Digital banks are expected to further advance financial inclusion. By adopting digital technology more widely for everyday transactions – which makes it possible to overcome geographic barriers, reduce transaction costs and promote better financial management by providing access to more personalized solutions backed by data analytics – opportunities for society to participate in the economy can be significantly increased. As businesses continue to move online, digital banking also provides a safer and convenient way to help people and businesses grow their wealth, engage in trade and commerce, and build resilience.³⁸

26. Central banks, for instance, have issued digital currencies in response to the growth in technological advancements both in the economy and the monetary system.³⁹ Depending on the specific design of a central bank digital currency, there are trade-offs between benefits in terms of users’ privacy and the integrity of the payment system. Every digitization of payments generates a “data trail” of information on individual transactions, which can be used to determine individuals’ creditworthiness but (when combined with other data sources) which can also provide deep insights into individuals’ behaviour, beliefs and habits.⁴⁰ At the same time, anonymization in digital transactions allows space for illicit transactions and money-laundering.⁴¹

27. The World Bank suggests countries could adopt a handful of key measures to boost financial inclusion through digital financial services, including better articulation of national strategies to increase financial inclusion and digitization of the economy; stronger regulatory capacity to comprehend the evolution of financial services and handle the additional risks brought by innovations and new business models; improvements in basic infrastructure, such as efficient and accessible retail-payment systems and the digitization of large-volume, recurrent payment streams; progress in financial and technological literacy, enhancing trust in digital financial services; and collection and use of reliable data on traditional and emerging financial technologies for policymaking purposes.⁴² However, the proposed measures must be understood in the light of how most migrants, displaced persons and women in low- and middle-income countries are employed in the informal sector. By way of being associated in the informal economy, these individuals depend upon informal networks of payment, borrowing or lending. Additionally, new technologies risk exacerbating gender and other disparities.⁴³ Apart from the gendered digital divide, it is likely that such persons may lack appropriate documents needed for financial inclusion.

28. According to a Global Payments Innovation Jury report of 2022 by the World Bank and the digital commerce company, Interswitch,⁴⁴ the use of mobile phones for financial transactions is eating into card payments. In Kenya, for example, account-to-account (A2A) payments account for 72 per cent of the total financial transactions, with mobile money

³⁷ Submission by Section on Archives and Human Rights, International Council on Archives, p. 5.

³⁸ Nor Shamsiah Mohd Yunus, Governor of Bank Negara Malaysia (Central Bank of Malaysia), “Advancing Digitalisation for Recovery, Sustainability and Inclusion” MyFintech Week 2022, 24 January 2022.

³⁹ Raphael Auer and others, “Central Bank Digital Currencies: Motives, Economic Implications and the Research Frontier”, BIS Working Papers, No. 976 (Bank for International Settlements, 2021), p. 6.

⁴⁰ *Ibid.*, p. 14.

⁴¹ See also Zijian Wang, “Tax Compliance, Payment Choice, and Central Bank Digital Currency”, Social Science Research Network (SSRN), last revised 15 June 2022.

⁴² World Bank Group and Association of Southeast Asian Nations (ASEAN), *Advancing Digital Financial Inclusion in ASEAN: Policy and Regulatory Enablers* (Washington, D.C., World Bank Group, 2019), p. 7.

⁴³ A/HRC/43/29, para. 12.

⁴⁴ *Payment Innovation: Myths and Realities*.

services like M-Pesa leading the way.⁴⁵ Almost half of Africa's gross domestic product is run via mobile phones and this percentage is likely to increase in the coming years. The continent now accounts for 70 per cent of the world's \$1 trillion mobile money value. The value of Africa's mobile money transactions edged up 39 per cent to \$701.4 billion in 2021 from \$495 billion in 2020. In the review period, registered mobile wallets in Africa topped 621 million, a 17 per cent increase from 562 million captured in 2020.⁴⁶

29. Even so, the Global Payments Innovation Jury report of 2022 says that while mobile phones are becoming the preferred form for payments globally, and are gathering momentum in developing markets, there are significant regulatory hurdles to overcome, such as telecommunications (telecoms) companies owning mobile money transfer and lending units, as well as shocks from other business activity.⁴⁷

30. Apart from the challenges faced by countries globally in taxing digital or platform companies with no physical presence, unequal exchange of financial information also hampers the ability of a country to implement a sound digital tax policy. Furthermore, huge disparities in broadband access remain between different groups globally and between low- and middle income countries.⁴⁸

2. Digital services taxes

31. The African Tax Administration Forum identified common digital goods and services, such as digital currencies and financial services, software, apps and advertisements, cloud services, corporate and educational training, communication and social media. Intangible goods and services are regulated through the allocation of taxing rights, which are globally accepted, and the enforcement of taxing rights, which is voluntary for States.⁴⁹ The Digital Service Tax of Kenya is at a rate of 1.5 per cent gross transactional revenue, and it targets both resident and non-resident digital service providers.⁵⁰ In Azerbaijan, the Government is presently implementing projects aimed at a more efficient taxation of the digital economy. For example, a project for the "virtual permanent establishment" of non-resident digital companies envisages the creation of an electronic platform that will allow online registration of these companies for tax purposes.⁵¹

32. To fulfil the 2030 Agenda for Sustainable Development, tax revenues should be used by Governments to finance crucial social, health and educational programmes for all members of their populations. In some countries,⁵² a withholding regime is applied on international business-to-customer supplies of services and intangibles. Costa Rica, for instance, applies such a withholding tax. Instead of the collection by non-resident suppliers, financial institutions, such as banks and payment service providers, are required to withhold 13 per cent of the amounts on consumer payments to non-resident businesses as a substitute for the value added tax (VAT) due.⁵³

33. Being indirect in nature, digital service taxes may cause fiscal distortions. There is a possibility that they may undermine digital and financial inclusion in low-income countries as the tax burden on consumers increases. Digital service taxes not only affect connectivity and affordability (consumption and pricing decisions) but also investment in information

⁴⁵ Harry Padoan, "M-PESA Leads Growth in Real Time A2A Transactions", TelcoTitans, 6 October 2022.

⁴⁶ Seth Onyango, "Africa accounts for 70% of the world's \$1 trillion mobile money market", Quartz, 4 May 2022

⁴⁷ P. 11.

⁴⁸ See submission by Afronomicslaw.

⁴⁹ *Suggested Approach to Drafting Digital Services Tax* (Pretoria, African Tax Administration Forum, 2020).

⁵⁰ The Digital Service Tax was introduced in the Finance Act, 2020. See Kenya Revenue Authority, "Introducing Digital Service Tax", available from <https://kra.go.ke/images/publications/Brochure-Digital-Service-Tax-Website.pdf>.

⁵¹ See submission by Azerbaijan.

⁵² OECD, World Bank Group, Inter-American Center of Tax Administrations and the Inter-American Development Bank, *VAT Digital Toolkit for Latin America and the Caribbean* (Paris, OECD, 2021).

⁵³ See submission by Costa Rica.

technology and the Internet value chain (capital investment decisions).⁵⁴ These decisions might lead to the loss of household and business incomes, with adverse effects on the human rights of low-income groups.

3. Cryptocurrencies

34. Cryptocurrency is a digital currency that uses cryptography to secure transactions. The transactions are usually recorded in a public ledger and stored in digital wallets. The nature of the currency⁵⁵ makes it extremely difficult to counterfeit or double spend. The units of the currency are created in a process known as mining. Cryptocurrency does not rely on banks and is more of a peer-to-peer lending network. Bitcoin is one of the original forms of cryptocurrency; basically, Bitcoin and other cryptocurrencies allow the movement of a unit of measure through a public distributed ledger, known as blockchain, from one person to another without having to use a third party. As the usage of cryptocurrencies rises, so do the associated risks of tax evasion and avoidance, as ownership of these assets is not easy to locate. Moreover, balances held in these accounts are untaxed.⁵⁶

35. In its *Global Financial Stability Report* of 2021,⁵⁷ the International Monetary Fund notes that the market capitalization of crypto assets has grown significantly amid large bouts of price volatility. The market capitalization almost tripled in 2021, to an all-time high of \$2.5 trillion. This was followed by a 40 per cent fall in the same month, as concerns from institutional holders about the environmental impact of crypto assets grew, and global regulatory scrutiny of the crypto ecosystem escalated. Moreover, the market capitalization of stablecoins has quadrupled in 2021 to more than \$120 billion.

36. In February 2022, the Financial Stability Board published an “Assessment of Risks to Financial Stability from Crypto-assets”. The report examines developments and associated vulnerabilities relating to three segments of the crypto-asset markets: unbacked crypto assets (such as bitcoin); stablecoins; and decentralized finance and other platforms on which crypto-assets trade. The Financial Stability Board points out that crypto-asset markets are fast evolving and could reach a point where they represent a threat to global financial stability due to their scale, structural vulnerabilities and increasing interconnectedness with the traditional financial system. It also notes that financial stability risks could escalate rapidly and calls for timely and pre-emptive evaluation of possible policy responses.

37. In June 2022, the European Commission reached a provisional agreement on a proposal for the regulation of crypto-assets markets, which covers issuers of unbacked crypto assets and stablecoins, as well as the trading venues and the wallets where crypto assets are held. With the new rules, crypto asset service providers will have to respect strong requirements to protect consumers’ wallets and will become liable if they lose investors’ crypto assets. The regulation will also cover any type of market abuse related to any type of transaction or service, notably for market manipulation and insider dealing. Actors in the crypto-assets market will be required to declare information on their environmental and climate footprint. The proposed regulation requires that the European Banking Authority be tasked with maintaining a public register of non-compliant crypto-asset service providers.⁵⁸

38. At the onset of the coronavirus disease (COVID-19) pandemic in Nigeria, many persons remained unbanked and those who could access the banks had to travel to urban areas, as most of the rural branches had closed. Aimed at financial inclusion,⁵⁹ the

⁵⁴ See submission by Afronomicslaw.

⁵⁵ Cryptography is enabled by encryption which secures the content of a transaction in such a way that it can only be accessed by the intended recipient. Encryption converts the plain text into the cipher text which cannot be understood until the intended recipient decrypts the message with a decryption key. The randomness of the encryption makes it highly secure and ensures an elevated form of privacy.

⁵⁶ UNCTAD, “The Cost of Doing Too Little Too Late: How Cryptocurrencies Can Undermine Domestic Resource Mobilization in Developing Countries”, Policy Brief No. 102, July 2022.

⁵⁷ *COVID-19, Crypto, and Climate: Navigating Challenging Transitions* (Washington, D.C., 2021).

⁵⁸ Council of the European Union, “Digital Finance: Agreement Reached on European Crypto-Assets Regulation (MiCA)”, press release, 30 June 2022.

⁵⁹ Robert Obioha, “Covid-19, Banks and the New Normal”, Financial Inclusion Nigeria, 2019.

Government launched e-naira, a digital currency. The e-naira⁶⁰ provides both a store of value and a payment system for its users. Some of the advantages cited by the Central Bank of Nigeria include that it provides an opportunity for growth by providing access to capital that can be used to grow businesses. Secondly, it has a form of traceability that ensures a reduction in illegal transactions and cases of fraud. Thirdly, e-naira allows for diaspora remittances, which is especially important in view of the number of Nigerian immigrants living abroad. This currency is well customized to serve the needs of its people. Furthermore, the currency has a strong, unique security structure that ensures it cannot be forged or counterfeited.

39. Private payment systems have a higher likelihood than public payment systems of affecting monetary policy stability in a country, which has implications on human rights. As issuers of the digital currency, Central Banks are responsible for maintaining public trust and accountability. Ensuring price stability, they play a key role in establishing the infrastructure needed to facilitate trade and its oversight.

4. Emerging technologies (metaverse, web 5.0)

40. A non-fungible token is a unit of data that certifies a digital asset as unique. It has to be a one-of-a-kind thing that cannot be traded for a similar thing. The authenticity of the non-fungible token is measured through the blockchain ledger. In the early years, the thinking behind the tokens was similar to the thinking concerning a work of fine art – such as a painting of the Mona Lisa or a unique composition by Mozart. The spotlight has now moved on to digital art.

41. Internet users have been excited by the ownership of an original non-fungible token and they have been sold for millions of dollars. There has been a great surge in artists using non-fungible tokens, which generate royalties each time they are sold. However, there is also the risk of the non-fungible token being used for illicit financial flows and therefore to promote money-laundering and tax evasion due to the global interest in non-fungible tokens.

42. In addition, the metaverse, like any other electronic environment, has the particularity that any person with access to the network can use it. This poses a challenge, given that the growth and development of ecosystems such as the metaverse are thanks to, among others, the fact that they are not limited by regulation. However, States must guarantee the rights of people, and they have the capacity to sanction people who carry out illegal actions, whether in the metaverse or in any other environment. Transactions should be treated as services provided in the physical world (between individuals or legal entities).

43. It is important to highlight that cryptocurrencies are the main means of payment in economic transactions on metaverse platforms. The expansion of these digital universes brought with it non-fungible tokens: unique cryptographic tokens recorded in a blockchain that can be used to establish the provenance and ownership of a given digital asset. These digital goods offer a greater challenge, in terms of taxation, due to their characteristics, since there is no unit of measurement for these tokens. The possibility of indirect taxes on digital marketplaces as been explored in Brazil.⁶¹ The fact is that, at first, the existing legislation in the most diverse areas of law (including civil, consumer, tax, labour and economic law) must be transferred to tax transactions in the metaverse. The fundamental and guiding principles that guide legal relations will be preserved, but specific rules will need to be created to adapt to the particularities of the metaverse.

44. The definition of the legal nature of the financial assets present in the metaverse will serve to guide the tax collection in these environments.⁶²

⁶⁰ To access the e-naira, a user can sign up by downloading an application and accessing the e-naira features that allow users to send and receive money. Users can also verify their payments by looking at their transaction history directly on the application, and financial transactions through the banks are now easier and cheaper, as enabled by the e-naira.

⁶¹ See submission by Defensoria Pública da União.

⁶² Ibid.

45. As the world of robotics and machine learning is developed, the question of who owns products, like paintings, created by a robot can make for an interesting reflection that may help to decide who owns the products or services created by such means.

5. Methodologies of digital transactions

46. Certain countries and institutions are allegedly pushing an anti-development agenda on data flows that appears to be harmful to the interests of the developing countries. Due to the fragmented ownership of the Internet, some users capture disproportionate gains, while others fail to benefit due to trade barriers, censorship, laws requiring local storage of data and other rules that limit the flow of goods, services and ideas.⁶³ Thus, there is an increasing need for global cooperation and coordination to regulate the Internet.

47. The connectivity-related digital divide is being widened by an emerging data divide, reflecting the substantial differences that exist between and within countries to harness data. Countries with limited capacities to turn data into digital intelligence and business opportunities and use them for economic and social development are at a clear disadvantage. It is important to broaden the international policy debate on harnessing cross-border flows of digital data.⁶⁴

48. Several countries are considering building a network of plurilateral trade arrangements, with a view to incorporating elements of the modern economy that are growing in importance, specifically digital services, harmonizing approaches to protecting the privacy of data and effectively enforcing trade policies and practices, both multilateral and bilateral.

49. Agreements in new areas, such as digital trade, the environment, micro, small and medium-sized enterprises, and women's economic empowerment need to be articulated. Connecting these businesses to value chains would make trade a direct instrument for socioeconomic inclusion.⁶⁵ Regionally, there are mechanisms like the Framework Agreement on Facilitation of Cross-Border Paperless Trade in Asia and the Pacific.

50. Common global rules for digital trade, complemented by action to narrow the digital divide, would lower the bar for businesses of all sizes to use the online economy to operate across borders. Reducing trade barriers to environmental goods and services is one place to start.⁶⁶ The High-level Panel on Digital Cooperation has also concluded that data flows are very different from trade flows and should not be included in trade negotiations.⁶⁷

51. Data is multidimensional by nature – with economic dimensions of private and social value that cannot be divorced from its other dimensions, such as those related to privacy, security and other human rights. A global approach is therefore needed in the governance of these flows to ensure data flow for the benefit of all, while human rights are safeguarded.⁶⁸ Human rights in the digital space cannot be overstepped, and data collection transparency, privacy protection and other “social” aspects of cross-border data flows must gradually become key topics on the agenda.⁶⁹

⁶³ Joseph S. Nye, “Who Owns the Internet? And Who Should Control It?”, World Economic Forum, 11 August 2016.

⁶⁴ UNCTAD, *Data and Digitalization for Development* (2022), pp. 17–18 and 52.

⁶⁵ World Trade Organization, “Multilateralism ‘Must Be Reimagined and Fit for Purpose,’ DG Tells Brazilian Diplomats”, 18 April 2022.

⁶⁶ *Ibid.*

⁶⁷ UNCTAD, *Data and Digitalization for Development* (2022), p. 69.

⁶⁸ *Ibid.*, p. 53.

⁶⁹ *Ibid.*, p. 80.

V. A human rights-centred approach to the fiscal elements of the digital system

A. Participation

52. The previous reports by the mandate holder have highlighted that participation, accountability and transparency are key pillars of fiscal legitimacy.⁷⁰ Civil society plays a key role here. In order to engage meaningfully in the development of policies, regulation and other measures relating to key areas of fiscal transactions (their creation, movement, storage, use review and analysis), it is critical to enhance the effective use of public resources for investment in human rights, including access to information.⁷¹ Financial and technical mechanisms are necessary to enhance timely access to information in order to hold decision makers to account and to provide effective guidance to States and other stakeholders.⁷² Digital technologies and online spaces are vital for the process of creating and distributing fiscal information. A major benefit of new technologies is their potential to empower individuals and groups and to enhance democratic citizenship by strengthening pluralist debates.⁷³ Journalists and civil society actors⁷⁴ must have open and secure access to online spaces, free from surveillance and censorship. Digital spaces are powerful platforms for spreading or reporting on good practices, empowering individuals, reporting abuse and mobilizing support.⁷⁵ States and online companies have a responsibility to ensure this and to make sure that recourse is available when threats arise.⁷⁶

53. Regulating the digital economy and taxing major digital companies would provide tax revenues that could be used to promote economic growth and accelerate development in all countries, especially in developing and least developed ones. Tax revenues are an essential pillar to fiscally support the realization of human rights and the mitigation of climate-related and other global shocks, and to reduce inequality and poverty and achieve the Sustainable Development Goals.⁷⁷

54. The adoption of digital technologies in financial transactions would generate enormous social and economic benefits amounting to hundreds of billions of dollars a year. According to a report issued by the World Bank,⁷⁸ the adoption of these technologies can lead to the creation of millions of jobs for young people and women. In this context, the report emphasized that the comprehensive adoption of digital technologies in the Middle East and North Africa would, over a 30-year period, double the rate of women's participation in the labour force, from 40 million to 80 million, and would lead to an increase in manufacturing employment by at least 5 per cent, equivalent to at least 1.5 million jobs. A comprehensive adoption of the system would also reduce frictional unemployment from 10 per cent to 7 per cent of the workforce over six years, allowing greater participation in national and global economies.

B. Accountability

55. Banking policymakers would often gain immensely from integrating dialogues on interoperability (the capability to exchange money from one supplier's mobile wallet to

⁷⁰ A/HRC/49/47, paras. 39 and 58.

⁷¹ Ibid., para. 58.

⁷² Ibid.

⁷³ A/HRC/47/52, para. 12 (a).

⁷⁴ Office of the United Nations High Commissioner for Human Rights (OHCHR), "Human Rights and Democracy in the Digital Age", 25 April 2022.

⁷⁵ A/HRC/47/52, para. 12 (c).

⁷⁶ See https://www.universal-rights.org/wp-content/uploads/2021/06/2021_URG_GLION_VII_REPORT_V6_PAGES_PROD_BD.pdf.

⁷⁷ See submission by Maat for Peace, Development and Human Rights.

⁷⁸ Ana Paula Cusolito and others, *The Upside of Digital for the Middle East and North Africa: How Digital Technology Adoption Can Accelerate Growth and Create Jobs* (Washington, D.C., World Bank Group, 2022).

another supplier's electronic account) with both telecommunications regulations and competition law enforcement agencies. Both comprehend dynamic marketplaces in the networking business, network externalities and the requirement of interoperability. To the digital financial service provider, client or customer safety is essentially a question that relates to financial regulation. Nevertheless, it also covers a number of concerns regarding the core telecommunication network, such as how costs are paid to customers. Disclosure about pricing and associated qualities of products is critical not just for consumer protection, but also for successful competition, since it allows consumers to evaluate the alternatives.⁷⁹

C. Access to information

1. Right to education and digital technologies

56. Digital technologies can bring important benefits regarding the creation and distribution of information on fiscal and financial matters. In order to become an empowering tool for all persons with regard to being an active member of society, including in the context of professional activities, and political and civic participation, digital education is essential.⁸⁰

57. First of all, it is important to understand the profit-driven agenda of digital technology lobbyists and companies.⁸¹ In addition, the digitalization of education should not increase inequalities and benefit already privileged segments of societies only.⁸² In both the global North and the global South, many individuals, especially those living in poverty, are deprived of access to education but are still dependent upon digital technologies for information. It is therefore essential to address the digital divide in order to tackle information inequality that may perpetuate pre-existing inequalities. Plans for digital education should be deployed in accordance with other human rights.⁸³

2. Fiscal legitimacy

58. Conflict hinders States in ensuring fiscal legitimacy and playing their welfare role. People living under occupation may be blocked from obtaining and communicating information, including all digital financial operations, without illegal interference to their privacy, as Internet and mobile operators might be under the control of occupying forces, impacting the country's information and financial sovereignty. Any Human Rights Council or General Assembly resolution on acts of aggression or breaches of the peace violating the norms of the Charter and related instruments should take into consideration global agreements on the regulation of technology.

59. While the digital economy is totally reliant on the growing interconnectedness of people, organizations and countries through the Internet, blocking countries' access to digital financial and banking platforms can have devastating effects on all human rights. The Society for Worldwide Interbank Financial Telecommunication, commonly known as SWIFT, facilitates secure and efficient communication among financial institutions around the world. Removing a country from the SWIFT platform – using unilateral coercive measures or economic sanctions that are imposed on countries beyond the authority of the United Nations and the rule of law – is a means of violating economic, social and cultural rights in sanctioned countries. Sanctioning a nation by eliminating its access to SWIFT can have negative impacts on how everyday individuals access basic amenities: access to medicines, food, sanitary products, medical equipment, medical care, health-care products and machinery, jeopardizing and risking many lives. Unequal access to digital financial platforms and to the

⁷⁹ Submission by Stephen Ngugi.

⁸⁰ [A/HRC/50/32](#), para. 96 (b).

⁸¹ *Ibid.*, para. 5.

⁸² *Ibid.*, para. 97.

⁸³ [A/HRC/50/32](#), para. 97 (b). See also submissions by Guatemala (in Spanish) and the Section on Archives on Human Rights, International Council of Archives; and [A/74/493](#), paras. 24, 29 and 45–46.

international market create complicated problems for nationals of sanctioned States who live or travel abroad, by blocking their access to bank accounts and bank cards.⁸⁴

3. International cooperation

60. Countries around the globe are facing a common threat posed by increasingly complex and innovative forms of financial crime. Tax avoidance and evasion, fraud, corruption, money-laundering and other financial crimes threaten the strategic, political and economic interests of all countries and undermine public trust in government and the financial system. Combating these closely related crimes requires financial transparency, more effective intelligence-gathering and analysis, robust legal and institutional frameworks, and effective cooperation and information-sharing between tax administrations and other law enforcement authorities.^{85, 86}

61. Additionally, the Global Forum on Transparency and Exchange of Information for Tax Purposes works on the implementation of global transparency and exchange of information standards around the world, with 165 members.⁸⁷ The procedures include automatic exchange of information or upon request, in which banking and accounting records as well as ownership of corporate entities and legal arrangements are shared between relevant authorities. It also provides a framework for obtaining information on request,⁸⁸ the automatic exchange of information⁸⁹ and capacity-building and technical assistance activities ensuring that all members receive support and benefit from the tools to implement the international tax standards.⁹⁰

4. Freedom of expression

62. The right to freedom of expression must be preserved online as well as offline and must go together with addressing online hate speech and disinformation. While social media provides unique opportunities for connecting with others and mobilizing public debate, it also presents several challenges to freedom of expression, such as companies' lack of effectiveness in responding to users' concerns, the opaqueness and troubling market dominance of these platforms, and Governments' failures to put in place rights-respecting regulation of this space. Crucially, any measures taken by companies and States to regulate speech must respond to the three-part test based on the principles of legality, necessity and proportionality.⁹¹

63. Hate speech and disinformation are rampant in the digital age, impacting negatively on human rights. In many countries, three quarters or more of the victims of online hate speech are members of minority groups. Women belonging to these groups are disproportionately targeted. Too often, hate speech is followed by hate crimes and violence, as it is used to prepare the ground for the dehumanization and scapegoating of minorities and for normalizing hate.⁹²

64. Internet and media shutdowns around the world, including in Europe, are also on the rise, impacting the political integrity, financial stability and national security of States, such as the use of Pegasus spyware in 45 countries, often in total secrecy and outside of any legal

⁸⁴ See submission by Organization for Defending Victims of Violence (ODVV), 2022.

⁸⁵ Ibid.

⁸⁶ OECD, "Tax and Crime".

⁸⁷ OECD, Global Forum on Transparency and Exchange of Information for Tax Purposes, "Putting an End to Offshore Tax Evasion".

⁸⁸ OECD, Global Forum on Transparency and Exchange of Information for Tax Purposes, "Exchange of Information on Request: A Robust and Transparent Review Process".

⁸⁹ OECD, *Standard for Automatic Exchange of Financial Account Information in Tax Matters*, 2nd ed. (Paris, 2017).

⁹⁰ OECD, Global Forum on Transparency and Exchange of Information for Tax Purposes, *10 Years of Capacity Building: 2022 Global Forum Capacity Building Report*.

⁹¹ OHCHR, "Human Rights and Democracy in the Digital Age", statement by the United Nations High Commissioner for Human Rights, 25 April 2022.

⁹² OHCHR, "Report: Online Hate Increasing against Minorities, Says Expert", 23 March 2021.

framework.⁹³ This type of technology, while innovative, has been used to violate the human rights of reporters or whistle-blowers who work towards the transparency of financial and tax information in digital systems.

5. Encryption and right to privacy

65. Powerful data-intensive technologies, such as big data and artificial intelligence, have the potential to create an intrusive digital environment. The use of such technologies both by States and private enterprises to conduct surveillance, analyse, predict and even manipulate people's behaviour can facilitate and deepen privacy intrusions.⁹⁴

66. Intrusive measures by States and businesses enable surveillance that feeds analysis, prediction and even manipulation of behaviour, at times to the detriment of free and fair elections and democratic processes. Recent revelations about global abuses of spyware, targeting journalists, human rights defenders, dissidents, opposition politicians and diplomats, are in flagrant violation of the right to privacy and the protection of personal data.⁹⁵ Encryption is a key enabler of privacy and security online, and it is essential for safeguarding rights, including the rights to freedom of opinion and expression, freedom of association and peaceful assembly. It ensures that individuals can share information freely, without fear that their information may become known to others, such as State authorities or cybercriminals. Encryption is essential if individuals are to feel secure in freely exchanging information, including financial information, with others.⁹⁶ In specific instances, journalists and human rights defenders cannot do their work without the protection of robust encryption, shielding their sources and sheltering them from powerful actors.⁹⁷ Encryption and anonymity tools can counter threats to privacy and allow users to exercise their rights to freedom of opinion and expression more safely. In parallel, national laws should be developed to ensure strong data protection, in line with human rights standards.⁹⁸

67. Functional democratic processes require a free flow of information. Whether during elections, conflicts or other complex emergencies, keeping free, pluralistic, independent information accessible to all, and allowing journalists and human rights defenders to perform their work, is paramount to the protection of human rights.⁹⁹

68. At the same time, these widely used encryption capabilities are abused to interfere with the rights of others, national security or the public order. Anonymous or encrypted communications make it difficult to investigate illicit financial flows, including tax evasion and tax avoidance, but also the transfer of funds arising from bribery and corruption, undermining democracy and the social contract.¹⁰⁰ The Stolen Asset Recovery Initiative by the World Bank Group and United Nations Office on Drugs and Crime found that the biggest challenge in an asset recovery case was producing the evidence that linked assets to criminal activities.¹⁰¹ Encryption makes it difficult for law enforcement and tax authorities to "follow the money".

69. Powerful data-intensive technologies are not only used for surveillance but also as an analysis tool for private companies to predict behaviour and habits. Artificial intelligence, for instance, is used by private financial institutions to calculate credit risks and is therefore used to determine the eligibility of borrowers and the terms of a loan. Algorithmic scoring models can facilitate and deepen privacy intrusions and further prevailing discrimination of

⁹³ [A/HRC/51/17](#), para. 4; and Bill Marczak and others, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries", Citizen Lab Research Report No. 113 (Toronto, Canada, University of Toronto, 18 September 2018).

⁹⁴ [A/HRC/39/29](#), para. 1.

⁹⁵ *Ibid.* See also [A/HRC/27/37](#); and [A/HRC/51/17](#), referring to the revelations about the use of Pegasus software by Forbidden Stories.

⁹⁶ [A/HRC/51/17](#), para. 21.

⁹⁷ *Ibid.*

⁹⁸ OHCHR, "Human Rights and Democracy in the Digital Age".

⁹⁹ *Ibid.*

¹⁰⁰ [A/HRC/29/32](#), para. 2.

¹⁰¹ Stolen Asset Recovery Initiative, "About Financial Investigations", available from <https://star.worldbank.org/focus-area/financial-investigations>.

already marginalized population groups, thereby intensifying inequality. Even if credit-scoring companies refrain from considering factors such as race or ethnicity, the models for scoring credit risks contain hidden biases against disadvantaged communities, limiting their access to credit, thus further financially excluding them.

70. Data-driven technology and artificial intelligence have a growing analytical power that may result in scoring and ranking of individuals to assess their eligibility for financial services and their terms (e.g., interest rates). This might intensify the marginalization and inequality of groups in society that are already discriminated against.¹⁰² They are then forced to accept loans with unfavourable conditions, furthering private debt or overindebtedness. The credit score algorithms themselves may not be biased against people from low-income groups, but the underlying data may be.¹⁰³ Firstly, the data is less accurate in predicting creditworthiness for groups that are already discriminated against and marginalized, often because those borrowers have limited credit histories. Secondly, the data set might reflect existing prejudices against minorities or women, or any other group in a situation of vulnerability.¹⁰⁴ Some scoring companies offer novel scoring models integrating data beyond traditional variables, focusing on behavioural clues to the borrower's personality, such as data on friends on social networks, fonts used in text messages or performance in fitness tracking apps.¹⁰⁵ Apart from exposing people's private lives to companies (and States), these data sets make individuals vulnerable in a number of other ways, such as data breaches exposing sensitive information.¹⁰⁶

VI. Conclusions and recommendations

71. **Digital technologies have a global impact on the lives of billions of people. The fast-growing digital economy has implications for human rights, the economy and the international financial architecture. While sometimes the impact of digital technologies can be positive, in others it can be negative.**

72. **The use of data in the digital economy is facilitating new and targeted products and services, as well as global trade. However, it is also a cause of concern due to violations of the right to privacy. Digital technologies are also being used to hamper the transparency of cross-border transactions, which in turn enables illicit financial flows and negatively influences conditions around debt sustainability. New digital lending practices via mobile applications are also important contributory factors to the rise in private debt and overindebtedness among households. In addition, the inadequate regulation of financial practices of private lenders and banks and abuse of digitally stored information contributes towards inequality and can breach the right to privacy. Cryptocurrency helps secure digital currency transactions, but at the same time it is also associated with a high risk of tax evasion and avoidance; and balances held in these accounts are untaxed. Encryption, while it enables privacy and security online can also be used to hinder investigations of illicit financial flows.**

73. **Insufficient financial accountability, transparency and integrity erodes the ability of countries to raise revenues and directly undermines their ability to realize human rights, the Sustainable Development Goals and economic development.**

74. **In order to address these challenges, the Independent Expert calls for the application of the rights and principles related to privacy, access to information,**

¹⁰² Edmund L. Andrews, "How Flawed Data Aggravates Inequality in Credit Scores", Stanford University Institute for Human-Centered Artificial Intelligence, 6 August 2021. See also [A/HRC/39/29](#), para. 16; and [A/HRC/48/31](#), para. 10 ff.

¹⁰³ See Laura Blattner and Scott Nelson, "How Costly is Noise? Data and Disparities in Consumer Credit", 17 May 2021, available at <https://arxiv.org/abs/2105.07554>.

¹⁰⁴ Karen Hao, "This is How AI Bias Really Happens – And Why It's So Hard to Fix", *MIT Technology Review*, 4 February 2019.

¹⁰⁵ Katja Langenbucher and Patrick Corcoran, "Responsible AI Credit Scoring – A Lesson from Upstart.com", in *Digital Finance in Europe: Law, Regulation, and Governance*, Emiliós Avgouleas and Heikki Marjosola, eds. (Berlin and Boston, De Gruyter, 2022), p. 165.

¹⁰⁶ [A/HRC/48/31](#), paras. 12–14.

participation, accountability, transparency and fiscal legitimacy, and for international cooperation and coordination on the development and deployment of digital technologies.

75. The regulation of the digital economy and taxing of major digital companies can provide tax revenues essential to promote economic growth and support development, particularly in developing and least developed countries. These revenues can provide financial support for the realization of human rights and investment in climate change mitigation initiatives, as well as efforts to reduce inequality and poverty, and to achieve the Sustainable Development Goals.

76. The Independent Expert makes the following recommendations to States, both individually and as members of various multilateral and international financial institutions and regional blocs:

(a) Engage in an open and continuous mutual cooperation with stakeholders across all sectors to ensure that technological advances do not compromise human rights and that digital economy innovations can be tapped to support the continued collection of resources for the realization of human rights;

(b) Encourage financial transparency, more effective intelligence-gathering and analysis, robust legal and institutional frameworks and effective cooperation and information-sharing between tax administrations and other law enforcement authorities, in order to fight increasingly complex and innovative forms of financial crime;

(c) Reframe and broaden the international policy debate on data flows and governance, moving away from a silo approach towards a more holistic and coordinated global approach. Trade policy and negotiations alone cannot fully address all aspects of data, both economic and non-economic in nature, and therefore need to be an integral part of global efforts to harness data and digitalization for sustainable development;

(d) Consider the impact of digital technologies on the right to a healthy environment, including by spreading green technologies and promoting net-zero carbon emissions;

(e) Allocate their fair share of taxing rights to all countries to tax the digital economy and the transfer of virtual assets and currencies. Low- and middle-income countries in particular should be able to tax major digital companies and platform businesses with an economic presence in their jurisdictions, to collect and mobilize the necessary revenues to finance the realization of human rights and the 2030 Agenda for Sustainable Development;

(f) Treat financial transactions in the metaverse as services provided in the physical world, and apply a specific legal framework to the metaverse based on human rights principles;

(g) Endeavour to adequately regulate the financial practices of private lenders and banks to curtail abuse of digitally stored information that affects particularly low-income groups;

(h) Create a neutral space where fiscal data on or related to digital systems is housed;

(i) Specifically with regard to multilateral institutions, including UNCTAD, contribute:

(i) To the establishment of synergistic linkages between e-commerce negotiations and the global debate on data governance;

(ii) To capacity-building in developing countries and least developed countries in order to bridge the digital divide, enhance digital inclusion and ensure effective participation in rule-making on e-commerce;

(iii) **To the development and implementation of national strategies and a regulatory framework on digitalization and data for sustainable development.**
