DEVELOPMENT FINANCE INSTITUTIONS AND DIGITAL RISKS

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

DEVELOPMENT FINANCE INSTITUTIONS AND DIGITAL RISKS

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

New York and Geneva, 2025

HR/PUB/25/1
ISBN: 978-92-1-159365-5
eISBN: 978-92-1-154325-4
Sales no.: E25.XIV.2

United Nations publication, issued by the Office of the United Nations High Commissioner for Human Rights (OHCHR).

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Symbols of United Nations documents are composed of capital letters combined with figures. Mention of such a symbol indicates a reference to a United Nations document.

The views and analysis expressed in this publication, as well as any errors, belong to OHCHR and should not be attributed to any of the commentators or contributors.

Cover image credit: © Adobe Stock/Generative AI/by Pete.

Contents

List of boxes

List of figures

List of tables

ACKNOWLEDGEMENTS

The content of this report is based on a literature review, consultations with bilateral and multilateral development finance institutions and a digital risk-mapping of nine multilateral development bank (MDB) portfolios in four sectors: (a) information and communications technology (ICT); (b) fintech; (c) health; and (d) public administration. The Office of the United Nations High Commissioner for Human Rights (OHCHR) assumes overall responsibility for the findings and recommendations contained herein. The views and opinions expressed in the report do not necessarily reflect the official policy or position of any of the contributors listed in these acknowledgements.

OHCHR wishes to acknowledge with gratitude the support of the Federal Ministry of Economic Cooperation and Development of Germany and the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) in connection with this report. OHCHR is grateful to Margaret Wachenfeld, Managing Director, Themis Research, for her research support in the preparation of this report; Amalia Palacios, Environmental Independent Researcher, for undertaking a digital risk-mapping analysis; Isabel Ebert, Adviser and Henrietta Dorfmüller, Research Associate, University of St Gallen Institute for Business Ethics, for technical guidance and an initial literature review and digital risk-mapping of ICT projects at eight MDBs; Gordon Myers, Senior Adviser, Sustainable Technology, Valoris Stewardships Catalysts, for technical guidance and a peer review; and Cathrine Bloch Veiberg, Head of Human Rights and Social Sustainability, UN Global Compact Network Denmark; Ioana Tuta, Senior Advisor, Human Rights, Tech and Business, Danish Institute for Human Rights; Angelina Fisher, Director, Policy and Practice, Global Law and Tech; Victoria Adelmant, Director of the Digital Welfare State Project, New York University School of Law; and Katelyn Cioffi, Senior Research Scholar, Digital Welfare State Project, New York University School of Law; as well as the other collaborators and commentators who have contributed their expertise, experience and time at various stages in the development of the present report, including: Dalile Antúnez, Jose Arraiza, Grant Binder, Laura Bingham, Maja Bott, Stefanie Brackmann, Sükran Çağlayan Mumcu, Debbie Cousins, Jens Deppe, Bruce Dunn, Tom Fisher, Sylvie Fraboulet-Jussila, Maria Isabel Gómez-Pineda Puebla, Christian Krämer, Barbara Linder, Greg Lockard, Neïla Mangin Maïza, Amar Mistry, Jeremy Ng Yung Jian, David Satola, Ute Sudmann and Lorenzo Urbinati.

Finally, OHCHR wishes to express its appreciation to the Federal Ministry of Economic Cooperation and Development of Germany, GIZ, the KfW Development Bank and the Danish Institute for Human Rights for their collaboration in organizing a webinar on the subject of managing digital risks in development finance, held on 11 September 2024, at which a number of the ideas, innovations and risk management practices presented in this report were discussed.

ABBREVIATIONS AND ACRONYMS

ADB	Asian Development Bank
AfDB	African Development Bank
AI	Artificial intelligence
AIIB	Asian Infrastructure Investment Bank
BII	British International Investment
DEG	Deutsche Investitions-und Entwicklungsgesellschaft mbH (German Investment and Development Corporation)
DFC	United States International Development Finance Corporation
DFI	Development finance institution
DPI	Digital public infrastructure
EBRD	European Bank for Reconstruction and Development
EIB	European Investment Bank
E&S	Environmental and social
FMO	Nederlandse Financierings-Maatschappij voor Ontwikkelingslanden N.V. (Dutch Entrepreneurial Development Bank)
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
IAM	Independent accountability mechanism
ICT	Information and communications technology
ID	Identification
ID4D	Identification for Development initiative
IDB	Inter-American Development Bank
IDB Invest	Inter-American Investment Corporation
IFC	International Finance Corporation
JICA	Japanese International Cooperation Agency
KfW	Kreditanstalt für Wiederaufbau (German Financial Development Cooperation or KfW Development Bank)
MDB	Multilateral development bank
MSME	Micro, small and medium-sized enterprise
OECD	Organisation for Economic Co-operation and Development
OHCHR	Office of the United Nations High Commissioner for Human Rights
SME	Small and medium-sized enterprise

FOREWORD

Thirty years ago, the Internet was only just beginning to transform our world. Since then, the digital technology revolution has dramatically and irreversibly reshaped the global economy, business, politics and virtually all facets of human interaction.

Digital technology can be a powerful driver of social development and economic growth. Digital technologies can bring Governments and citizens closer together, create economic opportunities, improve access to education, healthcare and other services, promote transparency and provide platforms for social and political interaction.

Digital technology development can also help create higher-value, skilled job opportunities, enhance financial inclusion and access to trade, and facilitate more effective and transparent governance and environmental management practices.

However, technological progress should not be confused or conflated with societal progress. The opportunities and benefits of digitalization are not available to all: according to the International Telecommunication Union, about one third of the global population remained offline in 2024. Moreover, as is described in the present report, digital technologies can be laden with serious and potentially irremediable human rights risks, at all stages of the data cycle.

The human rights risks of digital technologies can be latent, dynamic and unpredictable, and are often deeply dependent upon context. Specific digital technology choices in any given context can have profound, diffuse and enduring consequences.

In September 2024, at the Summit of the Future, world leaders adopted the Pact for the Future, which includes the Global Digital Compact and the Declaration on Future Generations. The Global Digital Compact is explicitly grounded in international human rights law and seeks, among other things, to close all digital divides, expand inclusion in and increase benefits from the digital economy for all, and foster a digital space that respects, protects and promotes human rights.

Development finance institutions have a vital role to play in leveraging their financing and technical know-how to ensure that digital development contributes to better human rights and development outcomes. Robust, comprehensive environmental and social risk management policies, anchored explicitly in internationally recognized human rights, should be seen as an indispensable component in the journey towards more sustainable and equitable digital transformations.

I am grateful to all the development finance institutions and other partners that have contributed in various ways to the preparation of this report. I trust that it will serve as a valuable resource for all actors committed to rights-respecting digitalization and sustainable development.

Volker Türk

United Nations High Commissioner for Human Rights

EXECUTIVE SUMMARY

Digital transformations are changing our world – the way we work, the way we interact and the way we do business. Bilateral and multilateral development finance institutions (DFIs) have growing portfolios supporting these transformations. The main focus to date has been on helping public and private sector clients harness the opportunities of digital transformation through financing, technical assistance, knowledge products and advisory services that support the development of relevant policy, legislation and standard-setting.

However, there is growing recognition that digitalization can be a "double-edged sword".[1] The underlying theories of change and the evidence base regarding the link between digital transformation and development outcomes are not always sufficiently robust in projects and in guidance. The design, use and regulation of digital products and services can create potentially adverse impacts for people and the environment ("digital risks") and complex, actual adverse impacts (harms) across populations, time periods and geographies. These may include violations of the right to privacy, the right to freedom of expression and association, the right of access to information, the right to equality and non-discrimination, the right to effective remedy and the right to participation, as well as a wide range of other civil, cultural, economic, political and social rights.

In 2024, the Office of the United Nations High Commissioner for Human Rights (OHCHR) carried out a mapping of 3,450 projects supported by nine major MDBs, representing billions of dollars in financing and advisory services, in order to shed light on how digital risks are identified and addressed. The growing volume of DFI-financed digital projects, which can range from wide-scale digital transformations to the integration of digital tools across sectors, raises pressing questions as to how digital risks are managed. The mapping exercise, part of a mixed methods research programme, suggests that MDBs have significant and growing exposure to adverse impacts on stakeholders from the development and use of digital technologies, and that potential adverse impacts and actual impacts are not systematically being identified and factored into project design and supervision on the basis of clear, transparent and enforceable standards. This in turn raises questions about how DFIs are implementing their mandates to do no harm and to contribute to positive development outcomes in this growing area of their portfolios.

Environmental and social (E&S) risk management is a central feature of bilateral and multilateral DFI operations and a prerequisite for project quality and sustainability. DFIs manage E&S risks to and impacts on stakeholders in the projects they finance through a range of policies, processes and tools. The present report uses examples from a wide range of initiatives of major MDBs and, to some extent, from bilateral DFIs, relevant to the assessment and management of digital risks. These include digital strategies and DFI approaches to what is referred to in this report as "digital risk management", which is the management of the risks of adverse impacts on people and the environment of digital transformations through digital projects, products and services. A wide range of other tools, contractual provisions, standard-setting exercises, publications and operational policies are also considered in the

[1] Organisation for Economic Co-operation and Development (OECD), *Development Co-operation Report 2021: Shaping a Just Digital Transformation* (Paris, 2021), p. 8.

present report. The important contribution of the World Bank publication entitled *World Development Report 2021: Data for Better Lives* and the Asian Development Bank (ADB) report entitled *Managing Digital Risks: A Primer* in highlighting and facilitating analysis of the human rights dimensions of digital risk management is recognized.[2]

Board-approved E&S safeguard policies play a central role in E&S risk management for DFI projects and investments. Unlike many other kinds of operational policies and approaches, E&S safeguard policies:

- **Establish binding requirements for DFI due diligence and client E&S risk management**, specific to the different stages of the DFI project cycle;
- **Are the product of public consultation processes, which can confer legitimacy**, strengthen ownership and trust and ensure that a wide range of stakeholders' views and perspectives are reflected;
- **Are approved by the executive boards of the DFIs**, which confer authority and facilitate their systematic implementation;
- **Are backed by independent accountability mechanisms (IAMs)**, which is particularly important in facilitating access to remedy for project-affected people, minimizing negative externalities of projects and strengthening lesson learning and feedback loops from operations to policy.

The safeguard policies of the leading MDBs have also indirectly influenced national laws and policies on E&S issues, in addition to their direct benefits at the project level. Hence, for all these reasons, what is included in DFI safeguard policies, and what is omitted, matters.

For the most part, since the 1980s, E&S risk management in DFI-financed operations has been focused on a particular set of E&S risks associated with traditional investment projects with a relatively well-defined physical footprint. Examples include resettlement, health and safety concerns, Indigenous Peoples' rights and pollution and other environmental impacts. However, neither E&S safeguards nor national laws and regulatory frameworks (with some exceptions) have kept pace with the risks presented by digital projects and advisory services that DFIs are financing.

Digital risks (potential adverse impacts) and actual adverse impacts from the design, use and regulation of digital technologies are different from more traditional E&S impacts in various important ways. Adverse impacts from the use of digital technologies can:

- Be **far more pervasive in scope** than the impacts of even the largest physical footprint projects because of the potential number of users;
- **Spread easily and quickly**, because digitalization, as a result of its scalability, permits the more widespread proliferation of harms;
- Introduce **novel harms** that are not possible with physical impacts (for example, through the recombination of information);

[2] See World Bank, *World Development Report 2021: Data for Better Lives*, (Washington, D.C., 2021); and ADB, *Managing Digital Risks: A Primer*, (Manila, 2023).

- Be **magnified easily, in terms of the scale, scope and irremediability of the impacts**, because the impacts can easily be repeated over and over again;
- **Amplify inequalities**, for example, from artificial intelligence (AI) datasets that reproduce pre-existing discrimination against particular population groups (particularly those already vulnerable or marginalized), or where access to technological infrastructure is limited by geography, literacy, health or other socioeconomic factors;
- **Exist perpetually**, with more long-lasting effects given that data can remain in the cloud, on social media, stored in computers and be reviewed or accessed indefinitely;
- Be **more ephemeral than physical records**, creating problems when digital records are lost through errors or changes;
- Be **far more prevalent**, because harms can occur across each and every function of the data-handling cycle: data generation, processing, storage and use, reuse or misuse;
- Be **out of the control of individuals** who do not maintain their own records or who are not able to control who has access to them;
- Be **invisible to those affected** because the processes are technical, opaque, complex and interlinked and often buried in coding language that even experts may be unable to decipher;
- Be **impossible to be aware of unless specific monitoring is in place**, without which the identification of harms may emerge only belatedly or haphazardly;
- **Disperse exponentially across affected stakeholders**, which may challenge the current generation of E&S safeguard policies under which potentially affected stakeholders are identified based on their physical proximity to the project;
- **Defy current approaches to classifying project risks**, including the correlation between E&S risks and the size of the project or company;
- Be **more challenging to assess** against the backdrop of constant, rapid innovation and the multiplication of emerging uses;
- Be **more unpredictable**, as some digital technologies and services may more easily be reused or redeployed in a way not contemplated when a project was originally conceived;
- Be **unknown at the time of financing** (for example, where DFIs are financing new business models or new start-ups, due diligence may be carried out before the start-up has fully developed or been launched);
- Be **more cumulative than impacts from physical projects**, such as in cases where a number of different types of technologies and data are pooled;
- Have **more of a "honeypot" effect than many physical projects**, given the high commercial value of potentially large amounts of pooled data, which may be vulnerable to data breaches and theft;
- Be **far harder to remedy**, given differences in the temporal and geographical dispersion of digital impacts, the irremediability of numerous digital harms and the challenge of developing appropriate reparations;
- Entail **regulatory challenges**, given the mismatch between the transboundary nature of technology and the jurisdictional boundaries of governance and regulation.

Notwithstanding these challenging risk characteristics, as the research for the present report highlights, the great majority of digital projects reviewed by OHCHR, including technical assistance projects providing regulatory advice, were assigned a risk classification of "C" or "low", or were given no risk classification at all. Risk classification has significant implications for the resources and due diligence assigned to projects. The distinctive characteristics of digital risks, and the apparent under-classification of digital risks to date, imply the need, in the opinion of OHCHR, for a generational change in DFI risk management approaches. A more systematic approach to identifying and mitigating digital risks, along with a proportionate risk-based approach, would contribute to better development outcomes.

Given the increase in the financing of projects involving digital risks, and given the relatively weak regulatory and institutional frameworks (including with regard to digital risk management) in many developing markets, **the central recommendation of OHCHR is that DFIs adopt transparent, systematic and enforceable standards to govern the identification and management of digital risks and impacts in DFI-supported projects, supported by expertise, awareness-raising and capacity-building among staff, clients and partners**. Another recommendation contained in this report is that E&S safeguards should play a central role in this regard, accompanied and reinforced by digital strategies, risk assessment tools and guidance. It is recognized that the process of updating E&S safeguards may take time and that, until those new requirements are in place, DFIs should adopt clear and transparent guidelines to require the assessment and management of a wide range of digital risks, which may include moratoriums on certain types of projects. The recommendations made in this report on the potential role of E&S safeguards should not deflect from the need to take other measures necessary to manage and disclose management of digital risks in the interim, including those detailed below and in chapter III.

At the time of writing, a response to these demands was beginning to be seen in E&S safeguard policies. Examples include the integration of several data protection, privacy and related digital risks within the European Bank for Reconstruction and Development (EBRD) Environmental and Social Policy and the ADB Environmental and Social Framework. While limited in scope and not yet sufficient to address all the risks highlighted in this report or in the respective portfolios of these banks, these provisions nonetheless represent an important start and, in the view of OHCHR, may form the backbone of more robust and consistent approaches to digital risk management.

The analysis in this report supports the following recommendations:

- **DFI digital strategies should specifically identify and address risks alongside opportunities in digital transformation projects**, in order to signal to staff, clients and stakeholders that banks take these risks and impacts seriously and will require them to be addressed as part of DFI support.
- **DFIs should develop clear guidance for staff on prerequisites for supporting potentially risky digitalization projects**, "red flags" for more intensive pre-project appraisal and escalation criteria where more extensive analysis and senior management judgment calls are warranted. Where potential digital harms are particularly severe (in terms of scale, scope and irremediability), these should be incorporated into exclusion lists.
- **DFIs should update their board-approved E&S safeguard policies to cover digital risks**, and should take a three-tiered approach to adapting existing E&S safeguards to the demands of digital risk assessment and management: (a) adapting sustainability policies (applicable to DFIs) to include specific requirements for digital risks; (b) adapting existing performance standards/requirements (applicable to clients) so that the digital risk issues embedded within existing E&S standards are identified and addressed; and (c) adding a new digital-specific performance standard or requirement, applicable to clients, that applies to digital components of projects (see annex I to the present report). Other measures to manage and disclose the management of digital risks should be encouraged in the interim.
- **The specific requirements of updated E&S safeguards should be aligned explicitly with the United Nations Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct as well as related OECD guidance**, which are increasingly reflected in regional and national regulatory frameworks and set higher standards than most DFI E&S safeguard policies on due diligence and risk management throughout the value chain, including in relation to downstream impacts on users and consumers of digital products and services.
- As a necessary complement to updated E&S safeguards, and to help operationalize digital risk management requirements, **DFIs should invest further in the development of tools on digital risk assessment and management**, building on emerging digital risk management tools and regulatory frameworks and the long-standing experience of DFIs in developing other kinds of E&S tools.
- **DFIs should strengthen transparency** through:
  - Disclosing a description of their risk management approach, including their appetite for managing these risks as part of their financing or advisory services;
  - Updating and disclosing exclusion lists and red flags in order to provide clarity to staff, clients and relevant stakeholders about what kind of digital risks are considered unacceptable and what kind of mitigation and remedial measures may be needed for higher-risk projects;
  - Issuing requirements for the systematic public disclosure of digital risks and management measures for relevant projects as part of project disclosures in updated E&S safeguards and access to information policies;

  - Improving project databases to permit easy searches for digital and venture projects so that institutional policy performance can be assessed;
  - Making clear, consolidated information on digital work publicly available on DFI web pages;
  - Providing a clear evidence base for choices made on digital projects through *ex-post* evaluations and other learning tools. DFIs should also be encouraged to disclose E&S monitoring reports.
- **DFIs should strengthen stakeholder engagement through the following measures:**
  - Developing or adapting tools for and approaches to identifying stakeholders in digital projects, targeted DFI staff and clients, and adapted to the digital environment;
  - Developing or adapting tools for and approaches to meaningfully engaging with stakeholders, including civil society organizations with specific expertise in digital issues, given the technically demanding and rapidly changing nature of this field;
  - Updating approaches to protection against reprisals for online participation. Clear requirements on this issue will be needed in updated E&S safeguards, for DFIs and clients, accompanied by detailed procedures.
- **DFIs should enhance accountability for digital projects and advisory services** through the updating of E&S safeguard policies according to the recommendations outlined above and the following complementary measures:
  - Fit-for-purpose client grievance mechanisms. New explicit requirements, specific expertise and procedural adaptations will be needed in order to enable client redress mechanisms to respond to digital impacts.
  - A stronger accountability ecosystem. Greater attention needs to be paid to understanding and strengthening the wider accountability ecosystem for addressing and remedying digital harms at the national level. Attention to digital issues should also be integrated into broader rule of law, justice and security reform work. There may be a wide range of actors involved in protecting against or adjudicating digital rights violations at the national level in any context, including national data protection authorities, consumer protection authorities, ombudsperson institutions and national human rights institutions. DFIs should be encouraged to consider how they may support this wider accountability ecosystem.
  - Fit-for-purpose IAMs. Just as DFI teams will need to build expertise and capacity, IAMs will require additional expertise to assess and address complaints dealing with digital technologies. More systematic disclosure and outreach in relation to the existence of IAMs is also needed.
  - Clearer links to IAMs. At the time of writing, only one case involving a digital project had been filed with an IAM of the nine major MDBs covered in the present report. DFIs and clients should be required to disclose the option of filing complaints to IAMs, and these mechanisms should be encouraged to expand their outreach activities to include actors dealing with digital technology impacts on users and communities.

  - Extension of IAM time frames to submit complaints. There may be long lead times before latent harms from digital impacts eventually materialize. It is vital that mechanism admissibility requirements are defined by reference to the date of the detection of harm, rather than project closure or other fixed cut-off dates.

- **DFIs should build the capacity and expertise of their E&S safeguard teams** to strengthen the stewardship and supervision of digital projects.

- **DFIs should strengthen coordination across digital expertise in different organizational functions** in order to enable 360-degree appraisal of projects.

© Adobe Stock/Generative AI/by Anastasiia

CHAPTER I
INTRODUCTION AND OVERVIEW

A. INTRODUCTION

Digital technologies are transforming our world at an exponential rate. The digital economy is a powerful driver of growth. All sectors of the economy and virtually all Sustainable Development Goals (SDGs) can benefit from digital innovation and investment.[3] Digital technologies can bring Governments and citizens closer together, create economic opportunities, improve access to education, healthcare and other services, promote transparency and provide platforms for social and political interaction.

However, digital transformations also bring E&S risks, including risks to internationally recognized human rights.[4] The Global Digital Compact,[5] adopted by member States of the United Nations in 2024, contains a set of objectives and commitments for global governance of digital technology and AI. The importance of principled guidance and strong human rights guardrails in guiding technological innovation has been highlighted by the General Assembly and the Human Rights Council.[6] Research and reporting on the human rights dimensions of digital transformations has been carried out by OHCHR, in which it recognizes that anticipating and mitigating the potential harm to people and the environment caused by designing, developing and deploying digital technologies are integral to realizing their benefits.[7]

Within this global push for responsible digital governance spurred by the Global Digital Compact, MDBs and bilateral DFIs, together collectively referred to as DFIs in the present report, play an important role in realizing a rights-respecting digital transformation. MDBs are funding an ever-increasing range of digital projects and initiatives, bringing the benefits of digitalization to millions across the globe. At the same time, such investments can also have profound and pervasive adverse human rights impacts. If DFIs make decisions and provide finance in a rights-respecting manner, development finance can act as a powerful

[3] See, for example, OECD, "Digital transformation in the age of COVID-19: Building resilience and bridging divides" (Paris, 2020); World Bank, *Digital Progress and Trends Report 2023* (Washington, 2023), chap. 2; and DEG, AfricaGrow and Steward Redqueen, *Responsible Investment in Technology: Market Study on the ESG Risks of Technology Investments* (Cologne, 2024), table 3.

[4] For a mapping of how the rights enumerated in the Universal Declaration of Human Rights are impacted in the digital world, see Michael J. Kelly and David Satola, "Internet human rights", *Journal of Law and Social Change*, vol. 26, No. 3 (2023), pp. 255–332. On the human rights impacts of generative artificial intelligence specifically, see OHCHR, "Taxonomy of Human Rights Risks Connected to Generative AI".

[5] The Global Digital Compact was adopted in 2024 by the General Assembly in its resolution 79/1 as part of the Pact for the Future.

[6] See, for example, A/RES/78/213; A/HRC/RES/53/29; A/HRC/56/45; A/HRC/51/17; A/HRC/48/31; A/HRC/44/24; A/HRC/39/29; A/HRC/27/37; and United Nations, "Hub for Human Rights and Digital Technology".

[7] See, for example, A/HRC/27/37; A/HRC/39/29; A/HRC/44/24; A/HRC/48/31; A/HRC/51/17; and A/HRC/56/45. See also United Nations, "Hub for Human Rights and Digital Technology"; and OHCHR, "Digital Space and Human Rights" and "B-Tech Project".

driver of responsible digitalization. Technology design and development and consequential risk management actions today may have impacts for generations to come.

The point of departure for this work is the OHCHR *Benchmarking Study of Development Finance Institutions' Safeguard Policies*, in which the absence of digital risk management is identified as among the most significant gaps in the current generation of DFI E&S safeguard policies.[8] The purpose of this report is to analyse current DFI policy and practice in connection with digitalization and digital transformations; highlight progress and apparent gaps in digital risk management; and provide recommendations for improvement. Specifically, the report addresses the following questions:

- What does the contemporary digital investment landscape of DFIs look like?
- How are DFIs adapting their risk management practices to identify and manage digital risks in connection with digital innovation, and where are gaps in policy and practice?
- How can the management of digital risks be better integrated into DFI policies, practice and accountability?

This report is in no way intended to undermine the case for DFIs to finance digital projects. Rather, it aims to assist DFIs in improving outcomes by prompting more specific attention to the risks of digitalization, whatever the benefits may otherwise be. DFI approaches to what the report refers to as "digital risk management" (e.g. the management of risks of adverse impacts on people and the environment of digital transformations through digital projects, products and services) is crucial in this regard. However, the limited transparency about current DFI approaches to digital risk management, as well as the opaque nature of some of the digital technologies, mean that even serious potential harms may not be immediately apparent. In the absence of comprehensive, transparent and enforceable[9] digital risk management requirements for DFI-financed projects, it will be more likely that harms and costs will be externalized to people and the environment, contrary to DFI mandates.

The impact of digitalization on human rights is a central preoccupation of the United Nations.[10] The Global Digital Compact contains a set of principles for achieving the goal of an inclusive, open, sustainable, fair, safe and secure digital future for all through digital cooperation that rests on international law, including the Charter of the United Nations, international human rights law and the 2030 Agenda for Sustainable Development. The Digital Compact commits signatories to respecting, protecting and promoting human rights in the digital space and to

[8] See OHCHR, *Benchmarking Study of Development Finance Solutions* (2023). In the present report, "E&S safeguards" or "safeguards" refer to board-approved operational policies that establish environmental and social due diligence and risk management requirements for MDBs/DFIs and clients, respectively, across all phases of the project cycle. Following the example of the IFC, MDB safeguards often take the form of a "policy", which defines the bank's own due diligence requirements, and a set of 8–10 MDB standards applicable to the client. Many private sector DFIs have adopted the IFC Performance Standards. Most MDBs have safeguards with a broad scope, covering most or all of their operational activities and financing modalities (though less commonly, advisory or technical assistance work). However, this is not a uniform practice. For example, the World Bank has an environmental and social framework that applies only to investment project financing and has separate board-approved policies for development policy and programme-for-results financing.

[9] In public administration, the main constituent elements of "accountability" are "responsibility, answerability and enforceability". The concept of "enforceability" does not necessarily mean enforcement through formal judicial or legal mechanisms. Rather, more generally, it requires putting in place mechanisms that monitor the degree to which officials and institutions comply with established standards and ensure that appropriate corrective and remedial actions are taken when this is not the case. See, for example, OHCHR and the Center for Economic and Social Rights, *Who Will be Accountable? Human Rights and the Post-2015 Development Agenda* (New York and Geneva, 2013). Contractual provisions for remedy play a potentially critical role in this regard, among other leverage options that may be at the disposal of a DFI in any particular context.

[10] See United Nations, "Hub for Human Rights and Digital Technology"; and OHCHR, "B-Tech Project".

adopting appropriate safeguards to prevent and address any adverse impact on human rights arising from the use of digital and emerging technologies.[11] As public sector financiers of these developments, DFIs are within the scope of the Compact commitments, and regional and international organizations have been invited to endorse it.

The legitimacy and centrality of human rights in the development and regulation of digital technology are increasingly recognized.[12] The international human rights framework helps to define the content and consequences of digital risks, as well as how to address them. The United Nations Guiding Principles on Business and Human Rights[13] set out a risk-based approach to managing business impacts on human rights that is increasingly being used by the technology sector and DFIs. This approach is also an important element that is re-emphasized in the United Nations Global Digital Compact.[14] The Guiding Principles and their extensive implementation guidance, including for the technology sector,[15] may inform the actions of DFIs and clients across a range of important functions, including risk prioritization, strengthening value chain due diligence, building and exercising leverage, and enabling and providing remedy, which are critical for the successful identification and management of digital risks. The Guiding Principles are closely aligned with the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct[16] and are increasingly reflected in a wide range of other international standards and regulatory frameworks specific to the digital sector, such as the European Union Digital Services Act[17] and the European Union Artificial Intelligence Act,[18] as well as emerging regulatory approaches in other States such as Brazil, Kenya, the Republic of Korea and Thailand, and a deepening web of regulation on responsible business conduct at the regional and national levels.[19]

The present report seeks to make the case for the introduction or strengthening of guardrails that may help to harness digital technologies for sustainable development objectives, rather than creating new challenges and insecurities. Many emerging national and international regulatory frameworks are also developing in this direction.[20] However, in the view of OHCHR, it will be difficult to achieve consistent practice without balanced digital strategies accompanied by comprehensive, transparent and enforceable digital risk management requirements that are applied systematically across the project cycle. OHCHR would argue that E&S safeguard policies have a particularly important role to play in this regard.[21] Safeguard policies are

[11] United Nations, Global Digital Compact, paras. 22 and 23.

[12] For example, the Institute of Electrical and Electronics Engineers (IEEE), one of the key standard setting bodies in the digital space, listed the respect, promotion and protection of internationally recognized human rights as the first principle in its set of general principles on ethically aligned design of autonomous and intelligent systems. See IEEE, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (2019).

[13] OHCHR, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect Remedy" Framework (New York and Geneva, 2011).

[14] United Nations, Global Digital Compact, paras. 22, 23 and 50. The Guiding Principles on Business and Human Rights are increasingly being integrated into E&S risk management policy and practice in public and private sector financing DFIs. See OHCHR, *Benchmarking Study of Development Finance Institutions' Safeguard Policies*.

[15] See United Nations, "Hub for Human Rights and Digital Technology"; and OHCHR, "B-Tech Project".

[16] See OECD, *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct*, OECD Publishing (Paris, 2023). See also OECD, *Responsible Business Conduct – Digitalisation and Responsible Business Conduct: Stocktaking of Policies and Initiatives* (2020) and "Responsible business conduct in the financial sector – Operationalizing RBC due diligence amongst financial sector practitioners" guidance.

[17] European Commission, Digital Services Act (2022).

[18] European Commission, Artificial Intelligence Act (2023).

[19] See the Business and Human Rights Resource Centre, "Mandatory due diligence".

[20] See OECD, "Digital Policy Platform".

[21] See footnote 8 on "E&S safeguards".

in most cases the main board-approved instrument that governs E&S risk management in DFI-financed projects. The purpose of safeguard policies is to establish clear, differentiated and contractually enforceable requirements for the DFI and clients, backed by transparency and independent accountability, all of which are indispensable to the growing challenge of managing digital risks across DFI portfolios.

The research undertaken for this report intentionally cast a wide net over the policies and practices of nine of the major MDBs[22] and, to a lesser extent, some of the leading bilateral DFIs.[23] These institutions have similar (though not identical) mandates and E&S policies, they are increasingly focused on digitalization and they frequently act in concert. The purpose in so doing was to sample from as wide a range of relevant practice as possible, distil broadly applicable recommendations and stimulate cross-fertilization of policies and practice. The present report provides an indicative rather than exhaustive review of DFI digital-related financing. The main trade-off is that it is not always possible within this report to analyse in depth, or draw many definitive conclusions in relation to the policies and practices of any particular institution. A certain degree of generalization is unavoidable and many of the conclusions of this report are qualified or attenuated as a result. Moreover, comparability between DFIs is constrained by material differences in the various mandates, legal frameworks, operations and policies of the institutions, as well as differences in disclosure practices, project terminology and sectoral categorization. In particular, the approach of OHCHR to the research for this report is sensitive to distinctions between sovereign (public sector) and non-sovereign (private sector) operations, given the distinctive mandates, operational contexts and leverage options associated with each.

DFIs are supporting digitalization in many ways. Some projects support public sector transformations for digitalizing governance and public service delivery, including through digital identification (ID) systems, which may fundamentally alter the way that Governments interact with their populations. These types of projects are increasingly being captured under the umbrella of digital public infrastructure (DPI), which was likened in its early stages to “the roads and bridges of our new digital era”, enabling countries to transport vital digital solutions to communities,[24] but which has more recently come to be recognized as a more significant, society-wide digital system.[25] DFIs frequently support projects that involve the integration of digital components into more traditional investment projects in the health, education and finance sectors, among others. Many DFIs have venture capital windows supporting innovative tech start-ups and some provide advisory services, including regulatory advice, for digital transformations.

The present report, and the main body of empirical research on which it was based, focuses on four sectors: public administration, finance, health and digital infrastructure and services. DFIs also support digital transformation in other sectors, such as agriculture, education,

[22] These include the Asian Development Bank (ADB), Asian Infrastructure Investment Bank (AIIB), African Development Bank (AfDB), European Bank for Reconstruction and Development (EBRD), European Investment Bank (EIB), InterAmerican Development Bank (IDB), IDB Invest, International Finance Corporation (IFC) and the World Bank.

[23] British International Investment (BII), German Investment Corporation (DEG), Dutch Entrepreneurial Development Bank (FMO), Finnish Fund for Industrial Cooperation Ltd. (Finnfund), Japan International Cooperation Agency (JICA), Swedfund International AB (Swedfund) and United States Development Finance Corporation (DFC).

[24] United Nations Development Programme, “UN Tech Envoy and UNDP launch initiative to ensure that digital infrastructure turbocharges the SDGs safely and inclusively”, 17 September 2023.

[25] See United Nations, Office for Digital and Emerging Technologies.

infrastructure and urban development. The main reasons for focusing on the four selected sectors were that they: (a) cover both the public and private sectors; (b) entail the relatively widespread use of digital technologies and relatively well-known digital risks; (c) may involve system-wide changes with deep and enduring implications for people (in particular, public administration and digital infrastructure projects); (d) may involve the collection and management of sensitive personal data; and (e) may be more likely to involve services to people, thus implicating their rights in a very direct way.

A detailed explanation of the methodology for this report is provided in annex II, including the search terms used to identify the digital projects covered. Research undertaken for the report included reviews of: (a) DFI digital strategies; (b) DFI publications, guidance and tools; (c) academic literature and project-level and policy analyses by civil society organizations; (d) a programme of semi-structured interviews with practitioners in DFIs; (e) written survey responses from DFIs to a set of questions on their digital risk management policies and practices; and (f) four reviews of project documentation from DFI project databases between 2023 and 2024, including an analysis of 3,450 projects across nine DFIs followed by more in-depth reviews of selected DFI projects.[26]

Several projects were selected on an illustrative basis for detailed analysis, based on publicly available project documentation, including project appraisal reports, project descriptions and E&S documentation. OHCHR notes that there is far more detailed project appraisal information available for public sector projects than for private sector projects. While project preparation documentation does not always provide a detailed picture of project implementation, it serves the critical purpose of providing stakeholders with advance notice of projects in order that any concerns can be raised and addressed in a timely and effective fashion.[27] Further project documentation, such as supervision or monitoring reports, may provide additional insights into how digital impacts are materializing and being addressed in practice.

When determining the scope of the research for this report, a threshold question was how much attention to give to risks and risk-management approaches associated with potential misuse of AI. The potentially severe and unpredictable nature of AI-related risks,[28] and the narrative around these risks, have created a global industry in ethical principles and policy and regulatory initiatives.[29] Certain DFIs have actively been exploring the role of AI in development, and to a more limited extent, in relation to human rights.[30] This report draws on some of the latter work and considers a number of AI-related risks at project level, but does

[26] See annex II.

[27] Project disclosure is an important dimension of DFI accountability, governance and corporate responsibility. See, for example, EIB, "Transparency and access to information".

[28] Center for AI Safety, "Statement on AI risk".

[29] Simon Chesterman, "The tragedy of AI governance", Just Security, 18 October 2023. For example, according to the AI Ethics Guidelines Global Inventory, there were 167 guidelines in existence as of April 2024.

[30] For example, in 2022 the World Bank launched the Tools for Identifying the Human Rights Impact and Algorithmic Accountability of Artificial Intelligence in World Bank Operations project aimed at developing tools and guidance needed to support operational teams to ensure that World Bank-financed projects adequately address AI-related risks, building on the rights-based framework for data enablers and safeguards established in the *World Development Report 2021: Data for Better Lives* (2021). See also World Bank, *Digital Progress and Trends Report 2023*, chap. 5, p. 85: "AI holds potential to accelerate productivity growth, expand opportunities, improve consumer welfare, and bring vast benefits to the global economy and society. However, the use of AI systems and tools could also cement big tech's market dominance, displace workers, widen inequality, strengthen the state's surveillance abilities, erode privacy, turbocharge misinformation, manipulate democratic processes, and increase security vulnerabilities". For a succinct account of some of the opportunities and challenges associated with AI and development, see Rabi Thapa, "Developing AI for development", World Bank, 9 April 2024.

not attempt anything close to a comprehensive analysis of how AI may affect DFI financing and project outcomes. In the view of OHCHR, the breadth, dynamism and complexity of the AI field would seem to justify a separate report.[31] The second reason for avoiding an extensive focus on rapidly advancing AI technologies, including generative AI, is that such an emphasis might unwittingly deflect attention away from many other kinds of digital risks that may still be severe and pervasive and deserve specific attention by DFIs, their shareholders and stakeholders in projects recently and currently being financed. As highlighted in the research undertaken for this report, there are already significant digital risks in DFI portfolios, even without the layers of risks that new forms of AI may add. While this report makes a modest contribution to baseline recommendations concerning risk management strategies for DFIs, which will significantly overlap with addressing AI risks, the increasing global attention to AI can be expected to drive innovation and adaptation of AI risk management approaches considerably further.

An additional choice on scope, OHCHR considered whether to focus on DFI exposure to digital risks through venture capital and start-up investments, which mostly occur through financial intermediary loans and investments. In this context, the risks may often be asymmetric to the company development stage and size of the enterprise, particularly where digital risks are involved: small players may have very significant impacts that are not considered or foreseen at early stages before their products or services garner wide uptake. Existing E&S management systems may be difficult to implement in the context of the small scale of many venture capital investment funds and start-ups, and in any case are not likely to incorporate sufficient attention to digital risks. Given these factors, along with the constraints of space and (often) variable approaches of DFIs to managing E&S risks for financial intermediary investing as compared to direct investments,[32] it was not possible to discuss these issues in depth. Nevertheless, for OHCHR, this would seem to be an important area for further research.

In chapter I of this report, the context is set for chapters II and III. Section B provides an overview of the opportunities and risks associated with digitalization and offers a definition of digital risks for the purposes of the present report. Section C discusses some of the key conceptual and practical differences between digital risks and more conventional E&S risks, in order to highlight why new policies and approaches to risk management are needed for digital projects. Chapter II analyses the state of play concerning DFI management of digital risks, including strategies, E&S safeguards and other operational policies and legal provisions, as well as other digital initiatives and tools. Chapter II also contains an analysis of digital risk management in the portfolios of nine leading MDBs in four sectors (public administration, finance, health and ICT), identifying gaps in current policies and practices. Chapter III draws together several conclusions and offers recommendations for the consideration of DFIs.

[31] See, for example, Massachusetts Institute of Technology, AI Blindspot; and White & Case, AI Watch: Global Regulatory Tracker.

[32] Danish Institute for Human Rights, *Fit for Purpose? An Analysis of Development Finance Institutions' Management of Human Rights Risks in Intermediated Finance* (Copenhagen, 2024).

B. DIGITAL OPPORTUNITIES AND RISKS IN DEVELOPMENT FINANCE INSTITUTION PORTFOLIOS

The potential benefits of digitalization are widely acknowledged. The coronavirus disease (COVID-19) pandemic was responsible for dramatically increasing demand for digital solutions worldwide, especially in developing countries, prompting a spike in demand for international support, knowledge-sharing and collaboration. Advances in digital technology, including in connection with AI, accompanied by evolutions in 5G and 6G cellular technology, robotics, the Internet of Things and cloud computing, all point to ever-increasing digitalization.[33]

Digital technology is sometimes assumed to be a “magic bullet”. However, while technology is moving at “warp speed”[34] in some countries, there remains a significant digital divide, with approximately 2.6 billion people still offline in 2024, mostly in developing countries.[35] The urban-rural gap in Internet access has barely decreased in the last several years, despite an overall increase in Internet access.[36] In 2022, mobile broadband coverage of 3G or higher was available to 95 per cent of the global population.[37] However, in 2024, 5G coverage was available only to 51 per cent.[38] Even with connectivity, Internet shutdowns and other unwarranted restrictions can undermine access.[39] Smartphones are a key enabler of access to information and services, but they remain unaffordable for many people, especially in low- and middle-income countries.[40] Data on digital skills remain scant[41] and a lack of adequate electricity to run digital devices can present an even more fundamental obstacle in many contexts. Given the slow progress towards achieving SDG Target 9.c,[42] the Secretary-General’s Roadmap for Digital Cooperation ambitiously calls for every person to have safe and affordable access to the Internet, including meaningful use of digitally enabled services, by 2030.[43] This message is re-emphasized in the Global Digital Compact.

The transformative opportunities presented by digitalization, and the continuing gaps, invite important roles for DFIs.[44] These institutions are increasingly financing an enormous range of digital transformations across a wide range of projects, programmes, advisory services and initiatives. The scale of DFI activities in this field was accelerated considerably by the COVID-19 pandemic. DFI digital strategies, where they exist (see subsection 1), foreshadow further expansion in the types and volume of digital projects from these institutions. Digitalization has become a central theme in the work of many DFIs. For example, the World Bank has noted that “the digital revolution holds the single most transformative potential for reshaping

[33] OECD, *Development Co-operation Report 2021*, p. 29.

[34] United Nations, “UN calls for closing Internet connectivity and digital governance gap”, 9 October 2023.

[35] International Telecommunication Union, “Facts and Figures 2024: Internet use”.

[36] International Telecommunication Union, “Facts and Figures 2024: Internet use in urban and rural areas”.

[37] United Nations, *The Sustainable Development Goals Report: Special Edition* (New York, 2023), p. 31.

[38] International Telecommunication Union, “Facts and Figures 2024: Mobile network coverage”.

[39] See *Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights* (A/HRC/50/55), particularly paras. 40–43, also noting that “priority countries for international connectivity assistance are often the same ones that resort to shutdowns.

[40] A4AI, “The cost of smartphones falls, but they remain unaffordable for billions around the world”, 31 August 2022.

[41] International Telecommunication Union, “Facts and Figures 2024: ICT skills”.

[42] SDG Target 9.c: “Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020.” “Significantly increase” is a non-specific target and “strive to provide” is an obligation of means, not of result.

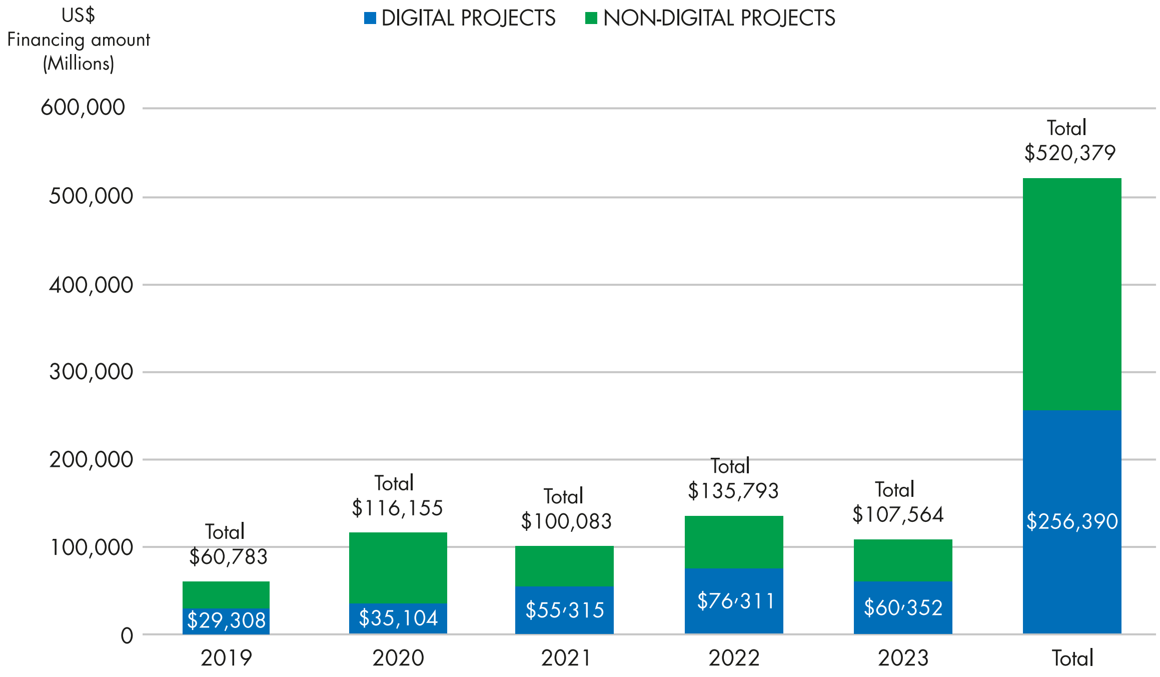
[43] See *Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation, Report of the Secretary-General* (A/74/821).

[44] See, for example, “Principles for Digital Development”.

development”[45] and has made “advancing digitalization” one of the eight global challenges it will focus on as part of its new overall strategy.[46] EBRD has stated that it “puts digital at the heart of its activities across its regions: investments, policy and advisory services.”[47]

Research undertaken for this report examined the project portfolios of nine major MDBs in four key sectors over a five-year period ending in November 2023 (see annex II for information on methodology). A total of 3,450 projects with significant digital components and a combined value of $256.4 billion were identified. The figures for 2023 did not cover the full year, only 10 or 11 months. The value of the digital portfolios of the MDBs across all sectors (beyond the four selected for the present report) is of course much higher. European Investment Bank (EIB) projects were excluded from the analysis used to calculate the figures presented in the graphics of this report (but otherwise captured in the rest of the report) because of several challenges in their datasets: (a) a lack of a standardized E&S categorization, as EIB primarily refers to European Union environmental impact assessment directives, making comparison with other DFIs difficult; (b) incomplete total estimated amount data, requiring manual extraction from individual project websites; and (c) inconsistent reporting of financing types, necessitating interpretation and manual completion.

FIGURE I
VALUE OF DIGITAL AND NON-DIGITAL PROJECTS FINANCED, 2019–2023



[45] World Bank, “The knowledge compact for action: transforming ideas into development impact – For a world free of poverty on a livable planet” (2024), p. 2. See also Axel Van Trotsenburg, “The digital era for all”, World Bank Blogs, 29 February 2024.

[46] World Bank, “Ending poverty on a livable planet: report to governors on World Bank evolution” (2023), p. 9.

[47] See EBRD, “Digitalisation”.

FIGURE II

NUMBER OF DIGITAL PROJECTS APPROVED, 2019–2023

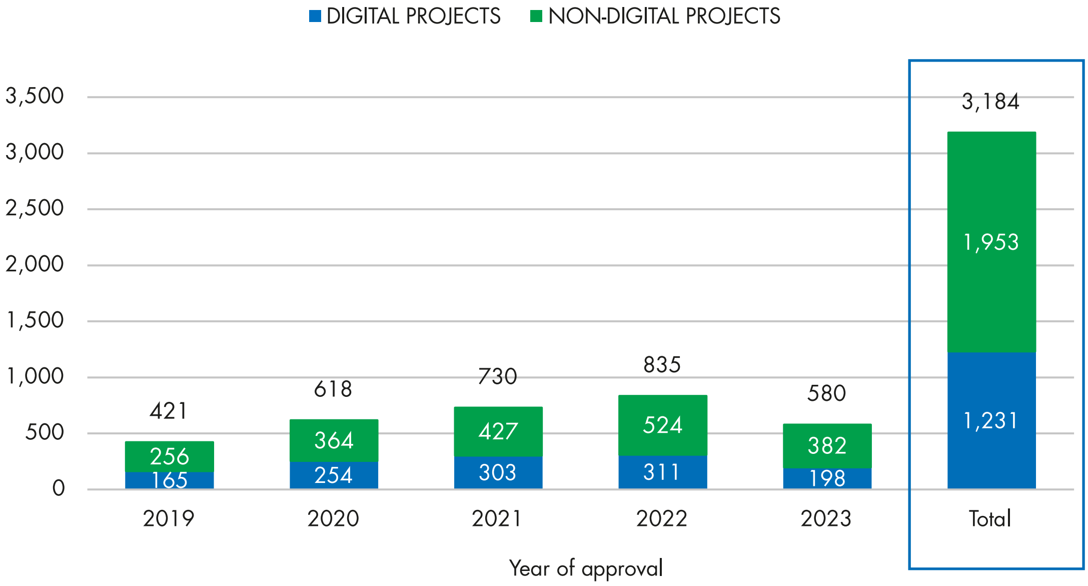


FIGURE III

NUMBER OF PUBLIC SECTOR DIGITAL PROJECTS BY TYPE OF PROJECT FINANCING, 2019–2023

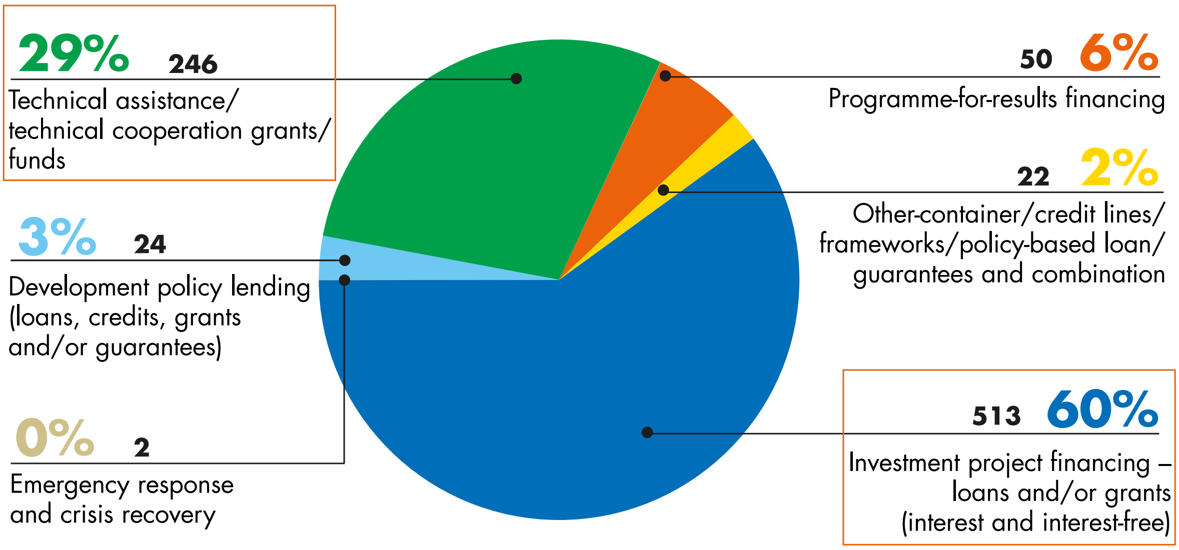
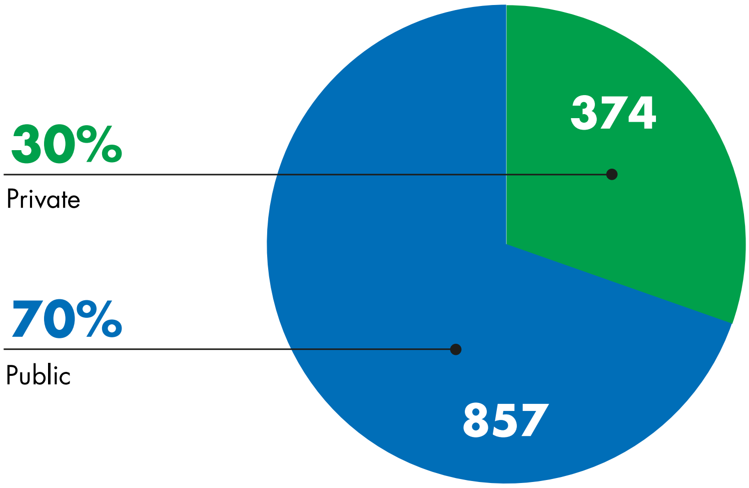


FIGURE IV
NUMBER OF DIGITAL PROJECTS BY TYPE OF RECIPIENT, 2019–2023



The growing volume of DFI-financed digital projects raises pressing questions as to how digital risks are managed. Awareness of the risks of digitalization has been increasing in recent years, against a tide of techno-optimism. The OECD, for example, has described digitalization as a "double-edged sword"[48] and, in its primer on digital risks produced in 2023, the ADB reaffirmed the potential transformative benefits of digitalization while noting that "the greater the digital transformation, the greater the associated digital risks".[49] Even the most upbeat predictions related to the digital revolution have been tempered by the recognition that constant vigilance is necessary at multiple levels to ensure that digitalization supports and does not undermine human rights and freedoms.[50]

Digital technologies connect, enabling rich new experiences and relationships, giving new voice and agency to many, but they can also divide, replicating discriminatory legislation or practices, exacerbating political, economic and social grievances, polarizing public debate and negatively affecting access to information, inciting violence and potentially eroding democracy. The same digital technologies that enable freedoms and opportunities may also enable digital repression and "digital authoritarianism" through means such as illegal surveillance, censorship, technology-facilitated gender-based violence, criminalization of freedom of expression and the imposition of Internet shutdowns.[51] Digital technologies can open vast new avenues for inclusion, but can just as easily lead to exclusion, discrimination and fomenting of hatred against minorities, women[52] and other population groups. E-commerce opens vast new opportunities for micro and small and medium-sized enterprises (MSMEs), but it can also entrench unfair, deceptive and abusive practices. Digitalization is creating new jobs while eliminating a range of others. Gig-economy models create flexible job opportunities but may

[48] OECD, *Development Co-operation Report 2021*, p. 8.

[49] ADB, *Managing Digital Risk: A Primer*, p. 43.

[50] See, for example, Seb Butcher, "2024 may be the year online disinformation finally gets the better of us", Politico (25 May 2024); Adrian Shahbaz and others, "Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet", Freedom House; and Access Now for the #KeepItOn coalition, "The Return of Digital Authoritarianism: Internet Shutdowns in 2021" (2022).

[51] OECD, *Development Co-operation Report 2021*, pp. 108 and 119.

[52] See United Nations Population Fund, *Technology-facilitated Gender-based Violence: Making All Spaces Safe* (2021); and *Right to privacy, Report of the Special Rapporteur on the right to privacy* (A/HRC/40/63).

undermine labour rights through precarious working conditions, uncertain hours, poor pay, exposure to violent content without mental health support and involuntary overtime.[53]

This report is concerned with all such risks of digitalization, in line with the mandates and roles of DFIs in financing and providing advisory services for projects involving such risks. This report uses the term "digital risk" to refer to potential adverse impacts on people and the environment associated with the design, use and regulation of digital projects, products and services, taking the international human rights framework as the basis for its analysis (see box 1 on definitions). The right to privacy is an internationally recognized human right that has an important function in human rights protection in the data economy, and it is vital for building and maintaining trust in the digital environment.[54] Data protection[55] and cybersecurity play critical roles in protecting the right to privacy and are increasingly reflected in DFI policies and risk management practices (although, as discussed further on, data protection and cybersecurity are often managed as commercial risks to a business or government service, rather than risks created by a business or government service to stakeholders). Some DFIs are paying additional attention to the risks of exclusion. However, as outlined in box 1, there are many other human rights risks in the digital sphere that are less clearly reflected in current DFI policy and practice, but which are equally as significant and important for these institutions and their clients to identify and address.

This report does not attempt to identify *a priori*, in categorical terms, a specific list of rights or corresponding risks particularly relevant to the design, development or deployment of digital products and services that DFIs and their clients should consider, nor is it proposed that these institutions adopt such an approach.[56] The main reason to avoid prescriptiveness in this context is that risks depend on design, development and deployment for specific end uses: as technologies and data uses morph and multiply across an ever-widening scope of activity, so too do the risks. The management of digital technology development, with its high-speed and unpredictable trajectory, is among the greatest challenges for regulators and other stakeholders.[57] A risk-based approach, taking into account the recommendations in this report, can help DFIs and their clients to more effectively and proactively identify and manage digital risks in the context of their operations. Relying unduly on project proponents to identify risks not only seems to be inconsistent with the way DFIs handle other areas of

[53] See Business & Human Rights Resource Centre, "Gig Economy".

[54] Deutsches Institut für Menschenrechte (German Institute of Human Rights), "Business & human rights in the data economy: a mapping and research study" (2020).

[55] Privacy International provides a simple explanation of the relationship between privacy and data protection: "Data protection is about safeguarding our fundamental right to privacy by regulating the processing of personal data: providing the individual with rights over their data, and setting up systems of accountability and clear obligations for those who control or undertake the processing of the data" – see Privacy International, Data Protection Guide and "A Guide for Policy Engagement on Data Protection – Part 1: Data Protection Explained" (2018), p. 12. The key protections that should be provided to protect personal data are detailed on page 15. The General Data Protection Regulation includes a set of key data protection principles that are at the heart of its increasingly globalized general data protection regime. Data protection is increasingly recognized as a right in itself, for example, under article 8 of the Charter of Fundamental Rights of the European Union and in an increasing number of national constitutions, alongside the right to privacy – see Privacy International, "A Guide for Policy Engagement on Data Protection – Part 1: Data Protection Explained", p. 13.

[56] As discussed further in the chapter on recommendations, a digital performance standard could and should identify some digital risks that should always be assessed, but should not limit the list of risks to be assessed.

[57] See, for example, the MIT AI Risk Repository, where over 700 potential risks advanced artificial intelligence systems could pose that would not have existed five years ago are documented. It is also noted that "the database also shows that the majority of risks from AI are identified only after a model becomes accessible to the public. Just 10% of the risks studied were spotted before deployment." Also see Scott Mulligan, "A new public database lists all the ways AI could go wrong", *MIT Technology Review*, 14 August 2024.

risk exposure, given clients' potential conflicts of interest, it also seems imprudent, in the view of OHCHR, given how rapidly digital technologies and associated risks are evolving. In such circumstances, there is a strong case for DFIs to develop their own internal expertise supported by an enabling policy framework, relevant guidance and resources.

Box 1 Definition and examples of digital risk

This report uses the term **"digital risks"** to mean potential adverse impacts on people and the environment associated with the design, development and deployment of digital products and services. Examples of digital risks are listed below, linking to many internationally recognized human rights. They also link to many other areas of work that DFIs focus on, such as in relation to gender, Indigenous Peoples and minorities, persons with disabilities, the rule of law, justice reform and security sector reform. This underscores the importance of taking a broad look at digital risks within digital projects and within a wide range of projects integrating digital technologies. A limited focus on data protection and cybersecurity is not sufficient.

Whether any such risks will materialize in any given project depends on such factors as the proposed operations, the operating context and the actors involved. Context can be critical: DFIs need to be careful that they are not unwittingly facilitating or playing a role in connection with the worst abuses in challenging, fragile or conflict-affected contexts.[58] Those involved in abuses may include project proponents (public or private), knowingly or unknowingly, along with other actors interacting with the digital products and services being financed, such as domestic or foreign Governments, technology companies, individuals, groups or criminal actors seeking to perpetuate harms through digital means.

Some of the risks discussed below are often thought of and managed as commercial risks by businesses or as operational risks by DFIs. They are highlighted in this box to underscore that they are not just commercial or operational risks to the business or financing institution but also risks to people, and should be managed accordingly.

- **Privacy risks**,[59] for example, through excessive or unnecessary data collection or retention; data use or misuse for purposes other than the designated use ("mission creep"), including government and private sector surveillance, profiling and discrimination; the lack of meaningful consent and the lack of transparency on data handling principles and practices; practices in making access to services conditional on the provision of personal data beyond what is strictly necessary; and the loss of control over data and privacy on cross-border data transfers.
- **Exclusion risks**, for example, through constraints on access to the Internet, mobile phones or banking services, thereby exacerbating inequalities; the exclusion of individuals whose biometric data are not easily captured or verified from accessing services such as social protection or healthcare; and the prioritization of urban areas or other specific demographics that widens digital divides.

[58] For example, repressive surveillance in authoritarian regimes or in conflict settings, including surveillance leading to arrest, detention, targeted killings and other forms of violence.

[59] Privacy risk includes potential impacts of data processing on individuals' dignity (embarrassment or stigma) as well as more direct harms such as discrimination, economic loss or physical harm. National Institute of Standards and Technology, "NIST privacy framework: a tool for improving privacy through enterprise risk management" (2020). See also *Legal standards for personal data protection and privacy in the digital age, report of the Special Rapporteur on the right to privacy* (A/HRC/55/46).

- **Bias and discrimination risks**, for example, through algorithms and automated decision and/or biased profiling; the under-representation of women or other key population groups in technology design, which may have discriminatory or inequality-enhancing impacts; and gendered stereotyping that portrays women as weak, incompetent and sexualized objects, incapable of leadership.
- **Freedom of expression and freedom of association risks**, for example, through content filtering or the regulation of content in ways that do not comply with the criteria for restricting expression and information; censorship or other undue constraints on access to information, including through Internet shutdowns; weak regulatory protection of the right to freedom of expression; restrictions on civic space; surveillance of human rights defenders or political opponents; and intimidation of the general population.
- **Increased risk of statelessness**, for example, when the shift to digital ID systems amplifies the exclusion of vulnerable groups, including stateless persons, and entrenches their exclusion from any form of recognized identification or access to services; and through arbitrary denial of recognition of nationality as part of the digitalization process.[60]
- **Safety risks**, for example, through online incitement to violence, online threats, cyberbullying, harassment and hate speech, access by children to harmful content and the promotion of violence including technology-facilitated gender-based violence.[61]
- **Data security risks**, for example, which undermine the right to privacy; unauthorized disclosure of biometric data and other sensitive personal data; identity theft; biometric data theft, which may be impossible to correct because of the nearly immutable character of biometric characteristics; warrantless search or surveillance, including politically motivated surveillance; data breaches that lead to the exposure of sensitive personal data and/or financial loss; and cybersecurity attacks that may disrupt services provided by Governments and businesses and impede access to vital services.
- **Data accuracy risks** with adverse human rights or social implications, for example, where inaccurate health or education data lead to incorrect assessments and unfairly block access to services (generalization errors).
- **Risks to dignity, physical and psychological well-being**, for example, when online threats and harassment, including through generative AI model outputs, cause harm to individuals' mental and physical health; and through the online identification and targeting of people to be harassed and attacked.
- **Environmental risks**, for example, those associated with the high energy and water consumption of data centres;[62] the contribution to greenhouse gas emissions of e-waste; e-commerce-related impacts including waste created by packages; greenhouse gas emissions from last-mile delivery and returns; and the environmental degradation and high carbon footprint of the cryptocurrency mining process.

[60] See José Maria Arraiza, "Will digital ID help stateless people? The threat of digital administrative violence", European Network of Statelessness, 23 November 2023; and Privacy International, "Digital national ID systems: ways, shapes and forms", 26 October 2021.

[61] See UN Women Asia and the Pacific, "FAQs: Trolling, stalking, doxing and other forms of violence against women", 10 February 2025.

[62] Steven Gonzalez Monserrate, "The cloud is material: on the environmental impacts of computation and data storage", *MIT Case Studies in Social and Ethical Responsibilities of Computing* (January 2022).

- **Accountability risks**, for example, through the opaqueness and lack of explainability of many digital systems, particularly AI models, which can hinder the transparency needed to ensure accountability and access to remedy; through inadequate mechanisms for remedy in cases where human rights are violated through the use or misuse of digital technologies; the diffusion of responsibilities through the digital project value chain;[63] and challenges related to designing appropriate grievance mechanisms and remediation measures.[64]
- **Risks of exacerbating vulnerability and marginalization.** People at particular risk in any context may include women, racialized communities, ethnic, religious or linguistic minorities, migrants, stateless persons, people living in poverty, persons with disabilities, older persons, environmental and human rights defenders, people discriminated against on the grounds of political opinion and lesbian, gay, bisexual, transgender and intersex (LGBTI) persons. Such population groups may be at risk of marginalization or vulnerability through specific targeting as well as through many of the actions identified above. People may also be further marginalized through skills gaps or an inability to adapt to or benefit from digital advancements, thereby deepening inequalities. For example, "gig" workers frequently lack job security and traditional employment benefits.

While awareness of digital risks has undoubtedly been rising, it is still often assumed, uncritically, that digital is always the best option. "Technology solutionism",[65] the assumption that development challenges can best be solved through (more) technology and "leapfrogging",[66] seems to have permeated many first-generation DFI digital strategies, leading to the uncritical promotion of digital solutions as the default, without sufficient attention to accompanying digital risks or opportunity costs (see box 2)[67] or, frequently, a clear and compelling theory of change.[68] Such an approach is obviously problematic. An uncritical default to digitalization may effectively foreclose the consideration of alternatives. For example, while a digital health project may sound appealing, context is everything: in a project context characterized by low digital skill levels, limited digital access and inadequate resources to maintain and service digital infrastructure once a DFI's support has ended, health funding may be more wisely spent on lower-technology options, such as improved primary healthcare facilities or supporting

[63] There may be other types of risks associated with the integration of digital components into projects, such as in connection with competition policy, tax or other regulatory issues, but the risks are not within the scope of the term "digital risks" as used in the present report.

[64] OHCHR, B-Tech Project, "Access to remedy and the technology sector: basic concepts and principles" (2021).

[65] The origins of this term, sometimes abbreviated to "tech-solutionism", can be traced to the idea of "technocratic solutionism" in the 1960s, which posits that problems have technocratic solutions even if they are multifaceted, complex and involve conflicts among values, ideas and interests. See Daniel M. Fox, *Engines of Culture: Philanthropy and Art Museums* (New York, Routledge, 1995), p. 2; and Jason Crawford, "Why I'm a proud solutionist", *MIT Technology Review*, 13 July 2021.

[66] Leapfrogging in this sense means "bypassing intermediate stages of technology through which countries have historically passed during the development process" – see United Nations Conference on Trade and Development, "Leapfrogging: look before you leap", Policy brief No. 71 (2018). See also Boutheina Guermazi, "Watching Tanzania leapfrog the digital divide", World Bank Blogs (9 November 2016); and BII, *Productive, Sustainable and Inclusive Investment 2022–26 Technical Strategy* (2021), p. 12.

[67] See also box 22 on a digital health project in Tonga; and IDB, "Research insights: How to identify affordable high-impact digital solutions for public services?" (2023). In the latter paper, various cost-benefit case studies are considered, but apparently without costing in the risks to stakeholders. While the Bank has developed useful tools for analysing costs for digital solutions for the health sector, its "total cost" approach does not appear to address costs to stakeholders or potential costs to the institution arising from situations where data is misused or leaked. See IDB, "Beyond the price tag: understanding the true cost of digital health tools" (2023). It would be useful if costs for stakeholders were incorporated more systematically into the research of DFIs on digital issues.

[68] Project descriptions are not always clear on how broadly defined project objectives are to be achieved, the actors involved or the methods and specificities of the technologies to be deployed. Victoria Adelmant and others, *Digitalization as Development: Rethinking the IFC's Risk Assessment and Remedy Frameworks in the Context of Digital Technologies* (New York, International Organizations Clinic, 2025), p. 12.

© Adobe Stock/Generative AI/ by ai tekno koncept

more community health outreach. Similarly, proposals to invest in data centres or other power-intensive infrastructure must be considered against climate and biodiversity impacts and competing energy and water needs in the host country.[69]

The underlying theories of change regarding the link between digital transformation and development outcomes must be made more robust. Implementing a digital system is not an end in itself – digital technologies should be supported when and where they can be shown to contribute to better human rights and development outcomes, not just because they are novel. In-depth *ex ante* analysis is needed in order to determine the best option in any specific context, supported by empirical evidence of the problem to be solved, without automatically tipping the scales in favour of digitalization.[70] It also requires not only consideration of the risks of adverse impacts on people,[71] particularly those that will be most affected, but also the distribution of risks across different stakeholder groups, based on meaningful stakeholder consultation from the earliest stage.

[69] Alexis Laurent and others, "Environmental sustainability of data centres: a need for a multi-impact and life cycle approach", Copenhagen Centre on Energy Efficiency Issue Brief No. 1 (2020); and Anastasia Balova and Nicholas Kolbas, "Biodiversity and data centers: what's the connection?", Ramboll, 20 August 2023.

[70] New York University School of Law, International Organizations Clinic, "Submission for the Review and Update of the ADB Safeguard Policy Statement" (April 2022): "Annex, Digital Risk Case Study – Tonga: eGovernment through Digital Health", on file with OHCHR; and Victoria Adelmant and others, *Digitalization as Development: Rethinking the IFC's Risk Assessment and Remedy Frameworks in the Context of Digital Technologies*, April 2025.

[71] Development Bank of Austria (OeEB) and DEG, *Explorative Research Study on Approaching DFI's Development Impacts from a Net Perspective* (2022).

Box 2 Case study – Is digitalization the best choice?

A **knowledge paper** published by the **EBRD** Evaluation Department in 2023, focused on the digitalization components of the **Kafr El-Sheikh Wastewater Project in Egypt**, was aimed at extracting lessons from the organization's experience with digitalization.[72] The project, co-financed by EBRD and EIB, was aimed at expanding wastewater treatment.

The project included two key digitalization components: the implementation of digital supervisory control and data acquisition (SCADA) systems for the plants and the development of a mobile application for customers. Significant risks to the sustainability of these digitalization efforts, which stakeholders had identified in advance, were highlighted as part of the analysis.[73] In the paper, it was noted that as a result of capacity constraints relating to the implementing partner and organizational preferences for analogue systems, there was a strong likelihood that the digital systems in question would not be utilized in the long run.

Concerns about job losses and stranded skills further reinforced the preference expressed by stakeholders for analogue rather than digital systems, while the need for a reliable power source and Internet connectivity for data transfer and remote monitoring presented significant operational challenges in the remote, rural regions where the plants are located. Ongoing maintenance costs associated with digitalization, whether through external service providers or software subscription services, also imposed financial burdens that were not adequately considered during project planning.

Digital risks can be both severe and systemic. For example, DFIs are increasingly funding broad, system-level projects that extend across sectors, such as digitalization of public administration or supporting DPI roll-out. This requires a new way of addressing risks, because looking purely on a project level will not match the systemic level impacts that these infrastructures are intended to have on society. Because of their breadth, system-based projects give the public sector (and private sector vendors supplying the technologies) wide discretion about how the project will be implemented as well as how much information about the effects of digitalization will be disclosed to the public. The technologies themselves are often opaque in terms of the type of data that is collected and how collection is done, how data is processed and analysed, how it will be put to use, who it may be shared with and who will have access. Most impacts will not be obvious, even to the well informed. The lack of technical details is not only a "technical" problem, it fundamentally affects the human rights impact of the system in question. Such projects by their nature fundamentally alter the relationship between the State and the public, and in doing so, may exert systemic and enduring impacts well beyond the effects of the digitization of discrete administrative functions.[74] The project proponent and the DFI should be required to make a convincing case to answer the question: "is it necessary and proportionate, or could a less intrusive system be used?"

[72] EBRD, "Understanding Digitalisation: Case Study of the Kafr El-Sheikh Wastewater Expansion Project" (2023).

[73] Ibid., p. 11.

[74] Victoria Adelmant and others, *Digitalization as Development*, pp. 9–11.

It is not only public sector activity that creates digital risks. Many DFIs have significant portfolios of private sector projects in which digital risks may be embedded. Risk factors include insufficient data protection, cybercrime,[75] the deployment of business models built on biased data sets or on data extraction, re-use and re-sale (including potentially to law enforcement or intelligence agencies) without adequate safeguards or consent, monetization of manipulative or addictive user services,[76] the use of algorithmic systems that manufacture virality and fuel social conflict, short-term rental platforms that lead to higher rental prices and reduced housing stock for low-income residents,[77] the development or deployment of intrusive facial recognition technologies, illegal profiling, inappropriate content moderation, failure to protect cybertheft of data, the sale of surveillance tools that violate the right to privacy,[78] and the ever-increasing demand and exploitation of data to train AI systems.

The extent of DFI exposure to these risks is difficult to assess, given the variable disclosure practices across multilateral and bilateral DFIs on how digital risks are addressed. While data protection, cybersecurity and exclusion risks are increasingly being addressed at the project level, at the time of writing, insufficient attention was being given to many other digital risks.[79] A more detailed empirical analysis of this question is provided in section B of chapter II, although the analysis is neither comprehensive nor, in many respects, definitive. As such, this would seem an apt time for a greater focus on more comprehensive stocktaking, as suggested in chapter III, and evaluation by independent evaluation departments of MDBs, in the view of OHCHR.[80]

It is recognized that digital risks can be managed according to a particular risk appetite but not always eliminated. In the view of OHCHR, the manner and processes through which DFIs and their clients determine their project risk appetites, and the manner in which any trade-offs between project goals and individual rights are addressed, should be transparent, participatory and subject to public justification and appropriate prevention, mitigation or remedial measures. The recommendations detailed in chapter III are intended to contribute to such a decision-making framework and, thereby, minimize digital risk exposure for DFIs and their clients, and most critically, project-affected populations.

[75] According to IT Governance, over 8 billion data breaches and cyberattacks were recorded in 2023 (IT Governance, "List of Data Breaches and Cyber Attacks in 2023 – 8,214,886,660 Records Breached", 5 January 2024). Many other breaches are likely unreported. According to estimates from Statista's Market Insights, the global cost of cybercrime is expected to surge in the coming years, from $9.22 trillion in 2024 to $13.82 trillion by 2028. See Anna Fleck, "Cybercrime expected to skyrocket in coming years", Statista, 22 February 2024.

[76] See OHCHR, B-Tech Project, "Addressing business model related human rights risks" (2020); OECD, "Six 'dark patterns' used to manipulate you when shopping online", 16 September 2024; and, OECD, *Dark Commercial Patterns* (2022).

[77] OHCHR, B-Tech Project, "Addressing business model related human rights risks".

[78] Geneva Centre for Security Sector Governance and Privacy International, "Understanding private surveillance providers and technologies" (2024).

[79] See, for example, ADB, *Managing Digital Risks: A Primer*.

[80] In 2021, the World Bank Group Evaluation Department conducted a 2022 assessment of the institution's preparedness for digital development: *Mobilizing Technology for Development: An Assessment of World Bank Group Preparedness* (2021). Not all DFIs make their evaluations publicly accessible (AIIB) or searchable (IDB, EIB). However, none of the independent evaluation departments of these institutions, as yet, appears to have carried out a broadly scoped evaluation of their parent institution's digital activities.

C. HOW DIGITAL RISKS DIFFER FROM TRADITIONAL ENVIRONMENTAL AND SOCIAL RISKS

E&S risk management is a central feature of DFI operations and a prerequisite for project quality and sustainability. For the most part, since the 1980s, E&S risk management in DFI-financed operations has focused on a particular set of E&S risks associated with traditional investment projects with a relatively well-defined physical footprint. Examples include resettlement, health and safety concerns, Indigenous Peoples' rights and pollution and other environmental impacts. E&S safeguards have been adapted in important ways in line with the evolving nature and scope of DFI-supported project risks, while still bearing the imprint of their origins. However, digital risks[81] and impacts are different from more traditional E&S impacts in various important ways. The nature of these differences, and the changes required to manage these differences, implies the need for a generational change in DFI risk management approaches, in the view of OHCHR. E&S safeguards should help clients to address digital risks, in line with the United Nations Guiding Principles on Business and Human Rights and other international human rights standards, and to navigate a changing regulatory landscape.

Adverse impacts from the use of digital technologies can:

- **Be far more pervasive in scope** than the impacts of even the largest physical footprint projects because of the potential number of users. Some digital products and services can be used by millions, if not billions of people. For example, e-government projects may impact the population of an entire country. Where there are errors in e-government services, people may be cut off from critical services and may be without redress, because of the opacity of the tools used for decision-making and the lack of effective accountability mechanisms.[82] This may be the case even in countries with relatively sophisticated technological and regulatory capacities.[83]
- **Amplify inequalities**, for example, from artificial datasets reproducing preexisting discrimination against particular population groups (particularly those already vulnerable or marginalized), or where access to technology infrastructure is limited by geography, literacy, health or other socioeconomic factors.
- **Spread easily and quickly**, because digitalization, owing to its scalability, permits more effective proliferation of harms. Systems can replicate any error or bias introduced at any level on a wider scale and at greater speed, exacerbating harms and inequalities.[84] AI is

[81] The term "digital risks," for the purposes of this report, is defined in box 1. Risks and impacts that may contravene internationally recognized human rights is a primary focus of the present report.

[82] On public administration systems generating false accusations of fraud, with severe and pervasive consequences, see *Report of the Special rapporteur on extreme poverty and human rights, Digital welfare states and human rights* (A/74/493); and Georgia van Toorn et others, "Introduction to the digital welfare state: contestations, considerations and entanglements", *Journal of Sociology*, vol. 60, No. 3 (September 2024), pp. 507–522.

[83] See, for example, A/74/493; BBC, "The Post Office scandal: Why hundreds were wrongly prosecuted", 30 July 2024; Adamantia Rachovitsa and Niclas Johann, "The human rights implications of the use of AI in the digital welfare state: lessons learned from the Dutch *SyRI* case", *Human Rights Law Review*, vol. 22, No. 2 (June 2022); and Melissa Heikkilä, "Dutch scandal serves as a warning for Europe over risks of using algorithms", *Politico* (29 March 2022). The use of the algorithm described in the *Politico* article resulted in several suicides and more than a thousand children were taken into foster care, indicating the type of irremediable impacts such technology can have. The Government of Denmark has also faced criticism for discriminatory impacts from the use of fraud-control algorithms in social programme – see Amnesty International, *Coded Injustice: Surveillance and Discrimination in Denmark's Automated Welfare State* (2024).

[84] See, for example, Eliza Strickland, "Racial bias found in algorithms that determine health care for millions of patients", IEEE Spectrum, 24 October 2019.

© Adobe Stock/by Delcio/peopleimages.com

expected to supercharge impacts, negative and positive, and may act as an "amplifier of digital repression".[85]

- **Introduce novel harms** that are not possible with physical impacts, such as through the recombination of information.
- **Be magnified easily**, in terms of the scale, scope and irremediability of the impacts. Impacts can easily be repeated over and over again, such as where unauthorized images are viewed repeatedly, compounding the harm caused. Threats and incitement online can lead to real-world consequences, such as violence, harassment and intimidation. Digital technologies may also be used to target people at a population level to predict population movements, which could lead to harms.
- **Exist perpetually, with more long-lasting effects.** Certain impacts from traditional (or physical) projects may also be irreparable and permanent in nature, for example, in the context of harms from gender-based violence, or where resettlement results in lasting impoverishment, or where cultural heritage is irretrievably lost. But many more types of digital harms remain in perpetuity, given the nature of digital storage. Collection of biometric data remains, even long after collection methods or uses may have changed. DFIs are also supporting Governments in rolling out digital infrastructure that may operate for decades. For example, large-scale e-government projects are typically intended to operate over long-time scales in order to justify the costs. The push for a "right to be forgotten"[86] assumes particular salience in view of the longevity of digital information.

[85] Allie Funk and others, "Freedom on the Net 2023: The Repressive Power of Artificial Intelligence", Freedom House, 2023; Airlie Hilliard, "An Exploration of AI Harms: the Need for AI Risk Management", Holistic AI, 21 August 2023; and Privacy International, "Examples of algorithmic management abuses".

[86] Michael J. Kelly and David Satola, "The right to be forgotten", *University of Illinois Law Review*, vol. 1 (May 2017), pp. 1–65.

- **Be more ephemeral than physical approaches.** In contrast to the problem of the perpetuity of harms, data uses may also create concerns through facilitating the disappearance of vital information. Among the advantages of digital technologies, compared with paper-based records, is that the former are less vulnerable to wear and tear and destruction. However, digital technologies can suffer their own types of disappearances, affecting whole categories of records. For example, a blockchain-based digital identity solution could become unreadable if a service provider goes bankrupt or records are destroyed though the corruption of files.
- **Be far more prevalent** because harms can occur **across each and every function of the data handling cycle**: (a) data generation; (b) processing; (c) storage, and/or; (d) use, reuse or misuse. Errors or misuse at each step are multiplied by the number of persons affected. At each step of the data chain, technical, social, organizational and legal practices will also import particular norms, values and biases. Choices about which data are collected and how certain populations or phenomena are represented in data can lead to a range of risks, reinforce discrimination, exacerbate inequalities and render particular populations or activities invisible because no data are collected about them, while other population groups may be overrepresented in other types of data sets.[87]
- **Very often be invisible to those affected** because the processes are technical, opaque, complex and interlinked and often buried in coding language that even experts may be unable to decipher. For example, while repeated attention has been drawn to biases in automated decision-making and AI, actually understanding the origins of bias and impacts on decision-making can be very complex and may not be apparent even to sophisticated users or the data subject.[88] Even some of the better-known or routine digital risks, such as risks to privacy, may be difficult for many stakeholders to grasp without technical knowledge or guidance. Opacity may also result from a lack of access to information and the invocation of exceptions to disclosure on unjustifiably broad national security or commercial confidentiality grounds. Moreover, choices made today about how digital infrastructure systems are configured may result in potentially unrestricted Government or private sector access to personal data for the duration of the infrastructure, without the knowledge or consent of users or the prospect of redress. This contrasts sharply with the immediate and obvious nature of many impacts from physical projects. The invisibility of impacts does not justify ignoring these risks – on the contrary, it makes it all the more important that risks and corresponding prevention and mitigation measures are transparently disclosed.
- **Be out of the control of the individual as the owner of their data.** For example, a paper vaccination booklet may be kept by its owner who may show it to who they want, keep it from who they want and destroy it if necessary. This is not possible with digital systems. Moreover, if somebody's digital identity gets turned off, the person concerned may lose access to services without knowing why. Such incidents may be inadvertent, caused by a technical fault, or may be intentional, as part of an explicit campaign of repression.

[87] Victoria Adelmant and others, *Digitalization as Development*, pp. 9–10.

[88] See Adriano Koshiyama and others, "Towards algorithm auditing: managing legal, ethical and technological risks of AI, ML and associated algorithms", *Royal Society Open Science*, vol. 11, No. 5 (May 2024). See also Algorithm Watch, "New project: auditing algorithms for systemic risks"; and Briana Vecchione and others, "Algorithmic auditing and social justice: lessons learned from the history of audit studies" in *EAAMO '21: Proceedings of the 1st Conference on Equity and Access in Algorithms, Mechanisms, and Optimization* (New York, Association for Computing Machinery, 2021).

- **Be impossible to know unless necessary monitoring and independent oversight are in place.** Without monitoring, the identification of harms may emerge only belatedly or sporadically, making it harder to develop the relevant evidence base about necessary prevention and mitigation measures.
- **Disperse exponentially across affected stakeholders.** Under the current generation of E&S safeguard policies, potentially affected stakeholders are usually identified based on their physical proximity to the project. The dispersed nature of potentially affected stakeholders (potentially across a region, a country or even the globe) makes it far harder for affected stakeholders to communicate, organize and act in concert to address concerns about potential or actual harms, especially where harms affect heterogenous groups. Similarly, a wider and more dispersed range of individuals and communities may be subjected to online threats, harassment or incitement to violence.[89]
- **Defy current approaches to classifying project risks.** Contrary to conventional E&S risk management practices, digital risks are not necessarily proportionate to the size of the project or company. Digital risk exposure may even be inversely correlated to company size: small companies involved in novel innovations may generate asymmetrically large risks and impacts. In addition, while the positive impacts of a technology may be assessed and classified in accordance with the functions that it enables, the negative impacts will usually be far more specific to a company or project, its business model and the context or operating market.[90] Therefore, classifying digital or technology projects on a sectoral basis may also be misleading and ineffective.[91]
- **Be more challenging to assess** against the backdrop of constant, rapid innovation, perpetual access to data and constant development of new data uses.[92] For example, DPI provides infrastructure that public or private actors can use to deploy new products or services. In addition, specific assessments are required in order to capture new risks that may arise from each additional deployment. To take another example, the rapid evolution of techniques of digital repression has been described by the Africa Digital Rights Network as "digital rights whack a mole," wherein "every new generation of technology used by activists to enable freedom of expression is met by multiple government tactics to deny citizens their digital rights".[93] The relevance and salience of a database of facial images has changed significantly in the face of the development of facial recognition technology.
- **Be more unpredictable**, as some digital technologies and services may more easily be reused or redeployed in a way not contemplated when a project was originally conceived. For example, biometrics collected for digital ID purposes may be used for surveillance purposes not originally within the contemplation of the financing organization.[94]

[89] OHCHR, B-Tech Project, "Access to remedy and the technology sector: understanding the perspectives and needs of affected people and groups" (2021), p. 7.

[90] DEG, AfricaGrow and Steward Redqueen, *Responsible Investment in Technology*, sects. 2.2 and 3.2.

[91] Ibid.

[92] Danish Institute for Human Rights, "Development finance for digitalisation: human rights risks in sub-Saharan Africa" (2023), pp. 18–19.

[93] See African Digital Rights Network.

[94] Katja Lindsov Jacobsen, "Biometric data flows and unintended consequences of counterterrorism", *International Review of the Red Cross*, vol. 103, No. 916–917 (April 2021), pp. 619–652.

© Adobe Stock/Generative AI/ by Justlight

- **Be unknown at the time of financing.** For example, where DFIs are financing new business models or new start-ups, as many increasingly are, due diligence may be carried out before the start-up has fully developed or been launched. In such cases, even if the model, product or approach can be explained to the DFI, it will not have been tested, and there may be no evidence of its performance or potential impact at the time of due diligence. This is particularly concerning with respect to the rapid proliferation of AI-driven projects.[95] Staged due diligence may be required for these kinds of projects[96] in order to make sure the DFI is assessing potential impacts at a time when the impact of technologies are clearer, especially if project partners are interested in "moving fast and breaking things".
- **Be more cumulative** than impacts from physical projects, such as in cases where a number of different types of technology and data are pooled, resulting in wider and more complex impacts that are more difficult to anticipate and identify.[97]

[95] Center for Financial Inclusion, *Investing in Equitable AI for Inclusive Finance: A Risk Management Guide for Impact Investors* (2023), p. 5.

[96] In the view of OHCHR, as a matter of policy, any proposal for a phased approach to E&S safeguard implementation should be defined narrowly and carefully and be subjected to a high standard of justification. For example, categorical carve outs for E&S safeguards in conflict settings or for complex operations should be avoided.

[97] Danish Institute for Human Rights, *Guidance on Human Rights Impact Assessment of Digital Activities* (Copenhagen, 2020) – see sect. 1.1.4 on cumulative impacts in "Phase 3: Analysing Impacts".

- **Have more of a "honeypot" effect** than many physical projects. Some physical projects lead to in-migration, attracting people to the project area in search of work or other benefits. Certain types of digital projects, particularly those that gather and pool large amounts of commercially valuable data, may magnify this effect exponentially. Data pools attract not only new uses not contemplated when the data were originally collected by public and private sector entities,[98] but have also been a magnet for data breaches and cybercrime.[99]
- **Be far harder to remedy.** The geographic dispersion of stakeholders, the temporal character of digital impacts, the irremediability of certain digital harms and the challenge of developing appropriate reparations, all present particular challenges to remedy. The remedy ecosystem used to address harms, through judicial, non-judicial and company-led grievance mechanisms, may be weak, fragmented and difficult to navigate.[100] Even in countries with relatively robust regulatory frameworks and judicial systems, such as in the cases of Australia, the Kingdom of the Netherlands and the United Kingdom of Great Britain and Northern Ireland, the road to justice can be a long and difficult one.[101]
- **Entail regulatory challenges**, given the mismatch between the transboundary nature of technology and the jurisdictional boundaries of governance and regulation.[102] In addition to the challenges pertaining to remedy noted above, even more fundamentally, it may be unclear to the DFI and its stakeholders which jurisdiction has responsibility for the effective governance of technology in cases where the DFI-funded project crosses jurisdictions.

[98] For an example of misuse of data across government agencies, see Zack Whittaker, "Australia's spy agencies caught collecting COVID-19 app data", TechCrunch, 24 November 2020.

[99] See, for example, IT Governance, "Global Data Breaches and Cyber Attacks in 2024", 2 May 2024, in which it is noted that "35,900,145,035 known records breached so far in 9,478 publicly disclosed incidents." The statistic is based only on publicly reported incidents over a four-month time frame.

[100] See OHCHR B-Tech project papers on remedy in the technology sector.

[101] For example, in the case of the UK post office scandal, in which more than 900 sub-postmasters were prosecuted for stealing because of incorrect information from the Horizon computer system, it took over 23 years of campaigning and a television drama based on the story to finally exonerate those falsely accused. The scandal has been described as the "UK's most widespread miscarriage of justice." See BBC, "Post Office scandal: why hundreds were wrongly prosecuted", 30 July 2024.

[102] OECD, "Framework for anticipatory governance of emerging technologies", OECD Science, Technology and Industry Policy Papers (Paris, OECD Publishing, 2024).

© Adobe Stock/Generative AI/by Anastasiia

CHAPTER II
STATE OF PLAY IN DEVELOPMENT FINANCE INSTITUTION DIGITAL RISK MANAGEMENT

Having discussed the concept of "digital risk" and explored some of the main differences between digital risks and more conventional E&S risks in DFI-supported projects, chapter II sets out a short overview of some of the main approaches that DFIs have taken to managing digital risks in practice. The analysis encompasses digital strategies, operational policy responses (including a particular focus on the role of E&S safeguard policies), contractual provisions, standard-setting activities and a range of operational tools and capacity-building measures. Chapter II concludes with a discussion of OHCHR analysis and findings from the project databases of nine major MDBs in four key sectors, which provides a foundation for the recommendations presented in chapter III.

A. CURRENT APPROACHES TO MANAGING DIGITAL RISK

DFIs have emerged as influential catalysts and partners in support of digital transformations, providing financing, expertise and knowledge products, and convening actors to address the numerous challenges and trade-offs involved. DFIs are increasingly developing digital strategies (both overarching and sectoral), leading and participating in digital initiatives, developing tools and publishing research. The following subsections provide examples of significant DFI initiatives and thought leadership in this area. The discussion does not purport to be comprehensive, only illustrative, given the breadth of activities involved.

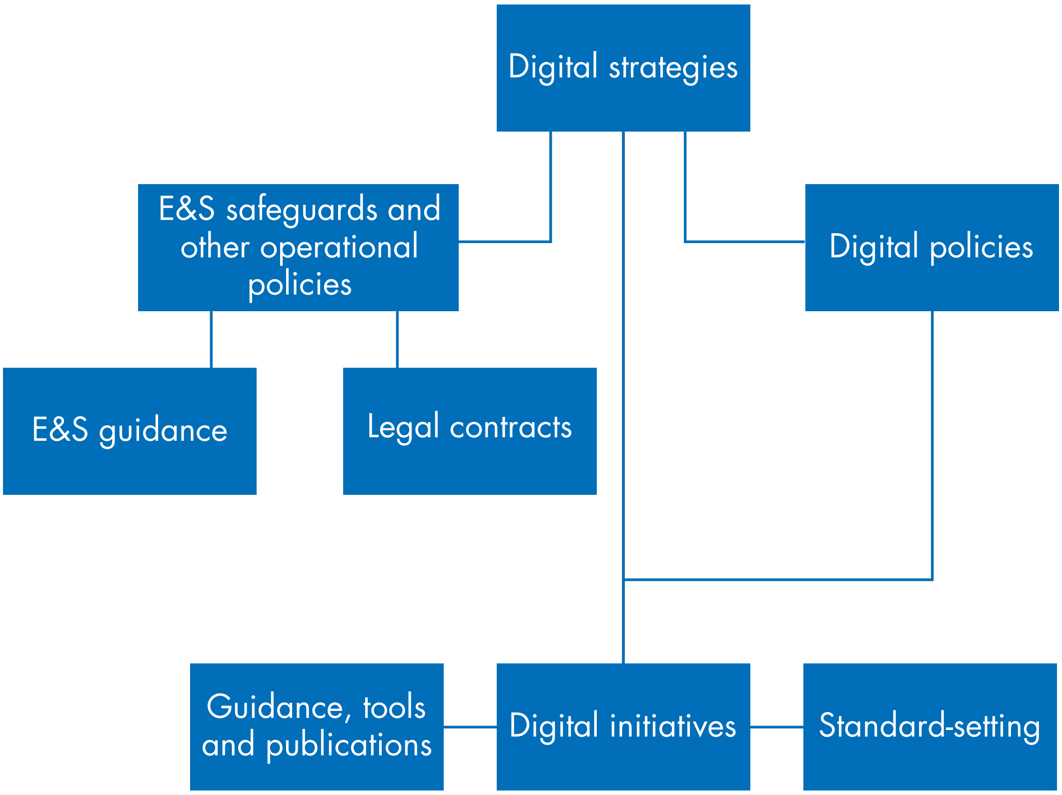
Notwithstanding the growing support by DFIs for digital transformations, it is difficult to understand from publicly available information what digital risk management requirements (if any) apply to projects, including advisory assignments, in order to manage potential and actual adverse impacts on stakeholders.[103] A certain range of digital risks, particularly those pertaining to privacy and data protection issues, are increasingly being addressed by some DFIs on a project-by-project basis through project design, appraisal, supervision and

[103] Advisory services for digital transformations can have very significant and even systemic impacts, especially in the case of regulatory advice. However, advisory work is usually assigned a low- (or no) risk rating, with the consequences that E&S risks are less likely to be identified and managed effectively, and relatively little documentation is disclosed.

implementation support to clients.[104] However, this often occurs outside the framework of the given E&S safeguard policies of DFIs or other publicly disclosed policy frameworks.

The following discussion examines the emerging variety of approaches through which some of the major multilateral and bilateral DFIs have been engaging with and seeking to manage digital risks to date. The analysis is focused on digital strategies, operational policies (including E&S safeguard policies), specialized legal provisions, standard-setting activities and other tools, initiatives and publications. Particularly close attention is paid to E&S safeguard policies, given their central role in E&S risk management and the factors outlined in section A.

FIGURE V
OVERVIEW OF DFI APPROACHES TO MANAGING DIGITAL RISKS



1. DIGITAL STRATEGIES

Strategies help DFI staff, borrowers and other stakeholders understand the rationale, objectives and focus of DFI financing for digital transitions, and signpost the institution's direction of travel. The majority of the DFIs reviewed for this report have digital strategies. The review in box 3 is focused on what, if anything, these strategies say about identifying and managing digital risks. The review highlights that some DFIs take a more balanced approach in their strategies than others, in the sense that digital risks are considered explicitly alongside

[104] For example, the World Bank provides technical support to project teams to help ensure that privacy and data protection risks are integrated in project design (such as through project appraisal documents), project implementation and contractual conditions with the client.

opportunities. However, even among those with more balanced strategies, the list of digital risks considered is often quite limited. The digital risks most frequently highlighted in DFI strategies are data protection, cybersecurity (and the associated need to build trust in the digital ecosystem), concerns about the digital divide, the risk of exclusion from digital goods and services, and digital skill development. Some contain brief references to AI, which can be expected to increase over time as the role of AI grows.[105]

However, numerous other sources of digital risk are less commonly referred to, including unlawful surveillance, abuse or misuse of personal data by Governments or private companies, and Internet shutdowns.[106] Exclusion is mentioned more often, but less so the bias and discrimination that may be driving exclusion. Moreover, while the importance of digital platforms for public deliberation may be highlighted, their susceptibility to information manipulation, censorship and misuse often is not.[107] The need for accountability of Governments and the private sector is very rarely discussed. If these issues are not highlighted in strategies, staff may not feel empowered to raise the issues and ensure that they are integrated in operations.

In order to be actionable, strategies need to be translated into operational policies and procedures. However, with some notable exceptions,[108] these documents are not often made publicly available. This means that even where DFI strategies do recognize digital risks, it is not always clear how the risks are to be addressed in practice. In such circumstances, stakeholders will have no means of knowing how strategies are intended to translate into action on the ground.

Furthermore, DFI strategies often do not deal with some of the more complex challenges such as:

- How to deal with requests from sovereign borrowers that have neither the commitment nor the capacity to implement appropriate safeguards to protect users from misuse. It is one thing for DFIs to support appropriate health and education programmes in authoritarian States, subject to certain conditions, where financing provides critical services directly to populations; however, it is quite another matter for DFIs to use public funds to finance tools of government oppression or business models that violate privacy and other human rights.[109]

[105] See box 24 for an elaboration of DFI work on AI.

[106] For an indication of the pervasiveness and severity of some of these risks see Allie Funk and others, "Freedom on the Net 2023: The repressive power of artificial intelligence", Freedom House. The World Bank *World Development Report: Data for Better Lives*, although a research report rather than a strategy, discusses some of these risks, including in the main messages section (pp. 2 and 196), where warning is given for abuse of data "for unchecked state surveillance or mission creep, thereby undermining trust in data use". See also Francesca Spidalieri and Melissa Hathaway, "De-risking digital investments to support cyber resilient development", World Bank Blogs, 4 May 2022, which notes that "most digital investments and development assistance programs have not placed the necessary attention (or de-risking mechanisms) on the risks stemming from the misuse of ICTs, including becoming tools for cybercrime, data exploitation, critical infrastructure failures, disruptions of essential services, increased surveillance, disinformation, digital authoritarianism, and other risks to health and safety".

[107] See, for example, ADB, "Strategy 2030 Digital Technology for Development Directional Guide: Supporting Inclusive Digital Transformation for Asia and the Pacific" (2022), p. 18, where it is noted that: "With infrastructure and systems across sectors and nations becoming increasingly interconnected and dependent on digital technologies and systems, this has exposed economic and social systems to a myriad of cyber security and privacy risks".

[108] For example, the World Bank has put into the public domain the *ID4D Practitioner's Guide* and a toolkit for regulatory authorities on digital identification for financial inclusion. Moreover, some of the leading MDBs have established a practice of consulting publicly on guidance notes accompanying their E&S safeguards, in addition to the policies.

[109] See, for example, Coalition for Human Rights in Development, International Accountability Project and Early Warning System, "Financing Repression: Why development banks must rethink finance in countries blocking civic freedoms" (2024).

© Adobe Stock/Generative AI/ by franxlin_studio

- How to deal with the uncertainty of emerging and, at times, competing new regulatory frameworks, or emerging and, at times, contentious concepts, such as "digital sovereignty".[110]
- How to respond to demand from clients for AI-driven solutions, given the particular uncertainties and potential systemic risks that may be involved.
- How to deal with dual-use items and what guardrails would be appropriate in this context. For example, DFIs mandated to support development and the SDGs should not support dual-use items that can be used for military applications.
- How to weigh up potential changes in Government, particularly in fragile and conflict-affected settings when planning and financing longer-term projects, such as large-scale digital ID programmes, e-government platforms and telecommunications infrastructure. The World Bank estimates that 60 per cent of the world's extreme poor will live in countries affected by fragility, conflict and violence by 2030.[111] Given the potentially vast changes that some digital projects involve, careful assessment is needed of the long-term consequences for the countries in question, taking into account political volatility and the potential consequences of regime change.[112]

[110] See, for example, European Centre for Development Policy (ECDPM), *Global Approaches to Digital Sovereignty: Competing Definitions and Contrasting Policy* (2023).

[111] See the World Bank, "Fragility, Conflict & Violence".

[112] DFIs need to be careful not to put digital tools into the hands of Governments or other parties that may use them for harmful purposes. For example, when the Government in Afghanistan fell, the Taliban accessed biometric data gathered by a range of organizations to track down those who had supported the North Atlantic Treaty Organization (NATO). See Katja Lindsov Jacobsen, "Biometric data flows and unintended consequences of counterterrorism", *International Review of the Red Cross*, vol. 103, No. 916–917 (April 2021); and Rina Chandran and others, "Afghan panic over digital footprints spurs call for data collection rethink", Reuters, 20 August 2021.

Box 3 DFI digital strategies that recognize digital risks

A number of DFIs explicitly reflect digital risks in their strategies,[113] although the specificity and detail of strategic approaches to managing risk vary considerably and are often far less detailed than discussions about opportunities.

- **ADB.** The ADB "Strategy 2030: Digital Technology for Development Directional Guide" is based on five principes: (a) digital transformation; (b) integrated approach; (c) inclusive digital development; (d) improved digital safeguards; and (e) a differentiated approach based on a country's digital readiness and demands.[114] With regard to digital safeguards, ADB focuses on the management of privacy and security risks and the promotion of the responsible use of technologies and data.[115] A lack of attention to digital risks to date is acknowledged in the strategy, although it also noted that ADB has nonetheless been advising Governments on e-governance reforms and other digital activities highlighted in the strategy.[116]
- **AIIB.** AIIB has stated that its vision is "to play a catalytical role in financing the growth of digital infrastructure in Asia".[117] AIIB invests in hard and soft infrastructure and its definition of risk comprises: (a) regulatory risks; (b) technology obsolescence risks; (c) reputational risk; and (d) E&S risks. Human rights impacts are specifically referred to.[118] The AIIB vision notes that regulatory requirements can differ quite significantly from country to country, leading to significant differences in social impact. With regard to specific transactions, it notes that "the Bank's investment will be based on solid regulatory risks analysis for digital infrastructure projects. This analysis will allow AIIB to balance out data privacy risk with reputational risk and make good investment decisions". Digital infrastructure risks in relation to social inclusion are also recognized, noting that these will be reflected and addressed in line with its E&S safeguards.[119] However, the AIIB E&S safeguards do not specifically address digital risks in contrast to emerging practice elsewhere. The strategy also recognizes that certain digital risks may be too high or evolve too rapidly to be adequately mitigated, in which case the given project will not be financed. In this regard, AIIB notes that "given the nature of the sector, prudence will be the primary principle adopted by AIIB in pursuing its investment in digital infrastructure".[120]

[113] Each institution adopts and presents strategies differently. For example, some are board-approved, while others are presented as strategies on websites. The excerpts were taken from documents or text labelled as strategies and have been footnoted to identify the source.

[114] ADB, "Strategy 2030 Digital Technology for Development Directional Guide: Supporting Inclusive Digital Transformation for Asia and the Pacific" (2022), p. 17.

[115] Ibid., p. 33. However, the subjects are only addressed in one paragraph on the last page of a 33-page document.

[116] ADB acknowledged that it has only "started to explore data privacy, security, and ethics in response to demands from DMCs and the Board of Directors" and that it has a new interdepartmental working group to explore improved approaches to risk assessment, and ethical concerns related to digital technologies and their impact for their operations. See ADB, "Strategy 2030 Digital Technology for Development Directional Guide: Supporting Inclusive Digital Transformation for Asia and the Pacific", pp. 11–12.

[117] AIIB, "Digital Infrastructure Sector Strategy" (2020), p. 4.

[118] Ibid., p. 6, where it is noted that: "Data sharing and processing have led to risks associated with inappropriate use of personal information by third parties, public or private. These risks materialize in an infringement on people's fundamental rights through the use of certain technologies or in the way that the data is collected, stored and used over time."

[119] Ibid., p. 7.

[120] Ibid., pp. 7–8.

- **EBRD.** EBRD has committed to using the digital transition as an enabler of transition in all of the economies and sectors in which it invests as part of its overall strategy. In its Telecommunications, Media and Technology Sector Strategy, EBRD explains that it will strengthen its focus on "investing in digital infrastructure and tech-enabled products and services, which are considered to be mutually reinforcing parts of an integrated digital landscape".[121] EBRD's approach to the sector focuses on four areas: infrastructure; new technologies; IT services; and privatization and commercialization.[122] The strategy document discusses a range of issues, including environmental, climate, energy and water use impacts of data centres, pollution impacts from mining, biodiversity impacts of sub-sea cables, cybersecurity risks, algorithm complexity, gender gaps and gaps in digital skills and connectivity. A previous digital strategy committed EBRD by 2025 to "review environmental, social and governance standards and client adherence to codes of conduct to ensure the ethical and responsible application and use of technologies" and to update "the Bank's due diligence as part of its compliance with relevant Environmental and Social Policy (ESP) Performance Requirements."[123]
- **EIB.** While EIB does not have a separate digital strategy, it notes in its global strategy (for investments outside the European Union) that its "main goal is to increase the impact of its activities aligned with EU priorities, notably its emphasis on the twin climate and digital transition". EIB also notes that it will promote European Union values as part of its work, including human rights and digital norms.[124]
- **JICA.** The "Global Agenda on Digital Development" of the Japan International Cooperation Agency (JICA) notes that in order to promote digitalization in developing countries, it is "indispensable to create a free and secure digital society". Support for the use of digital tools will be provided, giving "due considerations for fundamental human rights, rule of law and governance, and consolidation of democratization".[125]
- **World Bank.** In the World Bank publication *Digital Development: Global Practice*,[126] digitalization is flagged as "the transformative opportunity of our time".[127] More so than most other DFIs, it highlights a balanced approach to digitalization, stating that its aim is "to maximize the benefits of digitalization – the digital dividends – for all, while mitigating the risks".[128] It focuses on key elements which, combined, "form the basis for strong, inclusive, and responsible digital transformation for economies, governments, and societies": (a) broadband connectivity, access, and use; (b) digital data infrastructure; (c) digital safeguards; (d) digital and climate; and (e) ICT industry and digital jobs.[129] Digital safeguards covers data protection and cybersecurity for the purpose of "building and strengthening trust in usage of digital platforms and services among people, governments, and businesses".[130] The approach also highlights the importance of inclusive digital opportunities while managing risks of exclusion. A new position of Digital Vice President has been established to support these and related objectives.[131]

[121] EBRD, "TMT Sector Strategy 2025–2029" (London, 2025).

[122] Ibid., p. 6.

[123] EBRD, "The EBRD's approach to accelerating the digital transition, 2021–25" (London, 2021), pp. 3–4.

[124] EIB, "EIB Global Strategic Roadmap", p. 1.

[125] JICA, "Global Agenda for Digital for Development".

[126] It is not clear to OHCHR whether this publication constitutes a strategy. However, it is cited because of the balance it strikes between opportunities and risks.

[127] World Bank, *Digital Development: Global Practice* (Washington, D.C., 2024), p. 1.

[128] Ibid., p. 1.

[129] Ibid., p. 2.

[130] Ibid., p. 5.

[131] World Bank, "The Knowledge Compact for Action: Transforming Ideas into Development Impact – for a World Free of Poverty on a Livable Planet" (Washington, D.C., 2024), pp. vi, 2, 19 and 23. See also World Bank, "World Bank Group announces Sangbu Kim as Vice President for Digital Transformation", 30 July 2024.

By contrast, other strategies contain little or no mention of digital risks:

- **AfDB.** The AfDB digital strategy action plan notes that the organization is turning its attention to three digital pillars: (a) the scaling of inclusive digital infrastructure; (b) digital entrepreneurship and skills development; and (c) the sectoral adoption of digitalization. The plan includes a brief discussion of cybersecurity and data protection in the context of enabling polices and notes that regulatory frameworks are essential for digital transformation and the growth of the "startup ecosystem". It also mentions "gender mainstreaming" (promoting market access and building digital skills for women) and climate change as "cross cutting issues".[132]
- **BII.** The overall strategy of British International Investment (BII) includes a section on financing digital transformation, but digital risks are not addressed.[133]
- **IDB.** The work of the Inter-American Development Bank (IDB) on data and digital government is aimed at supporting Governments in designing and implementing digital transformation plans and initiatives to enhance the efficiency of the public sector and the quality of services provided to citizens and the private sector. Cybersecurity is emphasized, but other digital risks are not addressed.[134]
- **IDB Invest.** The brief digital transformation strategy of IDB Invest is focused on helping clients to develop their digital capabilities and providing advisory services related to carrying out a strategic, sustainable digital transformation integrated with the SDGs. However, it does not draw attention to digital risks.[135]
- **IFC.** IFC does not appear to have a specific digital strategy guiding its operations and investments.[136]

2. ENVIRONMENTAL AND SOCIAL SAFEGUARDS ADDRESSING DIGITAL RISKS

E&S safeguards[137] deserve particular attention in the present context. Unlike many other kinds of policies and approaches, E&S safeguard policies:

- **Establish binding requirements for DFI due diligence and client E&S risk management**, specific to the different stages of the DFI project cycle;
- **Are the product of public consultation processes**, which confer legitimacy, strengthen ownership and trust, and ensure that a wide range of stakeholders' views and perspectives are reflected;
- **Are approved by the executive boards of DFIs**, which confer authority and facilitate their systematic implementation;
- **Are backed by independent accountability**, which is particularly important in facilitating access to remedy for project-affected people, minimizing negative externalities of projects and strengthening lesson learning and feedback loops from operations to policy.

[132] AfDB, *Digital Transformation Action Plan 2024–2028* (2024).

[133] BII, *Productive, Sustainable and Inclusive Investment 2022–26 Technical Strategy*, p. 12. However, see footnote 144 below, and accompanying text.

[134] See the "Who we are" section of the IDB website.

[135] See IDB Invest, "Digital transformation".

[136] Nevertheless, the IFC "Strategy and business outlook FY24-26" includes a paragraph identifying digitalization as one of the Corporation's strategic priorities for the period.

[137] See footnote 8 above on "E&S safeguards".

The safeguard policies of the leading MDBs have also indirectly influenced national laws and policies on E&S issues, in addition to their direct benefits at the project level.[138] Hence, for all these reasons, what is included in DFI safeguard policies, and what is omitted, matters.

E&S safeguards originated in the late 1980s in response to a particular set of physical E&S risks associated with traditional infrastructure investment projects. Originating with the World Bank, safeguard policies have been replicated in all major MDBs and a number of bilateral DFIs, based on their recognized value to DFIs, their clients and their investees. They are now a key component of the "licence to operate" and value proposition of DFIs,[139] serving as an essential tool for promoting sustainability and managing E&S risks throughout the project cycle, based on publicly disclosed and differentiated requirements for DFIs and their clients, respectively. Accountability for harms to affected stakeholders as a result of policy non-compliance is facilitated by the IAMs of DFIs.[140]

The scope of E&S risks and impacts covered by E&S safeguard policies has expanded significantly over time, yet until recently there has been no reference to digital risks. In a 2023 review of DFI E&S safeguards, OHCHR identified a lack of attention to digital risks as among the most significant gaps in E&S safeguards.[141] However, this is beginning to change. At the time of writing, the updated E&S safeguards of EBRD and ADB explicitly included some limited attention to certain digital risks. The AfDB guidance note on assessing and managing E&S risks and impacts, which accompanies the 2023 update of the Bank's integrated safeguard system, provides guidance on a more comprehensive set of digital risks.[142] In the E&S implementation manual of IDB Invest, a brief reference is made to digital data and privacy considerations within the context of evolving E&S risks.[143] Among bilateral DFIs, the Policy on Responsible Investing of BII[144] explicitly includes discussion of privacy, data protection, cybersecurity and AI risks.

[138] See Benedict Kingsbury, "Operational policies of international institutions as part of the lawmaking process", in *The Reality of International Law: Essays in the Honour of Ian Brownlie*, Guy Goodwin-Gill and Stefan Talmon (eds.) (Oxford University Press, 1999), p. 323; and Daniel Bradlow, and Andria Naudé Fourie, "The operational policies of the World Bank and the International Finance Corporation", *International Organizations Law Review*, vol. 10 (January 2013), p. 3. Environmental impact assessments are an example of a policy innovation promoted by MDB safeguard policies.

[139] See, for example, World Bank, "External review of the board approved reforms to the inspection panel toolkit and the creation of the World Bank accountability mechanism", 30 January 2024, in which it is stated: "Accountability is at the core of the World Bank's value proposition as premier development finance institution". Useful evaluations include IEG-World Bank, *Safeguards and Sustainability Policies in a Changing World* (2010) (including chap. 4 on benefits and costs of safeguards); and ADB, *Real-Time Evaluation of ADB's Safeguard Implementation Experience Based on Selected Case Studies* (2016).

[140] IAMs can serve a range of important accountability functions, but they are only one part of the remedy ecosystem in any context. See OHCHR, *Remedy in Development Finance: Guidance and Practice* (New York and Geneva, 2022).

[141] OHCHR, *Benchmarking Study of Development Finance Institutions' Safeguard Policies*.

[142] AfDB, *Borrower Guidance Note for E&S Operational Safeguard 1: Assessment and Management of Environmental and Social Risks and Impacts* (2024), p. 18.

[143] IDB Invest, *Implementation Manual for the Environmental and Social Sustainability Policy* (2021), p. 161, includes a brief reference to digital data and privacy considerations within the context of evolving E&S risks, as follows: "Environmental and social risk management is an evolving area of work. There are topics where standards are only recently being discussed or have not yet been fully established, such as the human rights dimensions of digital data and privacy considerations".

[144] BII, "Policy on Responsible Investing" (April 2022).

Box 4 Provisions on digital risks in E&S safeguards and supporting materials

ADB

- ADB Environmental and Social Framework (2024)[145] defines "digital risks" as "risks relating to cybersecurity, data privacy, and data management resulting from creation, delivery, and use of digital technologies and information technologies".
- The E&S Policy, (in para. 24) states that the E&S risk classification will also consider risks that are relevant in the context in which a project is being developed or to be implemented, which may include digital risks for which the host country may have limited legal and regulatory framework, institutional capacity and understanding, that may have potential for significant E&S impact.
- The E&S Policy also states (in para. 33) that: "the Bank will consider in its review of a borrower's and/or client's environmental and social assessment all relevant environmental and social risks and impacts of a project as described in detail in the ADB Environmental and Social Standards 2 to 10, including but not limited to social risks and impacts such as digital risks".
- The Policy further states (in para. 34) that the ADB review of the E&S assessment process undertaken by a borrower and/or client will include considering and integrating into the E&S assessment process, as relevant, additional information obtained by ADB through its other tools and instruments, such as digital risk assessment.
- With regard to the ADB Environmental and Social Standard 1 (para. 26), the Policy states that the borrower/client will ensure that the E&S assessment will take into account all relevant environmental and social risks and impacts of a project as described in detail in Environmental and Social Standards 2 to 10, including social risks and impacts, such as digital risks.
- Environmental and Social Standard 1 (para. 34) states that where a project involves significant use of digital technology and/or information technologies, the E&S assessment will consider digital risks resulting from usage of such technologies. In the absence of a host country's applicable laws on digital risks, evolving good practices will be applied as appropriate to develop appropriate measures to manage such risks and impacts.[146]

EBRD

- In the EBRD Environmental and Social Policy, paragraph 2.13 states that the EBRD Bank is cognizant of the possible adverse E&S impacts, issues and risks of digitalization, cybersecurity and data privacy with respect to human rights and public health and safety.[147]

[145] See ADB, *Environmental and Social Framework* (2024), "Definitions". This Framework consists of an E&S Policy (applicable to ADB) and E&S Standards (applicable to the client).

[146] However, para. 34 of "Environmental and Social Standard 1" (within the ADB *Environmental and Social Framework*) addresses the situation of where national laws on digital risks are present, but inadequate.

[147] See EBRD, Environmental and Social Framework. However, in para. 2.13, it is stated: "The Bank will consider where the use of significant digitalization can have adverse environmental and social impacts in the projects it finances *in line with national legislation*" (emphasis added). At face value, the italicized phrase would seem to confine the Bank's due diligence on digital risk matters to the (frequently weak) parameters of national law, which would set up a contradiction with the Bank's policy commitment to respect international human rights (paras. 2.4 and 2.5). According to para. 17 of the EBRD "Environmental and Social Requirement 1", the client's digital risk management obligations lack any such constraint. Further, "The EBRD's approach to accelerating the digital transition 2021–25", p. 21, states that "The Bank will undertake its own due diligence in applying the ESP to ensure that the potential impacts of digitalization and cybersecurity on workers, project-affected people and broader stakeholders are taken into account". And to similar effect, the AIIB "Digital Infrastructure Sector Strategy" recognizes that "there are digital infrastructure-specific risks, especially in relation to social inclusion, and will ensure that these are properly reflected and addressed as guided by the Bank's Environmental and Social Framework and Corporate Strategy". At the time of writing, however, AIIB did not have specific digital risk requirements in its E&S framework.

- According to the EBRD Environmental and Social Requirement 1, para. 17, where projects or clients' business activities involve the management of digital personal data, significant reliance on digital services and technologies, or the substantial digitalization of services or products, the assessment process will consider E&S risks and impacts associated with cybersecurity, data protection and privacy.
- In the EBRD Environmental and Social Requirement 2, para. 4(c) clarifies that "gig workers", or digital platform workers, are covered by the labour requirements set out in the *Environmental and Social Policy*.[148]

EIB

The EIB *Environmental and Social Standards* contain brief references to the right to privacy and data protection, in line with the European Union General Data Protection Regulation.[149]

AfDB

The updated AfDB Borrower Guidance Note on the Assessment and Management of Environmental and Social Risks and Impacts, published as part of its Integrated Safeguards System, notes that E&S risk assessments should incorporate "misuse of information technology", which is highlighted as including inappropriate, lax or illegal collection, handing and safe storage of data such as:

- The misuse of surveillance technology, facial recognition, biometric technology or digital ID systems that exposes people to personal security risks.
- The collection of data on communities or stakeholder groups (especially those that may be vulnerable) that can be collated and used in ways the community may be unaware of and may exposure them to personal security risks.
- The inappropriate collection and use of data collected during social assessment, which introduces risks such as facial recognition bias according to skin colour, exclusionary data formats and discriminatory biases in algorithms.
- Poor data security practices that expose people's financial information, such as account details, the nature of their assets and compensation payments received, which makes them vulnerable to data theft, extortion, fraud and scamming practices.[150]

BII

In the BII Policy on Responsible Investing, two categories of policy are covered:

Risk-specific E&S requirements that certain clients must comply with include:

- Certain business activities create particular risks (including human rights, such as the right to privacy) for customers and clients. Businesses where these risks may be evident are financial service (including digital financial service) providers and investees that hold or have access to personal data. Investees that are financial service or digital financial service providers must have appropriate client protection procedures and practices. Investees that hold or have access to personal data must have processes and governance controls that monitor, manage and reduce risks related to data privacy.[151]

[148] In para. 4(c) of "Environmental and Social Requirement 2" of the EBRD Environmental and Social Framework, coverage is extended to "people engaged on individual service contracts through self-employment or digital labour intermediation platforms to perform work related to the project".

[149] EIB, *Environmental and Social Standards* (2022), see para. 7 of "Standard 1: Environmental and Social Impacts and Risks", para. 9 of "Standard 2: Stakeholder Engagement" and para. 18 of "Standard 8: Labour Rights".

[150] AfDB, *Borrower Guidance Note for E&S Operational Safeguard 1: Assessment and Management of Environmental and Social Risks and Impacts*, p. 18, para. 24.

[151] BII, "Policy on Responsible Investing", p. 21.

Recommended practices for clients, which address:

- AI, notably encouraging the responsible development and implementation of AI to meet human rights obligations under the United Nations Guiding Principles on Business and Human Rights and to avoid operational, financial, legal and reputational risks linked to AI.[152]
- Cybersecurity, data protection and data privacy, encouraging investees to incorporate data privacy principles into the development of legal, technology and policy frameworks, and embedding them into operations and business models. Important principles include freedom of expression and issues linked to content regulation and surveillance, forced shutdowns, requests for data and access and encryption.[153]

IDB

While not specifically reflected in its Environmental and Social Policy Framework, the IDB has set out an explanation of how the requirements in the framework apply to addressing risks to and impacts of digital rights in its projects. This includes incorporating the following in project E&S management systems: digital rights risk and impact assessments and corresponding intervention options and checklists to address them, a stakeholder engagement strategy that ensures citizen participation in the design and implementation of digital initiatives, and a grievance redress mechanism able to channel queries and requests on data processing.[154]

IDB Invest

The IDB Invest *Implementation Manual: Environmental and Social Sustainability Policy* notes that E&S risk management is an evolving area of work and that there are topics where standards are only recently being discussed or have not yet been fully established, such as the human rights dimensions of digital data and privacy considerations.[155]

The research undertaken for the present report indicates that E&S safeguard teams commonly identify risks associated with the physical footprint of digital projects, such as resettlement risks linked to the construction of digital infrastructure and climate change impacts of data centres or e-waste.[156] While some E&S summaries are beginning to include consideration of digital risks,[157] this practice seems inconsistent across projects and teams, and underlying definitions and approaches differ.

[152] Ibid., p. 29 and OHCHR, Guiding Principles on Business and Human Rights (2011).

[153] BII, "Policy on Responsible Investing", p. 32.

[154] Mauricio Tapia and Laura Romero, "5 Lessons on the Protection of Human Rights in Financing Digital Government Initiatives", IDB, 13 May 2024.

[155] IDB Invest, *Implementation Manual: Environmental and Social Sustainability Policy* (2022).

[156] See, for example, the BII sector profile on telecommunications, which addresses the physical impacts of mobile phone towers, air emissions, health and safety. In another project, BII was encouraged by Myanmar-based actors to prompt Frontiir to join the Global Network Initiative as a mitigation strategy to deal with the risky contextual environment. See BII, "Frontiir Pte Ltd".

[157] See, for example, the E&S review summary for IDB, Trinidad and Tobago, Conditional Credit Line for Investment Projects (CCLIP) for the National Digital Transformation Program (TT-O0011), Environmental and Social Review Summary, which includes an assessment and action plan on a range of digital issues: "Human rights risk and impact assessments are a requirement set out in the ESPS 1 para. 6; ESPS 1, footnote 51 and ESPF Guide for ESPS 1, GL33." The document also notes: "[a]n additional helpful resource is the Danish Institute's Human Rights Risk Assessment Guidance Tool: https://digitalrights-check.bmz-digital.global/". The action plan for the project includes the implementation of an Environmental and Social Management System (ESMS) with a specific focus on digital rights, privacy and digital inclusion (pages 2–5). See also BII, Frontiir Pte Ltd (2019), where BII was encouraged by Myanmar-based actors to prompt Frontiir to join the Global Network Initiative as a mitigation strategy to deal with the risky contextual environment.

© Adobe Stock/Generative AI/by yong

Significantly, digital projects are very often classified as low risk because they involve risks that are not yet reflected in MDB E&S safeguard policies, thus triggering fewer (or no) due diligence requirements.[158] Even more concerning is that advisory projects involving regulatory advice (which may have systemic impacts) are often assigned no risk categorization, meaning there is no project documentation to identify associated risks.[159] In fact, the majority of the 3,450 projects reviewed in the OHCHR digital risk-mapping exercise had no risk categorization whatsoever.[160] For a breakdown of digital projects by the E&S classification assigned by the DFI, see figure VI.

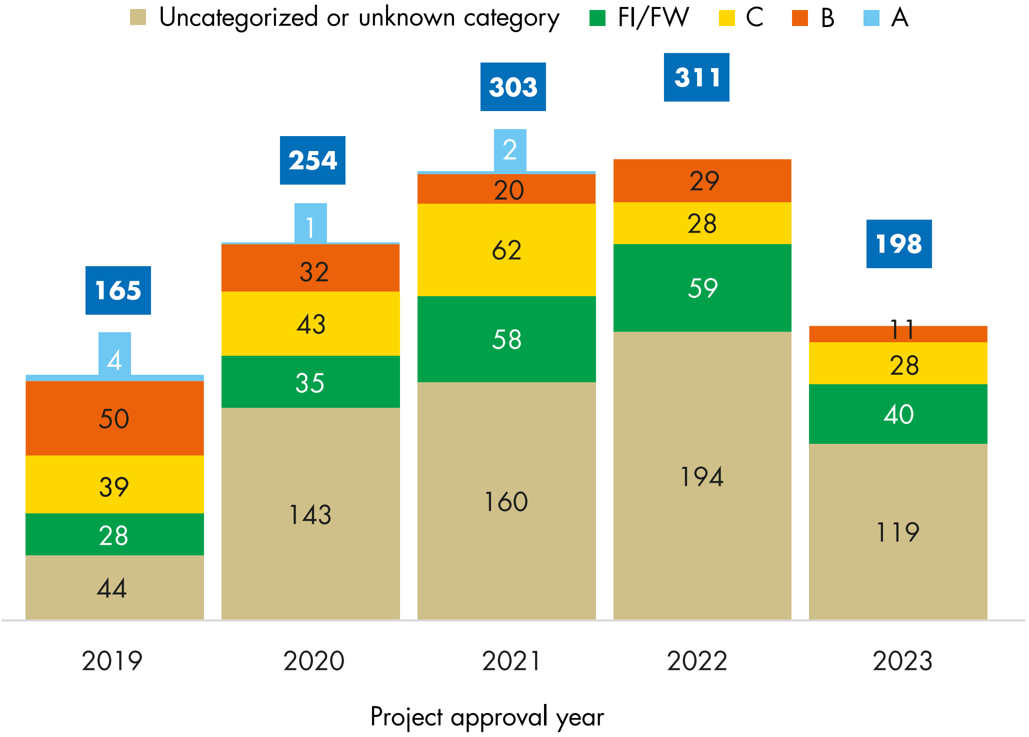
[158] See, for example, IFC, "Guidance Note on Financial Intermediaries" (2023). Table 1, p. 5, notes that for equity investments in venture capital funds, the fund must screen an investee company involved in non-IT-related activities (e.g. manufacturing, logistics, agriculture, etc.) against key requirements of the IFC Performance Standards, but for "IT-related activities, the assessment focuses on PS2 (labor and working conditions)." DFC, "Environmental and Social Policy and Procedures" (2024), p. 24, notes that "FIs that invest in tech or tech-enabled investments that do not involve significant physical assets and investments in financial institutions or fund-of-funds" are categorized as FI-C (the lowest risk category).

[159] Compounding this concern, MDBs are not always clear about the scope of application of their E&S safeguards and whether advisory projects are included, even in the newer safeguards. See, for example, ADB, *Environmental and Social Framework*, p. 7, which seems to provide little clarity on this point.

[160] In addition, most MDBs do not seem to provide a sufficiently clear explanation about the content of their project databases, explaining what projects are included and which ones are not. To this extent, it is difficult to establish whether there may be further relevant projects to review, for example, those funded by trust funds.

FIGURE VI

DIGITAL PROJECTS BY E&S RISK CLASSIFICATION, 2019–2023



The diverse and rapidly evolving nature of digital risks presents particular challenges to E&S safeguards, which, in the case of the major MDBs, may have a lifespan exceeding 10 years.[161] Balancing the need for publicly consulted, board-approved policies with the operational flexibility required to address the rapidly evolving character of digital risks can be challenging. Chapter III outlines a framework that seeks to marry principle with pragmatism, under which a certain set of core digital risk management concerns and requirements would be embedded in E&S safeguards, complemented by a potentially wide range of other guidance material, approaches and tools that could be adapted and updated as emerging needs require.

3. OTHER OPERATIONAL POLICIES THAT ADDRESS DIGITAL RISKS

The research undertaken for this report failed to disclose any other types of publicly available operational policies that specifically govern the identification and management of a broad range of digital risks throughout the project cycle.[162] As is understood by OHCHR, some DFIs have operational policies that govern digital risk management, although, unlike E&S safeguards, these policies are not necessarily public. Most DFIs are at a relatively early stage of addressing these issues, hence policy development can be expected to follow emerging practice.

[161] The prescribed lifespan of the current generation of MDB safeguards is typically in the vicinity of five years. However, as of 2024, the IFC *Sustainability Framework: Policy and Performance Standards on Environmental and Social Sustainability: Access to Information Policy*; and the ADB *Safeguard Policy Statement* had been in effect for 12 and 15 years, respectively.

[162] In addition, in the responses from DFIs to the OHCHR questionnaire in August 2024 did not identify additional non-public policies, but a number of non-public risk management tools were highlighted (see box 5).

Nevertheless, in the view of OHCHR, the breadth of digital activities among DFIs,[163] and the severity of many digital risks, make it all the more important to put in place transparent, consistent and effective policy approaches at the earliest possible time.

Some digital risks, such as cybersecurity, may be managed as operational or commercial risks rather than E&S issues. This means these risks are being viewed and managed as risks to the business, rather than as risks to people arising from business activities, contrary to the understanding of risk in E&S safeguards. This is a crucial distinction when considering which teams should be involved in managing digital risks.

Some DFIs have internal digital risk management processes for projects (see box 5). DFIs typically have their own privacy and data offices managing how these issues are handled within the institution. The offices, while focused on internal operations, are often well resourced and help raise staff awareness of these issues. E&S teams have a different mandate and typically have a clearance function that investment teams do not have.

Box 5 Examples of internal digital risk management processes

Certain MDBs apply, or are in the process of developing, digital risk screening procedures in their portfolios. Certain bilateral DFIs are also making inroads in this direction. For example, **Finnfund** has reported to OHCHR that it has put in place the following measures to address digital risks during appraisal and monitoring of investments:

- An information and communications technology and cybersecurity/data-security screening questionnaire;
- Additional due diligence procedures related to data protection, cybersecurity and risks of surveillance;
- A requirement for investee companies to have certified information security management systems (e.g. ISO 27001);
- A requirement for investee microfinance institutions to comply with Client Protection Pathway principles on the protection of microfinance customer privacy and data;[164]
- Specific reporting requirements by companies, such as Internet service provides or mobile network operators, to report on requests for client data and information or requests to shut down connectivity services (certain websites or full Internet) received from the authorities of a country of operation, and to disclose to Finnfund the procedures applied to respond to and manage such requests.[165]

[163] See, for example, World Bank, *Mobilizing Technology for Development*, which sets out a huge range of activities across the World Bank and IFC (p. 8, box 1.4), focused on the disruptive and transformative technologies programmes and units of the World Bank.

[164] See Finnfund, "Client protection in microfinancing".

[165] See also Sylvie Fraboulet-Jussila, "A tale of surveillance – investor's role in dealing with data confidentiality", Finnfund, 27 June 2022.

4. SPECIALIZED LEGAL PROVISIONS

DFIs set out their requirements for borrowers in their loan contracts (which may be referred to by various names, including financing agreements, credit agreements and lending agreements) and investment contracts. Conditions borrowers/investees must meet and commitments about how projects will be managed are set out in these contracts and typically require compliance with national law as well as with the relevant DFI E&S safeguards. The crafting of these provisions typically entails coordination between legal or compliance departments, investment teams, sector specialists and E&S specialists.

Anecdotally, as is understood by OHCHR, some public-sector financing MDBs have incorporated digital risk management requirements into lending agreements,[166] although the extent of this practice is not clear. In response to an OHCHR questionnaire in connection with the present report, two bilateral DFIs focused on private-sector funding described the coverage of specialized provisions addressing digital issues in their contracts with private sector clients (see box 6). Further research on the frequency, scope, specificity and impact of digital risk management contractual provisions would be useful. Contractual provisions are legally binding (unless waived) and, if sufficiently specific, provide potentially significant leverage over a client if the DFI chooses to exercise it. However, if contracts are not publicly disclosed, there is no way for affected stakeholders to know what conditions have been required of clients. For the reasons outlined in the methodology section (see annex II), it is the view of OHCHR that contracts should not be the sole source of information to potentially affected stakeholders about digital risk management requirements. Rather, in addition to contracts the information should be included for high-risk projects in project summaries and E&S summaries, and should be integrated for all projects in project appraisal documents in advance of project approval.

Contracts between DFIs and their private sectors clients are not publicly available. Loan contracts for sovereign clients are very different from loan contracts with private sector clients. Some DFIs disclose their contracts with sovereign clients. According to Publish What You Fund, ADB,[167] IDB[168] and the World Bank[169] disclose sovereign contracts, whereas AfDB,[170] AIIB,[171] EBRD[172] and EIB[173] do not.

[166] This is the case for the World Bank, as discussed earlier (footnote 104 above).

[167] See Publish What You Fund, "DFI Index AsDB – sovereign", which includes an analysis of ADB disclosure of core information, including loan contracts. The Fund scores sovereign lenders on their disclosure of "core information" including the disclosure of loan contracts. The Publish What You Fund assessment helpfully includes an assessment of both policy and practice on contract disclosure.

[168] See Publish What You Fund, "DFI Index IDB – sovereign", which includes an analysis of IDB disclosure of core information, including loan contracts.

[169] See Publish What You Fund, "DFI Index World Bank", which includes an analysis of World Bank disclosure of core information, including loan contracts.

[170] See Publish What You Fund, "DFI Index AfDB – sovereign", which includes an analysis of AfDB disclosure of core information, including loan contracts.

[171] See Publish What You Fund, "DFI Index AIIB – sovereign", which includes an analysis of AIIB disclosure of core information, including loan contracts.

[172] See Publish What You Fund, "DFI Index EBRD – sovereign", which includes an analysis of EBRD disclosure of core information, including loan contracts.

[173] See Publish What You Fund, "DFI Index EIB – sovereign", which includes an analysis of EIB disclosure of core information, including loan contracts.

Box 6 Examples of specialized contractual provisions in private sector contracts

The **BII** standard legal requirements for equity investment require investees to maintain (through their management system) adequate and proportionate policies and procedures for the group to protect the security of IT systems, personal data and the rights of individuals to privacy.[174]

The "digital specific" contractual provisions of **Finnfund** are additional to its standard E&S contractual provisions and may include, where applicable:

- Transparency reporting
- Certification of information security management systems
- Client data protection
- Compliance with local laws and regulations governing digital rights and risks
- Relevant regulatory licences in place
- Actions under a specific E&S action plan.[175]

5. OTHER DIGITAL INITIATIVES, TOOLS AND PUBLICATIONS

DFIs have promulgated a wide range of other initiatives, tools and publications relevant to digital risk management in recent years. Numerous DFIs are actively involved in developing knowledge products, leading and participating in expert or multi-stakeholder initiatives, developing standards, benchmarking and gathering and analysing data. The practice of the World Bank is particularly noteworthy in this regard.[176]

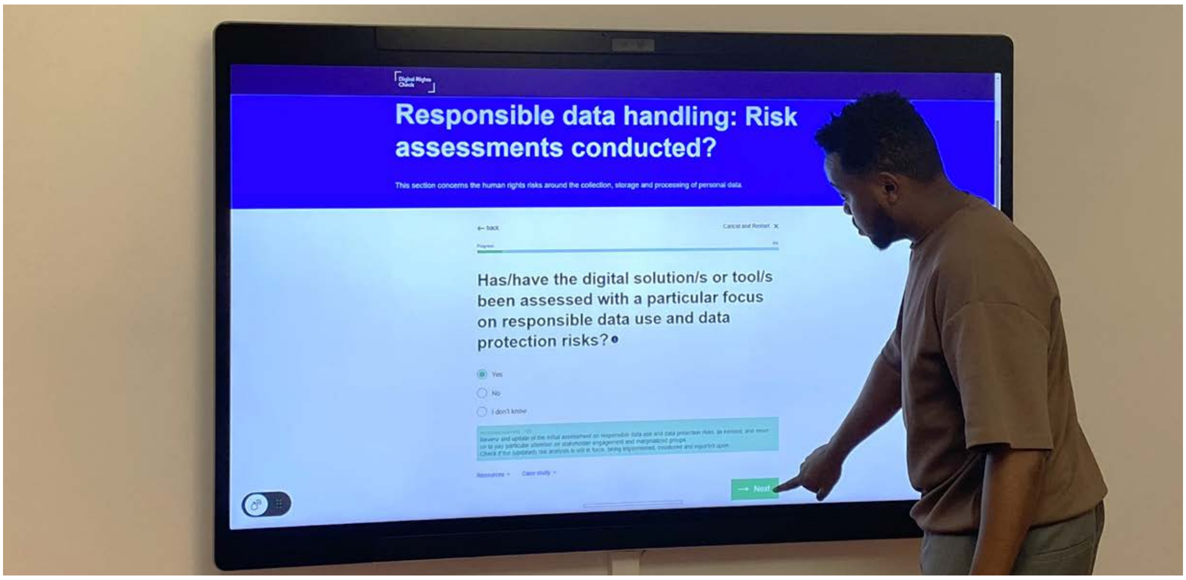
This section discusses only a handful of examples, in part due to the limits on publicly available documentation. Most DFIs have web pages describing their digital sector work, but very few list the tools used to guide their work in the sector, at least not in a comprehensive fashion. Hence, for any DFI, it can be difficult to glean a clear picture of the purpose, scope, uses and outcomes of the application of these tools in practice, in a manner that may help project-affected people.[177]

[174] Summary of information provided by BII, September 2024, on file with OHCHR.

[175] Summary of information provided by Finnfund, September 2024, on file with OHCHR.

[176] See, for example, World Bank, *Mobilizing Technology for Development*, box 1.4, p. 8. While it is a few years out of date at the time of writing, the Bank evaluation included a wide range of initiatives, although these focused only on disruptive innovations supported by the Bank.

[177] Among the more obvious exceptions is the World Bank *ID4D Practitioner's Guide*. However, the Guide is presented as one of several tools and there seems to be little clarity as to how the range of available tools should be applied, and in what sequence, when designing and implementing digital identification programmes.


Responsible data handling: Risk assessments conducted?
Has/have the digital solution/s or tool/s been assessed with a particular focus on responsible data use and data protection risks?
Yes
No
I don't know
Next

© KfW Development Bank/Maja Bott

Box 7 Examples of digital initiatives and tools

OHCHR has not reviewed the content of the following tools, but instead simply notes what appears to be relevant initiatives that could be built on to raise awareness of digital risks.

The **ADB Digital Learning Lab** programme seeks out innovative solutions across a range of areas including AI and big data.[178]

EBRD offers a cyber tool kit to support clients with digital and cyber resilience.[179] EBRD also supports States in carrying out digital maturity assessments, although these are not publicly available.[180]

IDB, through its **IDB Lab**, oversees the **fAIr LAC** initiative, which is aimed at promoting the responsible and ethical use of AI in entrepreneurship and innovation environments, based on a framework of trust, transparency and non-discrimination. The initiative provides several self-assessment tools in order to test whether a company is using ethical AI principles and to produce actionable recommendations.[181]

The **Social Digital** initiative from **IDB** is aimed at leveraging the benefits of technology to offer more and better social services in health and social protection, education, labour, social security, migration and gender and diversity."[182]

The **Machine Learning ESG Analyst (MALENA)**, from the **IFC**, is an AI analyst tool designed to extract insights from unstructured environmental, social and governance data at scale, enabling faster analysis and increased productivity. The tool is available cost-free to the public.

[178] See the ADB Digital Sandbox.

[179] See EBRD, "Digitalisation".

[180] See Owain Rich, "Digital approach with subtitles" (a Vimeo video), 4 May 2022. At the timing of writing, the tool did not appear to be available, but an example of the application of the tool is available in the eGA Digital Maturity Assessment of Montenegro – E-riigi Akadeemia.

[181] See IDB, *Artificial Intelligence for Social Good in Latin America and the Caribbean: The Regional Landscape and 12 Country Snapshots* (2020); IDB fAIR LAC; Cristina Pombo, "The IDB is bringing responsible and ethical AI to Latin America and the Caribbean"; and "OECD.AI Policy Observatory".

[182] See IDB, "Social Digital".

JICA has a cluster strategy for cybersecurity that is aimed at supporting responses to threats in cyberspace.[183]

The **World Bank** has a number of tools and initiatives:

- **The Cybersecurity Multi-Donor Trust Fund** produces tools and guides on cybersecurity, although not all of these are publicly available. The *Guide to Developing a National Cybersecurity Strategy* is aimed at expanding the coverage of good practices relating to the development of domestic cybersecurity and cybercrime legislation and regulation, and to safeguarding human rights and liberties.[184] The Bank has also developed a handbook on cybercrime that specifically discusses human rights concerns (*Combatting Cybercrime: Tools and Capacity Building for Emerging Economies*).
- **The GovTech Global Partnership** is a multi-stakeholder initiative that includes GovTech countries, development partners, private sector, academia, civil society and others involved in the GovTech domain. It brings together other global practices with the Bank, including those working on digital development, payment systems, data governance and sector specialists. This work is also supported through the GovTech Working Groups and the GovTech Innovation Lab.[185]
- **The GovTech Maturity Index** is a tool that measures countries' maturity in digital government transformation in focus areas including core government systems and shared digital platforms, online service delivery and digital citizen engagement.[186]
- **The Digital Economy for Africa (DE4A) Country Diagnostics** tool provides a snapshot of the state of the digital economy in a given country in Africa based on the five pillars of the Digital Economy for Africa initiative: digital infrastructure, digital public platforms, digital financial services, digital businesses and digital skills.[187]

One notable gap is the apparent lack of specific guidance on how to manage "business model risks" in DFI-financed private sector digital operations. Technology company business models are being increasingly criticized for creating or exacerbating negative impacts on a range of human rights.[188] Until recently, little attention has seemingly been paid to these kinds of risks in DFIs, with only isolated exceptions, such as in relation to the situation of platform workers.[189] In 2024, the Kreditanstalt für Wiederaufbau (German Financial Development Cooperation or KfW Development Bank), building on earlier work from the Danish Institute for Human Rights and the Deutsche Gesellschaft für Zusammenarbeit (GIZ), published a user-friendly digital risk management tool aimed specifically at addressing a range of human rights concerns (see box 8).

[183] JICA, "JICA Global Agenda for Digital for Development: Cluster Strategy for Cybersecurity" (2023).

[184] See International Telecommunication Union and others, *Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity* (2021).

[185] See World Bank, "Golden Program on GovTech & Public Sector Innovation – Overview".

[186] See World Bank, "Golden Program on GovTech & Public Sector Innovation – Data & Analytics" and United Nations, E-Government Development Index.

[187] See World Bank, "The Digital Economy for Africa Initiative".

[188] See OHCHR B-Tech Project, "Addressing business model related human rights risks", which analyses a "business model" in terms of a company's value proposition, value chain and revenue model.

[189] See, for example, BII and Swiss Investment Fund for Emerging Markets, "Managing labour risks and opportunities of platform work" (2022); and EBRD, *Toolkit for EBRD Clients – EBRD Performance Requirement 2: Labour and Working Conditions*, para. 4 (c).

Box 8 New tools for assessing and managing digital risks (including human rights risks)

- **The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)** offers its "Digital Rights Check" tool to staff and partners working in technical development cooperation and development finance to help ensure that digital projects or solutions do not negatively affect human rights.[190]
- **The KfW Development Bank** has developed its "KfW Digital Rights Check for Financial Cooperation" tool, based on the work of GIZ and the Danish Institute for Human Rights as well as the Principles for Digital Development.[191] KfW has made the tool available to other development banks that are financing public projects.
- The "Responsible Investment in Technology: Investor Guidelines for ESG Risk Management" published by the **German Investment and Development Corporation (DEG)** includes an environmental, social and governance risk management framework that caters to technology risk. It is also relevant for investors on a broader scale and can be integrated into existing environmental, social and governance risk management approaches to cater to the increasing adoption of technology in traditional businesses. The guide is aimed at helping investors improve their environmental, social and governance and human rights due diligence and their monitoring of technology investments.[192]

Several DFIs have produced publications that specifically address and call for greater attention to be paid to human rights risks in the digital sphere (see box 9).

Box 9 Examples of digital publications that address human rights risks

DFIs have developed a wide range of guidance documents on digital transformations, reflecting different balances between opportunities and risks. Several **specifically address human rights risks**, including:

- **World Bank**, *World Development Report: Data for Better Lives* (2021). The publication provides a detailed overview of the data landscape and proposes a rights-based approach, whereby access to personal data must first be adequately safeguarded before enabling use and reuse, and notes that safeguards for personal data should be grounded in the human rights framework based on international law.[193]

[190] See Digital Rights Check, "Introducing the Digital Rights Check" and the Danish Institute for Human Rights, *Guidance on Human Rights Impact Assessment of Digital Activities*. With regard to the latter, although it is not specifically for DFIs, it is useful for these entities because it is built on an impact assessment approach.

[191] See "Principles for Digital Development".

[192] DEG, "Responsible Investment in Technology: Investor Guidelines for ESG Risk Management".

[193] World Bank, *World Development Report 2021: Data for Better Lives* – see the overview, footnote 20 and p. 190. See also p. 207 of the report, on which it is stated: "One of the biggest contributors to the trust framework is the adoption of personal data protection legislation following a rights-based approach", and p. 194, where "substantive rights" (such as the right to privacy and non-discrimination) and "procedural rights" (such as necessity, transparency, accountability, proportionality and due process) are considered. The World Bank has also embarked on a project entitled "Tools for identifying the human rights impact and algorithmic accountability of artificial intelligence in World Bank operations".

- **ADB**, *Managing Digital Risks: A Primer* (2023). The publication contains a chapter discussing the human rights risks and implications of digitalization. No binding standards for the Bank or its clients are set out in the document; however, the importance of managing digital risks from the earliest stage of the project cycle is highlighted and it is recommended that clients should incorporate human rights risk factors associated with the data cycle (collection, storage, use and re-use) into their risk assessments to ensure the protection of vulnerable groups.[194]
- **IDB**, *Government Digital Transformation Guide* (2022) states that the digital regulatory framework for any country should include the development and publication of legal, ethical and moral codes that guarantee the rights of citizens in a new digital model. The IDB guide discusses human rights risks mostly in the context of privacy, data protection and cybersecurity, but also considers the right to access to information, human rights impacts of disruptive technologies, and to a lesser extent, discrimination in connection with access to e-services.[195]

6. STANDARD-SETTING ACTIVITIES

A range of DFIs, particularly the leading MDBs, are actively engaged in normative and technical standard-setting activities of different kinds in the digital space. The need for relevant, rigorous standards in this area is widely recognized. For example, EBRD has stated: "As a multilateral institution, the Bank will maintain the highest international standards within its digital approach".[196] However, it is not often clear how normative or ethical commitments are being implemented: some DFIs refer to applying international standards or collaborating on international standards in their digital strategies, but without identifying the standards concerned or the specific objectives for which given standards are selected, or how these are to be applied in projects and regulatory guidance to clients.

Box 10 Examples of standard-setting activities

The following standard-setting initiatives are addressed briefly in the next section.

- The **World Bank and partners** developed a set of **principles on digital ID** accompanied by a set of tools, knowledge products and examples of country-level actions.[197]
- The **IFC** and the **World Bank** are leading proponents of the **Ethical Principles in Health Care (EPIHC) initiative**, which includes digital dimensions.[198]

[194] ADB, *Managing Digital Risks: A Primer*, p. 74. In the report (p. xi), digital risk is defined more broadly than in the present report: "Digital risks can be defined as the risks associated with the creation, delivery, and use of digital technologies, processes, and services that are deployed to achieve operational efficiencies, scale new business models, or deliver new services to customers or the public".

[195] IDB, *Government Digital Transformation Guide* (2022), pp. 202, 205, 226–238, 287, 292 and 500 (on the right to privacy) and chap. 3.4 (pp. 409–414) on discrimination issues. Moreover, the IDB "Digital Inclusion Strategies: A Primer for Latin American Policymakers" (2024), provides guidance and best practice examples in relation to the legal and policy environment, digital literacy, addressing discrimination, participation and other prerequisites for inclusive digital strategies. See also Maria Isabel Gomez-Pineda Puebla and others, "Digital government driven by ESG: sustainable and inclusive public services", IDB, 31 July 2023.

[196] See EBRD, "Digitalisation".

[197] See World Bank, "ID4D".

[198] See IFC, "EPiHC Hits 100 Signatories, Emphasizing Importance of Ethical Provision of Healthcare", 15 June 2021.

Given the increasingly contested digital regulatory space,[199] clarity on the processes through which standards are developed is as critical as the content. As noted in a recent report from OHCHR on technical standards in the digital space and human rights: “Technical standards reflect the interests, values and concerns of those participating in their development. Many of the decisions made in the development process have crucial ramifications for human rights.”[200]

Given the increasing restrictions on human rights in the digital space in many parts of the world,[201] including censorship, surveillance and access restrictions, DFIs may find themselves under increasing pressure from some sovereign borrowers to accept, if not endorse, regulatory systems that limit or abridge the rights to freedom of expression, association and assembly and other internationally recognized human rights. Without clear policies and principles to guide regulatory work, DFI staff may run an increased risk of inadvertently enabling digital authoritarianism, contrary to international human rights law.

This problem may be compounded by the lack of specific standards and digital risk management requirements for entities contracted to implement digitalization projects. While procurement documentation is usually available for public sector projects above a specified contracted amount, the procurement documents themselves are not always specific about the standards (if any) being applied. Implementation may be left to private contractors, with no transparency on the terms of engagement or in relation to what standards or approaches are being applied.[202] Greater transparency would be beneficial in this respect.

B. ANALYSIS OF DIGITAL PROJECTS IN FOUR SECTORS

This chapter examines four key sectors: public administration, finance, health and digital infrastructure and services. As noted in the introduction, these sectors were selected for analysis because projects in these sectors (a) cover both the public and private sectors; (b) entail the relatively widespread use of digital technologies and relatively well-known digital risks; (c) may involve system-wide changes with deep and enduring implications for people (in particular, public administration and digital infrastructure projects); (d) may involve the collection and management of sensitive personal data; and (e) may be more likely to involve services to people, thus impacting on their rights in a very direct way.

[199] See, for example, ECDPM, *Global Approaches to Digital Sovereignty*; and Colum Lynch, “Exclusive: At UN, China seeks greater state control over internet”, Devex, 21 May 2024.

[200] See OHCHR report, *Human rights and technical standard-setting processes for new and emerging digital technologies* (A/HRC/53/42), para. 17; and Center for Human Rights and Global Justice, NYU Law, Institute for Law, Technology and Innovation and Temple University, “Shaping digital identity standards: an explainer and recommendation on technical standard setting for digital identify systems” (2023).

[201] See, for example, Adrian Shahbaz and others, “Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet”, Freedom House; and Access Now for the #KeepItOn coalition, “The Return of Digital Authoritarianism: Internet Shutdowns in 2021” (2022).

[202] New York University School of Law, International Organizations Clinic, “Submission for the Review and Update of the ADB Safeguard Policy Statement” (April 2022). In comparison, the reliance by MDBs on borrowers’ electronic procurement systems is guided by the “Guide for the assessment of electronic government procurement systems intended for use under MDB financed operations” (2023), which includes indicators for information security management. The strengthening of e-government procurement systems is guided by the Methodology for Assessing Procurement Systems e-Procurement (E-PROC) module, which provides a harmonized tool for use in the assessment of the electronic procurement ecosystem at the national and subnational levels.

As mentioned earlier, between November 2023 and January 2024, OHCHR analysed a total of 3,450 projects financed by nine of the major MDBs in the above four sectors. The methodology for the project analysis is set out more comprehensively in annex II. The headline findings from the project database analysis are as follows:

- On the basis of publicly disclosed documentation, more attention seems to be given to digital risks in public sector projects compared with private sector projects. However, the very limited information disclosure for private sector projects makes it difficult to be sure.
- In public sector projects, across MDBs and within particular MDBs, there seems to be inconsistency in the degree of attention paid to digital risks. Digital risks are sometimes addressed as operational risks and in other cases as E&S risks. The approach taken by particular MDBs often appears to be driven as much by the discretion of investment team leaders as the consistent application of clear policy.
- Except where physical impacts (such as resettlement) were at issue, the "digital" dimensions of projects did not appear to have an appreciable impact on E&S risk ratings, which is not surprising given that E&S safeguards are only now starting to address a limited range of digital risks. As noted in section A above (and see figure VI), digital projects have routinely been assigned low-risk ratings, triggering less extensive diligence requirements.[203] Alternatively, such projects may not be assigned any E&S risk classification, which, as discussed earlier, was the case for the majority of the projects reviewed.
- Given the relatively limited attention paid to digital risks, with some exceptions, there was correspondingly little discussion of prevention and mitigation measures.

1. PUBLIC ADMINISTRATION SECTOR

Seven of the nine MDBs surveyed for the present report support a broad spectrum of public sector projects, offering various types of financing from direct loans to policy-based lending and advisory services.[204] These projects range from regulatory advice and support for the digitalization of service delivery to supporting entirely new methods of interacting with public services and the wholesale digitalization of public administration (see box 11).

[203] This applies for direct investments and financial institutions where the policy indicates a clear intention to treat all information technology and technology projects as lowest risk. See, for example, the IFC "Guidance Note on Financial Intermediaries" in table 1 (p. 5), which notes that for equity investments in venture capital funds, the fund must screen an investee company involved in non-information-technology-related activities (manufacturing, logistics, agriculture, etc.) against key requirements of the IFC Performance Standards, but for "IT-related activities, the assessment focuses on PS2 (labor and working conditions)". See also DFC, "Environmental and Social Policy and Procedures" (2024), p. 24, which notes that "FIs that invest in tech or tech-enabled investments that do not involve significant physical assets and investments in financial institutions or fund-of-funds," are categorized as FI-C (the lowest risk category).

[204] The exceptions are IFC and IDB Invest, which focus exclusively on financing the private sector. Among the MDBs financing the public sector, only AIIB explicitly states that it does not offer regulatory advice – see AIIB, "Digital Infrastructure Sector Strategy" (2020), p. 6. Bilateral DFIs finance only private sector projects.

Box 11 Examples of types of digital public administration projects

- **Providing regulatory advice** on, for example, e-governance, e-commerce and digital transformation
- **Establishing digital ID systems** to identify citizens or residents
- **Providing digital public services**, such as e-government systems that provide social protection and tax administration services
- **Establishing digital platforms**, such as digital payment e-commerce and e-procurement platforms, and digitalizing public financial management
- **Developing digital tools for the public sector**, such as in relation to digital payments
- **Transforming public databases**, such as in relation to digital censuses, digital cadastres and judicial archives

This subsection provides a more detailed analysis of the potentially profound and pervasive impacts that digital ID and digital public services projects may involve. The analysis of projects in these areas yields the following insights:

- **DFIs are frequently financing projects in countries with weak (if any) legal protections for human rights, including in the digital sphere**, such as in relation to privacy and data protection laws, independent data protection authorities, consumer protection in the digital sphere and citizenship laws. Even where relevant legislation such as a data protection law exists, it may not be properly enforced. A strong data protection regime, involving strong legislation and an effective data protection authority, should be a precondition to the deployment of digital public administration projects. However, this is not sufficient on its own. The risks associated with digital identity systems and many other aspects of DPI systems may be very broad, encompassing not only data protection but issues relating to citizenship and statelessness, discrimination, policing and security services. It may often be the case that the pre-existing regulatory framework will create conditions for human rights abuses to occur in connection with digital projects. This may occur, for example, where pre-existing discrimination and exclusion are tied to the legal and regulatory frameworks governing citizenship and registration, access and eligibility for social programmes, and the rights to privacy and freedom of expression, and create unwarranted distinctions and disparities on the basis of socioeconomic class or caste, ability, age, ethnicity, race, gender and sexual orientation.
- **Many data protection laws and other relevant laws also have national security exemptions that may be very broadly or vaguely worded.** In many contexts, a data protection commissioner may face serious challenges if not outright prohibitions on investigating actions of the military or security services that contravene the right to privacy. The implication is that, however vital a data protection regime may be for the deployment of a digital ID system or other DPI systems, numerous other safeguards may also be necessary, including citizenship laws that are fit for purpose, effective anti-discrimination measures for vulnerable or marginalized populations and appropriate democratic oversight of the military, intelligence and security services.[205] While some DFIs and projects address some

[205] See the series of "SSR Backgrounders" from the Geneva Centre for Security Sector Governance (DCAF) on digitalization and the security services, including Sondra Cheong, "Intelligence oversight in the age of digitalization" (Geneva, 2024).

of these foundational issues and include actions to address them,[206] practice across the board seems inconsistent at best.

- Despite the important work undertaken by various DFIs in connection with the rule of law, civic engagement,[207] accountability and security sector and justice reform, such work does not often appear to be connected directly to digital projects. **Project-level grievance mechanisms are a common focus of support by numerous MDBs in connection with their financed projects**. However, as discussed later in this report, project-level grievance mechanisms, while serving important purposes in relation to more routine complaints, are generally not equipped to address severe digital impacts or systemic issues. Linking digital ID or DPI projects to broader rule of law, justice and security sector reforms appears critical for ensuring effective judicial oversight and safeguarding against human rights abuses.
- In some cases, **DFIs are financing projects in countries where abridgements of the right to privacy and other human rights risks are pervasive**, raising serious risks that these institutions may be inadvertently enabling surveillance, harassment, exclusion and discrimination. This is not to understate the extremely difficult choices that DFIs may face on whether to support digital transformation in countries with authoritarian Governments and poor human rights records. However, these choices are often not addressed in public documentation. There may be limited prevention or mitigation measures to address such concerns if the project goes ahead.
- **Certain projects may have irremediable impacts**, such as those involving the collection of biometric data or the construction of data-heavy digital infrastructures without sufficient safeguards. The long-term consequences and potential for misuse rarely appear to be discussed to any great extent in project documentation, raising questions about whether such projects should be funded at all.

Digital identification

The right to recognition as a person before the law is a human right.[208] Currently, around 850 million people globally lack reliable legal identification. For this reason, SDG Target 16.9 commits States to provide legal identity for all, including birth registration by 2030. Legal identity connects individuals to the Government typically through birth registration and a civil registration and a vital statistics system. This approach is endorsed by the Legal Identity Agenda Task Force, an inter-agency body coordinating efforts to achieve that target.[209]

[206] The World Bank has developed several important and useful tools to assess the ecosystem for developing identification projects, which appear to provide the basis for a broader-based assessment than tools available from other MDBs. However, the extent to which these tools address oversight of intelligence services and their use of data from digital identification is not clear. See World Bank, *ID Enabling Environment Assessment (IDEEA): Guidance Note* (Washington, D.C., 2018); and World Bank, "Guidelines for ID4D Diagnostics" (Washington, D.C., 2018). "ID4D Diagnostics – Country Action" also features country reports using ID4D diagnostics.

[207] See World Bank, "Amplifying People's Voices: Opportunities for Mainstreaming Citizen Engagement through Digital Technologies" (March 2022). Numerous opportunities are addressed in the report, although there does not seem to be any mention of risks in connection with personal data collection or the use of digital technologies to exclude particular population groups or track human rights defenders.

[208] The Universal Declaration of Human Rights, art. 6 (1948) and the International Covenant on Civil and Political Rights, art. 16 (1966) establish the right of everyone to be recognized as a person before the law.

[209] See DESA, *Guidelines on the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems* (United Nations publication, 2023), which states the following: "As reflected in indicator 16.9.1 related to that target, birth registration should be the primary means for the granting of legal identity, and civil registration remains the "gold standard" by which legal identity should be maintained by Member States".

There is no definition of “digital identification” or “digital ID” under international law and programmes vary widely. Digital IDs can be linked to legal identification, although this is not necessarily the case. A digital ID can also be used to determine access to (or exclusion from) a wide range of public services, such as enrolling in school, accessing healthcare and receiving social entitlements, as well as private services such as opening bank accounts and engaging in online transactions.[210] The drive to commercialize identification is sometimes justified by reference to the prospective economic benefits,[211] but the potential negative human rights impacts are less easy to quantify[212] and can have very serious consequences for individuals and groups.

National identification systems that are discriminatory or ineffective may particularly impact individuals that are stateless and exacerbate exclusion from public services. Vulnerable or marginalized population groups, such as women or gender minorities, displaced persons, migrants and nomadic communities, regularly encounter denial of identity documents. Digital ID programmes alone will not address these barriers and without clear and robust preconditions and safeguards may even entrench them.

The United Nations, the World Bank and others have acknowledged the sensitivity of personal information collected through digital ID formats, emphasizing the need for robust data protection, the right to privacy and cybersecurity.[213] The United Nations has characterized privacy in terms of autonomy, choice, personal expression and social identity, and has highlighted the risks to these dimensions where individual consent is lacking and where identification is tied to a unique personal ID number, pooling all personal information in one place.[214] While unique identifiers may aid interoperability across government systems and is an essential building block of DPI, it may be a double-edged sword, exacerbating the risks of surveillance and arbitrary exclusion from social services.

The digital ID system in India, the world’s largest, has received both praise and criticism, offering lessons for other countries.[215] In different parts of the world, identification systems

[210] United Nations Trade and Development, *Digital Identity for Trade and Development: TrainForTrade Case Studies in South-East Asia* (2020).

[211] See, for example, McKinsey Global Institute, *Digital Identification: A Key to Inclusive Growth* (2019), which found that digital identity could potentially generate an average benefit of six per cent of GDP per country. However, some consider that the numbers around GDP growth are speculative and poorly supported.

[212] For a succinct outline of human rights risks pertaining to digital ID projects, see Danish Institute for Human Rights, “Development finance for digitalisation: Human rights risks in sub-Saharan Africa”, table 1, p. 16. There has been extensive academic discussion of digital IDs. See for example, Information Technology for Development, vol. 27, No. 1 (2021) on digital identity for development.

[213] See DESA, *Guidelines on the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems* (United Nations publication, 2023), para. 52. A closer examination of ID4D guidance reveals that, while cybersecurity is recommended, it is not a mandatory component of an identification system support, despite detailed guidance on its implementation. See the World Bank, *ID4D Practitioner’s Guidance* (Washington D.C., 2019), p. 102, which notes the following: “It is recommended that practitioners implement a cybersecurity program to build the capacity of the ID authority to protect its assets and the capacity of the central cybersecurity agency to perform a supportive and enabling role”.

[214] See DESA, *Guidelines on the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems* (United Nations publication, 2023), which notes that “The most common way of sharing information across databases is through a unique personal identifier, as discussed above. While this facilitates data-sharing, it also poses a risk to privacy if individual records are merged across a wide range of registers, leading to the potential to consolidate a complete record of engagements and track transactions” (para. 96). See also Gretchen Bueermann and Giulia Fanti, “Why a ruling on digital ID by Kenya’s High Court has global implications for online privacy”, World Economic Forum, 31 March 2022.

[215] See, for example, Mansi Jaswal, “What are Moody’s concerns about India’s Aadhaar biometric system? 6 points”, mint, 26 September 2023; Jean Drèze and Reetika Khera, “Six types of problems Aadhaar is causing – and safeguards needed immediately”, Scroll.in, 2 January 2022; Dharvi Vaid, “The link between India’s biometric ID scheme and starvation”, DW, 26 March 2021; Rajeswari Rajagopalan, “India’s Cyber Vulnerabilities Grow”, The Diplomat, 6 November 2023; and Access Now, “Busting the Dangerous Myths of Big ID Programs: Cautionary Lessons from India” (2021).

© Adobe Stock/by bonnontawat

have been used for mass surveillance,[216] targeting, profiling and exclusion from services,[217] with a particular impact on stateless populations. The concentration of personal data in one interconnected system not only heightens the risk of identity theft, but may also produce situations where data initially collected for identification are repurposed without consent, broadening access to these databases[218] (a problem known colloquially as "function creep"). The accompanying transactional data, and data matching and mining capabilities, pattern recognition and other functions that are afforded by a centralized system with a search capability and persistent unique identifiers, may also facilitate precisely targeted surveillance capabilities.

The collection of biometric data as the foundation of identification systems has raised significant additional concerns for several reasons.[219] Studies and real-world experience have demonstrated that biometric scanners often fail to work accurately for everyone, particularly people of colour, which is especially problematic when biometric authentication is required to access all government services.[220] The risk of biometric data theft is another major concern, compounded by the growing prevalence of data leaks and breaches.[221] Unlike emails or passwords, biometric traits such as irises and fingerprints cannot be replaced. Consequently, the theft of biometric data can lead to lifelong identity theft and fraud, with no way to fully remediate the harm.[222] Moreover, these programmes frequently rely on private sector, for-profit technologies, which introduces an additional layer of risk, including potential conflicts of interest and vulnerabilities in data security, as well as data sovereignty where the companies

[216] John Thornhill, "India's all-encompassing ID system holds warnings for the rest of the world", *Financial Times*, 11 November 2021.

[217] Privacy International, "The 'Identity Crisis' around the world", 16 September 2023; and Privacy International, "Understanding identity systems part 1: Why ID?", 31 January 2019. See further materials from Privacy International on digital identification.

[218] Center for Human Rights & Global Justice, New York University School of Law, *Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID Rights and Digital ID* (2022). Annex 1 includes a response from the World Bank and suggested corrections in relation to a previous draft.

[219] DESA, *Guidelines on the Legislative Framework for Civil Registration, Vital Statistics and Identity Management* (United Nations publication, 2023), para. 75.

[220] Amiya Bhatia and others, "Without an Aadhaar card nothing could be done": a mixed methods study of biometric identification and birth registration for children in Varanasi, India", *Information Technology for Development*, vol. 27, No. 1 (2021), pp. 129–149.

[221] Matt Burgess, "A Leak of Biometric Police Data is a Sign of Things to Come", Wired, 23 May 2024.

[222] See OHCHR report, *The right to privacy in the digital age* (A/HRC/39/29), para. 14.

are transnational and transferring data across borders. The use of biometric technologies in humanitarian contexts raises particularly pressing concerns given the multiple vulnerabilities experienced by displaced and conflict-affected populations.[223]

Most of the DFIs that provide public sector financing support digital ID and e-government services projects. The World Bank has taken a leading role in this regard through its Identification for Development (ID4D) initiative. This initiative, which is active in nearly 60 countries and is endorsed by over 30 organizations, including ADB and AfDB, advocates for and supports digital ID systems globally.[224] The ID4D initiative has established a set of 10 principles focused on inclusion, design and governance, aimed at ensuring that identification systems are "inclusive, protective of individual rights and data, and designed to support development outcomes."[225] The ID4D initiative also plays a significant role in knowledge-sharing, developing tools and research, and identifying both the benefits and barriers associated with digital ID.[226]

The ID4D initiative principles recognize the potential scale of harms associated with digital ID systems, which may be instantaneous in nature and qualitatively and quantitatively different from impacts associated with paper-based systems.[227] The principles outline what is needed to mitigate these risks: "This requires clearly defining the purposes and intended uses of the system; adopting and resourcing adequate legal and regulatory frameworks that remove barriers to access and provide sufficient safeguards and oversight; implementing inclusive policies and practices for identification system enrolment and use; following a people-centric and data privacy-protecting approach for design and risk assessment; and selecting context-appropriate, equitable, and accessible technologies that ensure the quality, security, and utility of the system now and in the future".[228]

These are all important safeguards,[229] especially in contexts with weak rule of law or authoritarian governance, where critics, journalists, political opposition groups, human rights defenders, ethnic minorities and other groups may face particularly drastic consequences related to privacy breaches and other misuse of their data.[230] The critical issue is whether and how these ID4D principles are integrated into actual projects and what actions are taken when

[223] As noted in a recent review of the use of sensing technologies in DFI projects, the "use of biometric technologies in humanitarian contexts raises additional concerns, especially where the provider of biometric technology is a commercial actor, the implementer is an international organization that is immune from legal challenges in domestic courts, and the subjects of biometric surveillance experience multiple forms of vulnerability". Victoria Adelmant and others, *Digitalization as Development*, p. 28. The breadth of the disclaimers in the World Bank primer on biometrics provides apt warning of the challenges in this area – see: World Bank, *A Primer on Biometrics for ID Systems* (2022).

[224] World Bank, *Putting People at the Center of Digital Public Infrastructure (DPI), Annual Report 2023*, p. iii.

[225] World Bank, "Principles on Identification for Sustainable Development: Toward the Digital Age" (Washington, D.C., 2021), p. 3.

[226] Various tools have been developed by ID4D, including the *ID4D Practitioner's Guide*, "Guidelines for ID4D Diagnostics" and "ID Enabling Environment Assessment (IDEEA)". The AfDB digital strategy emphasizes support for e-government and digital ID programmes to enhance effectiveness, transparency, security, civic accountability and service delivery to citizens. Other DFIs are supporting digital identification projects, but it is not always clear what tools and standards they are using. See, for example, Cloe Otiz de Mendivil and Ariel McCaskie, "How Barbados is Bridging its Digital Infrastructure Gap", IDB Caribbean DEVTrends+, 12 May 2022.

[227] See World Bank, "Principles on Identification for Sustainable Development", p. 7., which notes that "While these risks are present in any identification system, they may be amplified by digitization. With digital technologies, the potential scale and harm of the mismanagement or misuse of personal data are much greater than with paper-based systems."

[228] Ibid., p. 8.

[229] See, for example, World Bank, *Mobilizing Technology for Development*, p. xvi, in which it notes that "Attention to DTT risk is particularly important in Identification for Development systems, which are especially vulnerable to inadvertent data spills or willful misuse".

[230] South African Institute of International Affairs, "Policy briefing 282: Digital identification and biometrics in East Africa: Opportunities and concerns" (2023).

they are absent. As has been observed: "It is not clear how existing normative frameworks, such as the *Principles on Identification for Sustainable Development*, are used, what enforcement mechanisms are in place to ensure compliance, and under what circumstances red lines are drawn due to human rights-related risks or evidence of actual violations".[231] Others have expressed concerns about a lack of transparency, about how the guidance is contextualized, operationalized and enforced in specific contexts, and in relation to the adequacy of evidence, transparency and engagement to explain options and choices being made.[232] The ID4D initiative rightfully identifies international human rights as justification for the programme, but does not appear to rely on human rights factors to justify exclusions from or discontinuation of digital ID systems.[233]

In the following boxes, a small selection of projects involving digital ID from various MDB project databases is highlighted. The selection is only illustrative, not necessarily representative; however, the available project documentation raises questions about the adequacy of the analysis of digital risks, whether proposed prevention and mitigation measures would likely be effective, and in some cases, whether the project should have been supported at all in view of the prevailing contextual risks. As noted above and elaborated in the project examples, OHCHR views strong data protection law, institutions and enforcement as necessary, but not sufficient prevention and mitigation measures; yet they are often the main focus of regulatory analysis and action. The range of harms that may occur through the implementation of digital ID systems requires consideration of a wider range of measures to be put in place prior to the system being rolled out. An analysis of the robustness and rights-compatibility of nationality and citizenship laws should be a routine part of the process, along with an analysis of existing discrimination in access to services. Moreover, as highlighted above, digital ID programmes should be predicated on appropriate democratic oversight, including in relation to military, intelligence and security services.[234] In the view of OHCHR, if functions such as voting and social protection are explicitly invoked as use cases to justify digital ID programmes, the way in which these functions use digital ID should also be legitimately within the scope of the project.

[231] Access Now, "Open letter: World Bank and its donors must protect human rights in digital ID systems", 7 March 2023.

[232] See, for example, David Indeje, "First Public Gathering of New Digital and Human Rights Coalition", KICTANet, 26 February 2024.

[233] See Center for Human Rights & Global Justice, New York University School of Law, *Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID*, p. 58, which notes that "In many ID4D publications, once the benefits have been assumed, the second step is to acknowledge any potential harms as risks and barriers to the system itself. These harms are never presented as reasons not to continue with a digital identification system altogether, merely as factors to inform design and implementation".

[234] See the references in footnote 205.

Box 12 Examples of digital identification projects

- **The AfDB-financed Comorian Economic Digitalization Support Project**, valued at 22.53 million euros, is an initiative to support the digitalization of the Comorian economy and improve the governance, quality, affordability and accessibility of public services.[235] Serious human rights abuses were reported in Comoros during and preceding project appraisal, relevant to the project, including violations of the right to life and freedoms of access to information, expression and assembly, and risks to a wide range of human rights following a post-election Internet shutdown in January 2024.[236] However, E&S risks were rated only as moderate, limited in scope to physical infrastructure risks. The scope of stakeholder engagement was also limited to those who might be impacted by physical infrastructure, rather than users and consumers and those impacted by data protection gaps, exclusion from services and other issues.[237]
- **The AIIB-financed Rwanda Digital Acceleration Project** is aimed at helping to bridge the digital divide in Rwanda. However, it makes only passing mention of privacy and data protection risks, notwithstanding the intention to expand the digital ID project and use biometric ID. While the project documentation notes that the ID4D principles will be applied, no mention is made of contextual risks in Rwanda that may influence the State's use of data collected, including structural discrimination and threats to the right to privacy, freedom of expression and other rights, and restrictions on Internet freedom.[238] Notably, risks relating to data protection, cybersecurity and privacy were rated as "low".[239]
- **IDB provided technical assistance in connection with digital ID and civil registries to different countries in the context of the COVID-19 pandemic.** Project documentation notes that "the one main risk, linked to concerns from civil society, that a strong national identity system may affect the privacy of individuals. Throughout the implementation of the TC, we will heed much attention to avoid this controversy and find the best medium between protection of privacy and promotion of benefit by the identification system".[240] This formulation conveys the unfortunate implication that privacy is viewed mainly as a reputational risk to IDB and that the right to privacy may be offset against other project benefits.

[235] See AfDB, "Comoros: African Development Bank grants over 9 million euros for digitizing the Comorian economy", 30 September 2024.

[236] See Access Now, "#KeepItOn: Comoros must not black out the internet to quell post-election results", 9 January 2024; OHCHR report, *Summary of stakeholders' submissions on the Comoros* (A/HRC/WG.6/46/COM/3); OHCHR, "Comoros: UN Human Rights Chief calls for calm and urges the authorities to protect free assembly, uphold democratic principles", 17 January 2024; and, IDEA, "Comoros-January 2024".

[237] AfDB, "Project Appraisal Report: Comorian Economic Digitalization Support Project" (2024), pp. 11–12.

[238] See Freedom House, "Freedom on the Net – Rwanda"; and Human Rights Watch, "World Report 2022 – Rwanda: Events of 2021".

[239] See AIDB, "Rwanda: Rwanda Digital Acceleration Project (Digital Investment for Recovery, Resilience and Connectivity)".

[240] See IDB, "Promoting Identity Management in LAC for Effective COVID-19 Actions".

- In December 2023, the **World Bank announced its support for the Ethiopia Digital ID for Inclusion and Services Project**, a $350 million initiative with a substantial European Sustainability Reporting Standards rating.[241] The project is also aimed at supporting the integration of digital ID into services in key sectors, such as social protection, financial services, healthcare (including health insurance), agriculture and education.

  In the World Bank Project Appraisal Document, it is noted that Ethiopia did not yet have a data protection law in place, although as of 2023 a draft was under consideration.[242] It was also noted that Ethiopia did not yet have in place adequate data control systems or approaches to sharing data with third parties.[243] Accordingly, one of the project components was designed to support the legal and regulatory preparatory work on digital ID and related topics, such as data protection and privacy, through a comprehensive legal and regulatory framework.

  Despite commitments in the project documentation that the registration process would be voluntary and would not be rolled out fully until the end of 2027, in July 2023, the National Bank of Ethiopia reportedly announced that it intended to make the use of digital ID mandatory for banking operations in Ethiopia by 2024.[244]

  Ethiopia has a long history of digital repression and state surveillance, as well as ethnic profiling.[245] A project report on consultations with vulnerable groups noted that: "Establishing a continuous dialogue between the population and the government is essential to ensure comprehensive representation and consideration of all viewpoints".[246] However, the bitter and protracted civil war in the country raises serious questions about the prospects for such a dialogue. In the E&S documentation, a number of mitigation measures are noted, including the fact that discrimination would be addressed through the non-collection of ethnic data in the national identification database. However, as important a measure as this is, on the face of it, it does not seem to address the risk that ethnicity may be inferred from family names and to some extent addresses and language preference.[247] The financing agreement ultimately contained disbursement conditions preventing the release of funds for data services and establishing a Data Protection Commission until the Personal Data Protection Proclamation had been ratified by parliament.[248]

[241] See World Bank, "World Bank Supports Ethiopia's Digital ID Project to Increase Access to Services and Economic Opportunities", 13 December 2023 and "Ethiopia Digital ID for Inclusion and Services Project".

[242] World Bank, "Ethiopia – Digital ID for Inclusion and Services Project" report, pp. 5–6. By way of comparison, the High Court of Kenya invalidated the application of the digital identification system in Kenya in the absence of an applicable data protection law. See Danish Institute for Human Rights, "Development finance for digitalisation: Human rights risks in sub-Saharan Africa", p. 14, and Privacy International, "Data Protection Impact Assessments and ID Systems: the 2021 Kenyan ruling on Huduma Namba", 27 January 2022.

[243] World Bank, "End-user Perspectives on Fayda ID from Marginalized and Vulnerable Groups" (Washington, D.C., 2024), pp. 20–21.

[244] Josh Einis, "Ethiopia to Mandate Digital ID for Banking Operations", *Payments Journal*, 14 July 2023.

[245] Freedom House rates Ethiopia as "not free" across its global freedom scores and Internet freedom scores. See Freedom House, "Freedom in the world 2025: the uphill battle to safeguard rights" (2023) and "Freedom on the Net 2024 – Ethiopia". Ethiopia is ranked 129th across 142 countries in the 2023 World Justice Project Rule of Law Index. See also Kebene Wodajo, "Digitalizing Identity: Precautionary Thoughts on Ethiopia's "Fayda" Number", OpinioJuris, 2 October 2022; and International Crisis Group, "Ethiopia's Ominous New War in Amhara", 16 November 2023. Telecommunications services have been suspended in the Tigray area of Ethiopia ever since the civil war broke out on 4 November 2020. The inhabitants of Tigray had experienced a complete communications blackout for 787 days by the time a peace accord between the Government of Ethiopia and the Tigray inhabitants' Liberation Front started to take effect at the end of 2022. At the time, this was the longest continuous shutdown of its kind (see Carolyn Tackett and Felicia, "After years in the dark, Tigray is slowly coming back online", Access Now, 17 March 2023; and Zecharias Zelalem, "Six million silenced: a two-year internet outage in Ethiopia", Context, 29 September 2022). See salso OHCHR, "Update on the human rights situation in Ethiopia in 2023" (June 2024).

[246] World Bank, "End-user Perspectives on Fayda ID from Marginalized and Vulnerable Groups", p. 24.

[247] Kebene Wodajo, "Digitalizing Identity: Precautionary Thoughts on Ethiopia's "Fayda" Number", OpinioJuris, 2 October 2022.

[248] World Bank, "Financing Agreement (Ethiopia Digital ID for Inclusion and Services Project)" (December 2023), schedule 2, sect. III (B) (1) (b). The events of suspension under article 4.01 of the financing agreement included a failure by the Government of Ethiopia to establish the Digital Identification Institution and Data Protection Commission foreseen by the Personal Data Protection Proclamation, within two and three years of project effectiveness, respectively.

The Proclamation came into effect in April 2024; however, the national context appears to raise serious questions about the prospects for its implementation.[249]

- **The World Bank Burundi Digital Foundation Project** is aimed at increasing connectivity and access to e-services, including establishing an identification programme. It includes advice on establishing the appropriate regulatory framework on identification, data protection and cybersecurity.[250]

  Positively, the World Bank Project Appraisal Document notes that "international best practices and standards in cybersecurity and data protection will also be embedded in technical specifications when procuring hardware or software through the project", although the applicable standards are not specified.[251] Selected digital risks (digital exclusion, content and data protection and privacy) are considered under "social" risks but are rated as only moderate, notwithstanding the challenging human rights context,[252] and in any case do not appear to be reflected in the applicable financing agreements[253] or subject to any mitigation measures in the project's E&S commitment plan.[254]

  The World Bank Project Appraisal Document worryingly notes that even with data protection and cybersecurity protections, "systems cannot be fully protected, which means that related residual risk remains substantial".[255] Prospects for remedying residual impacts seem to depend on a project-level grievance mechanism, which, as of May 2024, had yet to be established.[256]

  The Additional Financing Agreement contains a requirement that, no later than two years after project effectiveness, and prior to rolling out the biometric census and identification system, the Government of Burundi shall "develop a data protection legal framework and establish and operationalize an independent data protection authority".[257] However, there was no disbursement condition to this effect and given the national context, there are serious questions relating to how a data protection law and authority would function in practice.[258] In any case, it would not address more fundamental concerns relating to citizenship rights, surveillance and policing.

[249] See the references in footnote 245, and Oded Yaron, "Ethiopia Obtains Phone-Hacking Tech from Israeli Firm Cellebrite", Haaretz, 18 December 2022.

[250] World Bank, *Burundi – Digital Foundations Project* (Washington, D.C., 2022). While project stakeholders would not usually be expected to access or comprehend its contents, the financing agreement includes the dispositive description of the project components and the steps that are expected to be implemented: World Bank, "Financing Agreement and Agreement to the Original Financing Agreement: Additional Financing for the Burundi Digital Foundations Project – Modernization of Public Financial Management" (2022).

[251] World Bank, "Financing Agreement and Agreement to the Original Financing Agreement: Additional Financing for the Burundi Digital Foundations Project – Modernization of Public Financial Management" (2022), p. 42.

[252] See OHCHR, "Oral briefing of the Commission of Inquiry on Burundi", 23 September 2021. See also Human Rights Watch, "Burundi: Entrenched Repression of Civil Society, Media", 26 May 2024; and Access Now, "Access urges UN and African Union experts to take action on Burundi internet shutdown", 13 January 2023.

[253] See World Bank, "Official Documents – Financing Agreement for Grant Number E0930-BI" (Washington, D.C., 2022), and World Bank, "Financing Agreement and Agreement to the Original Financing Agreement: Additional Financing for the Burundi Digital Foundations Project – Modernization of Public Financial Management" (2022).

[254] World Bank, "Additional Financing Environmental and Social Commitment Plan (ESCP) – Digital Burundi Additional Financing – Modernization of Public Financial Management – P180987" (Washington, D.C., 2023).

[255] World Bank, *Burundi – Digital Foundations Project* (Washington, D.C., 2022), p. 42.

[256] World Bank, "Burundi Digital Foundations Project (P176396): Implementation Status and Results Report" (Washington, D.C., 2024), p. 7.

[257] See World Bank, "Financing Agreement and Agreement to the Original Financing Agreement: Additional Financing for the Burundi Digital Foundations Project – Modernization of Public Financial Management" (2022), schedule 2, sect. IV.

[258] See, for example, *Report of the Commission of Inquiry on Burundi* (A/HRC/48/68); Human Rights Watch, "Burundi: Events of 2023"; *Burundi: Compilation of information prepared by the Office of the United Nations High Commissioner for Human Rights* (A/HRC/WG.6/43/BDI/2); and OHCHR report, *Summary of stakeholders' submissions on Burundi* (A/HRC/WG.6/43/BDI/3).

© Adobe Stock/Generative AI/by bihanc

Box 13 Example of a biometric data collection project

In 2018, **IFC** invested $700,000 in a biometric technology company called **IrisGuard** in order to scale up its iris-based e-payment solution designed for refugees. The goal was to enhance financial inclusion and improve the lives of Syrian refugees in Jordan and the surrounding region. The investment was aimed at supporting IrisGuard in expanding its business model by identifying new products and partnerships, and to help the United Nations High Commissioner for Refugees (UNHCR) and the World Food Programme (WFP) to register refugee populations.

However, the publicly available information on this investment from IFC is limited only to a brief project description and a standard statement relating to its E&S safeguards. There is no mention of privacy concerns or data protection, despite the highly sensitive biometric data handled by IrisGuard.[259] At the time of the investment, there were growing concerns about the use of biometric data in humanitarian contexts.[260]

In such circumstances, robust risk mitigation and data protection measures would seem to be called for. However, at the time of writing, the privacy notice on the IrisGuard website still lacked details on how it manages and protects data collected from its products or how it transfers biometric data to third parties.[261] Since the investment, there have been growing concerns about the sharing of sensitive refugee data without adequate consent, as refugees, because of their situation, have limited alternative but to consent during data collection, which may amount to consent under duress.[262]

[259] See IFC, Project Information & Data Portal, "IrisGuard AS".

[260] See, for example, Paul Currion, "Eyes wide shut: The challenge of humanitarian biometrics", *The New Humanitarian*, 26 August 2015.

[261] See IrisGuard UK Ltd, "Website Privacy Notice".

[262] See Access Now, "Iris scanning of refugees is disproportionate and dangerous – what's happening behind IrisGuard's closed doors?", 26 January 2023; and Nazih Osseiran, "In Jordan, refugees scan irises to collect aid. But is it ethical?", Reuters, 13 December 2022.

Digital public services

Governments are increasingly delivering public services digitally and using digital ID to help determine eligibility for various benefits. These benefits may include social protection programmes, such as cash and food assistance, access to school meals,[263] education support, subsidized medical care, disability benefits and housing and job allocation. The digitalization of these services offers numerous advantages, including speed, efficiency and streamlined delivery, which can enhance coverage and strengthen emergency protection systems. The COVID-19 pandemic accelerated many of these transitions. As Governments rely more and more on decision-making assistance from digital technologies to determine who receives public services, the details of the design and use of these digital systems need to be better understood. Baseline studies and rigorous ongoing monitoring are needed in order to help understand the scale of potential exclusion. While digital systems can improve the inclusion of recipients, errors in their application can deny people access to essential services. Even in countries with advanced digital capabilities, there have been well-documented instances where such errors have had severe consequences.

As discussed earlier, DFIs are playing a growing role in helping Governments to integrate digital ID with payment systems, data exchange and services, under the auspices of DPI.[264] In addition to DFIs, organizations and entities such the United Nations, the Group of 20, the Group of Seven and OECD are actively shaping DPI. At the time of writing, a multi-stakeholder group to develop a universal safeguards framework for DPI was being convened by the United Nations.[265]

All DFIs that provide public sector support are involved in financing and technical assistance for various digital public services. A number of risks are commonly identified in this context, such as the exclusion from services, discrimination from biased algorithms (especially in relation to AI) and cybersecurity threats. However, analysis of the broader consequences of these systems is often missing. The possible consequences include harms arising from the accumulation of sensitive personal data, data leaks, unauthorized data sales, the use of data for monitoring and manipulation,[266] intentional exclusion, arbitrary surveillance and the profiling of those seeking assistance. Several of these issues have been highlighted by human rights organizations in investigations of digital public service projects (see box 14).

[263] Association for Progressive Communication, "Extreme poverty and digital welfare: New report from UN Special Rapporteur on extreme poverty raises alarm about the rise of a digital welfare dystopia", 10 July 2024.

[264] World Bank, "A Digital Stack for Transforming Service Delivery: ID-Payments and Data Sharing" (2022). See also World Bank-IDB, "Unlocking the potential of digital public infrastructure (DPI) in Latin America and the Caribbean: a region-specific perspective" (2024).

[265] United Nations, "UN Tech Envoy and UNDP launch initiative to ensure that digital infrastructure turbocharges the SDGs safely and inclusively", 17 September 2023.

[266] OECD, *Development Co-operation Report 2021*, p. 34.

Box 14 Human rights analyses of DFI-funded digital public services

Privacy International reviewed a number of social safety-net projects that involved increasing integration of technological and data-intensive solutions financed by the World Bank during the COVID-19 pandemic. The purpose was to inform the World Bank's future implementation of these kinds of projects, reflecting on how certain aspects of social protection projects can inadvertently lead to excessive surveillance of marginalized communities, impact equal access to urgent social protection disbursements and interfere with people's dignity and right to privacy.[267]

Human Rights Watch carried out a detailed review of the World Bank's financing of a cash transfer programme in Jordan that relied on targeting algorithms and the use of social registries, systems that enable the collection and analysis of large amounts of personal data to determine eligibility for social assistance programmes. The report also included brief reviews of similar poverty-targeting programmes in other countries in the Middle East and North Africa. In the report, concerns were highlighted about forms of automation that exclude people from services or that single them out for investigation based on errors, discriminatory criteria or stereotypes about poverty. It was also noted in the report that despite these harms, the allure of technology-based solutions to complex social problems is proving hard to resist.[268]

In addition to design concerns, digital public service systems are inherently complex to establish and implement, as reflected in the multifaceted activities detailed in project appraisal documents. As a result of their complexity, adjustments to the systems may be needed post-implementation to ensure that affected populations are not unintentionally (or intentionally) prevented from accessing services. And while clients are typically required to establish grievance mechanisms for addressing project-related concerns, the effectiveness of these mechanisms in addressing these kinds of more systemic issues in digital public services is questionable. These issues may include unauthorized use of sensitive personal data, data leaks, algorithmic bias, inaccurate registry data, weak enforcement of data protection laws, lack of transparency in automated eligibility criteria and the absence of non-digital alternatives for accessing social safety-net payments.[269] Experience in resolving such concerns has been mixed (see box 14). These systems should be anchored in law, with effective remedies that are integrated with existing administrative and judicial review practices, along with legal aid. This underscores the need for robust and independent administrative and judicial oversight and due process protections, which should be core components of all digital public service projects in the view of OHCHR.

In the following box, a selection of projects involving digital public services taken from various MDB project databases is presented. They raise similar concerns to those arising in digital ID projects: the existence or adequacy of contextual risk analysis, the adequacy of the discussion in project documentation of digital risk assessment and management,

[267] Privacy International, "The World Bank & social protection during crises: a privacy trade-off?", 22 August 2022.

[268] See Human Rights Watch, *Automated Neglect: How the World Bank's Push to Allocate Cash Assistance Using Algorithms Threatens Rights* (2023) (see the response from the World Bank, pp. 156–163), and also Stephen Kidd and others, "Social registries: a short history of abject failure", Working Paper (2021), co-published by Development Pathways and Act Church of Sweden.

[269] See Privacy International, "The World Bank & social protection during crises: a privacy trade-off?".

the adequacy of the proposed mitigation measures and the apparent failure to adequately consider project alternatives including the no-project scenario.

Box 15 Examples of digital public services projects

The ADB Bangladesh Strengthening Social Resilience Program is aimed at supporting the Government of Bangladesh in consolidating over 100 different social protection programmes delivered to the most vulnerable, including developing an integrated social protection digital registry using management information systems. Despite the wide scope and potential systemic impacts of this project, there is no reference to concerns related to data protection, privacy, cybersecurity or misuse of data. The project does address exclusion, but only in the context of financial inclusion approaches.[270]

The Digital Cambodia Advisory Project financed by ADB is aimed at providing knowledge and technical assistance to the Government of Cambodia in order to develop and implement a one-stop shop model for decentralized service delivery using a digital platform that is integrated with the national identification system.[271] Project documents note that the "key barriers to achieving digital transformation in Cambodia are (a) gaps in supporting infrastructure; (b) weak governance and institutional capacity to implement the digital transformation; and (c) limited awareness and knowledge of, and human capacity for, digital technology". However, publicly available project documents contain no mention of safeguards pertaining to such issues, and there is no reference to data protection, privacy, accountability or any of the other concerns covered by the ID4D principles.

The AfDB-financed Digitization of Government Payments in Mano River Union Programme is aimed at establishing a digital payment ecosystem and creating an enabling environment for the mass digitization of all types of payments (Government to person (G2P) and person to Government (P2G)).[272] The regional project does not address key risks related to the establishment and use of identification systems. There is no discussion of whether the countries have data protection or other necessary legislation in place.

The Barbados Digital Government Project, financed by IDB, is aimed at increasing the adoption of digital channels in order to improve access to public services by individuals and businesses. Data protection is mentioned only in a footnote, noting that the country has an existing data protection law. However, there were no actions to review the adequacy of the law, in its formulation or implementation, or any other mention of digital risks. The project was rated category C (low risk).[273]

The Bangladesh Enhancing Digital Government and Economy Project, financed by the World Bank, is aimed at supporting the Government of Bangladesh in establishing an integrated cloud-computing platform for use by any government agency to build, operate and maintain its sector-specific systems, applications and public services.[274] The project appraisal document notes that the Government of Bangladesh has sought to digitalize government and public services since 2009 and has made its Digital Bangladesh programme integral to its overall economic development strategy.

[270] See ADB, "Bangladesh: Strengthening Social Resilience Program (Subprogram 1)".

[271] ADB, "Technical Assistance Report: Kingdom of Cambodia: Supporting the Implementation of Cambodia Digital Government Programs at Subnational Administrations" (2024).

[272] See AfDB, "Multinational – Project for Digitization of Government Payments in the Mano River Union (MRU) – Project Appraisal Report (P-Z1-HB0-064)".

[273] IDB, "Barbados Public Sector Modernization Programme (BA-L1046)" (2019).

[274] World Bank, "Bangladesh: Enhancing Digital Government and Economy Project" (Washington, D.C., 2020).

The World Bank has been involved in earlier digital transformation programmes with the Government of Bangladesh, including digital identification. Despite this, the project appraisal document notes that the Government still did not have a data protection law in place and, moreover, that the law governing the use of identification systems, including on data collection, needed to be updated as part of the current project.[275] The project was assigned a "high" risk rating because of the need to update government policies, laws and strategies for transforming digital government.[276]

Despite the high risk, the wide scope and the potential systemic impacts of the project, there is no further discussion in the project appraisal document of risks for Bangladeshi citizens or others who may be excluded from government services as a result of digitalization. Even with a high-risk rating, the E&S safeguard review concludes that "the Project does not present any significant adverse social issues according to the WB safeguard policies and procedures",[277] which underscores the disconnect between E&S safeguards and digital risk management demands in these kinds of projects. The project appraisal document indicates that the project will provide support to the Government on regulatory reforms and that the World Bank would introduce a legal covenant and disbursement condition to mitigate the privacy risks associated with the potential misuse of personal data.[278] The Financing Agreement ultimately required the preparation and delivery of an expert report to the Minister for Information and Communication Technology, within 24 months of project effectiveness, on the policy, legal and regulatory framework on data protection and privacy issues. The disbursement condition for part two of the loan agreement was that the Government prepare a digital government operations manual satisfactory to the World Bank.[279]

2. FINANCIAL SECTOR

Access to affordable financial services is essential for poverty reduction and economic growth. Digital financial services play an increasingly crucial role in expanding access, reducing transaction costs and enhancing financial inclusion. The digital financial services transformation encompasses the digitalization of traditional financial services, the emergence of a whole new range of companies specialized in digitally facilitating financial services (fintech),[280] from small to large, and big tech firms moving into digital finance.

[275] World Bank, "Independent Evaluation Group (IEG): BD: IDEA project (P121528)" (2019): "A total of 40.39 million citizens had access to secure and reliable means of identification, with their NID cards personalized by the project closing date, representing only 50.5 per cent of the target of 80 million citizens" (p. 6). The implementation completion review further found that "the appropriate lesson should be that legislative actions must be planned for deep in advance of project approval or effectivity" (p. 17). Independent Evaluation Group (IEG) World Bank Group, "Implementation Completion Report (ICR) Review, Bangladesh IDEA Project (P121528)" (2019), p. 17.

[276] World Bank, "Bangladesh: Enhancing Digital Government and Economy Project", pp. 5 and 24.

[277] Ibid., p. 2.

[278] Ibid., p. 25.

[279] World Bank, "Official Documents – Financing Agreement for Credit No. 6675-BD" (2022), schedule 2, section III (b) (1) (b).

[280] Fintech activities include payments, lending, credit scoring, insurance, investments and cryptocurrency operations.

While digital financial services increase customer access, significant challenges persist, including for offline populations whose access may in fact diminish as a result. Those who can access digital financial services may face new risks, such as the expansion of data acquisition and retention without sufficient clarification and consent,[281] data misuse, profiling,[282] cybersecurity breaches,[283] discrimination by proxy and fraudulent extortion. Predatory practices targeting vulnerable individuals may exacerbate financial vulnerability and debt stress. The extensive data surveillance and integrated ecosystems of big tech can intensify these risks,[284] potentially amplifying existing discriminatory and extractive practices.

AI increases both the opportunities and risks of digital financial services.[285] It can enhance efficiency, reduce costs, enable innovative products and improve credit access for underserved individuals and businesses.[286] However, discriminatory algorithms may disproportionately harm marginalized consumers.[287] Datasets used to train AI, often based on developed markets, may not accurately reflect emerging market contexts, leading to errors and exclusions,[288] while alternative credit assessment processes require attention to ethical data handling and privacy.[289] The absence of regulation that would apply to the use of AI in many regions also raises concerns about whether emerging fintech companies will prioritize equitable AI practices,[290] the lack of which may lead to increased indebtedness and burden people with repayment obligations they would not otherwise have taken on. With pressures to demonstrate quick profitability, there is a risk that consumer protections, particularly for women, low-income individuals and other marginalized or vulnerable groups, may be overlooked unless and until DFIs and investors require otherwise.[291]

[281] Privacy International, "Fintech: Privacy and Identity in the New Data-Intensive Financial Sector", 1 December 2017.

[282] Financial organizations may employ algorithms and data analysis to create customer profiles for marketing or risk assessment. However, this can lead to concerns about intrusive profiling and loss of privacy. See OECD International Network for Financial Education, "Digitalisation of Consumer Finance and Financial Education in South East Europe Policy Brief" (2021).

[283] Digital finance systems are susceptible to cyberattacks, data breaches and fraud, which can lead to financial losses and data exposure. ADB Briefs, "Managing fintech risks: policy and regulatory implications" (2023).

[284] Myriam Vander Stichele, "Fintech's red flags", SOMO, 27 March 2023.

[285] Cambridge Centre for Alternative Finance and World Economic Forum, "Transforming Paradigms: A Global AI in Financial Services Survey", *SSRN Electronic Journal* (2020).

[286] See FinRegLab, *Explainability & Fairness in Machine Learning for Credit Underwriting: Policy & Empirical Findings Overview* (2023); and Ana Cristina Bicharra Garcia and others, "Algorithmic discrimination in the credit domain: what do we know about it?", *AI & Society*, vol. 39 (2024), pp. 2059–2098, in which it is noted that "Researchers are still only dealing with direct discrimination, addressed by algorithmic fairness, while indirect discrimination (structural discrimination) has not received the same attention".

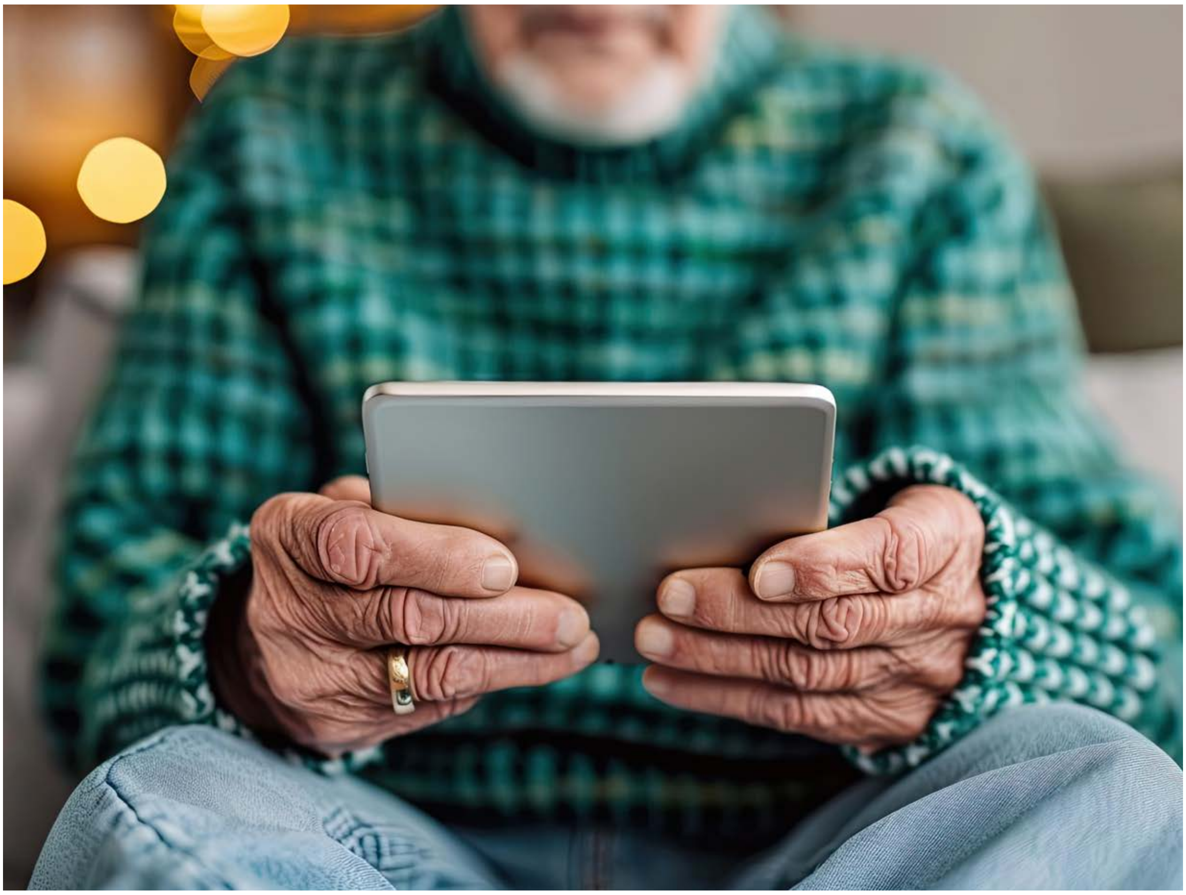
[287] Algorithms and automated processes in digital finance can perpetuate biases and discriminate against certain individuals or groups, potentially infringing on the right to non-discrimination. Aleksandr Alekseenko, "Privacy, data protection, and public interest considerations for fintech" in *Global Perspectives in FinTech*, Hung-Yi Chen, Pawee Jenweeranon and Nafis Alam, eds. (Palgrave McMillan, 2022).

[288] Center for Financial Inclusion, *Investing in Equitable AI for Inclusive Finance: A Risk Management Guide for Impact Investors* (2023), p. 6.

[289] Privacy International, "Fintech: Privacy and Identity in the New Data-Intensive Financial Sector"; and Keoitshepile Machikape and Deborah Oluwadele, "Advancing Financial Inclusion and Data Ethics: The Role of Alternative Credit Scoring", in *Society 5.0*, Knut Hinkelmann and Hanlie Smuts, eds. (2024), pp. 229–241.

[290] Center for Financial Inclusion, "Investing in Equitable AI for Inclusive Finance", p. 3.

[291] Center for Financial Inclusion, "Shaping a Responsible Digital Finance Ecosystem" (2023), p. 8.



© Adobe Stock/Generative AI/by Sumet

DFI approaches to addressing digital risks in digital financial services

DFIs support a broad spectrum of finance projects in both the public and private sectors. Examples include providing policy and regulatory advice, strengthening public institutions to regulate digital transformations, supporting digital transformations of financial institutions, supporting the uptake of particular financing functions such as digital payments and credit systems, supporting financial inclusion projects focused on various segments of the market, supporting digital financial services for MSMEs through a variety of types of financial institutions and vehicles, and providing venture capital funding and investment to support innovative fintech start-ups and digital innovation.

DFIs entering the digital financial services sector face a rapidly evolving landscape of technological advancements where regulation often lags well behind the rapid pace of such developments, leaving potentially significant gaps in identifying and addressing risks, such as those identified earlier in this report. Governments are often cautious about implementing regulatory frameworks that they perceive might hinder innovation and may struggle to keep up with the complexities of digital finance.[292]

[292] Myriam Vander Stichele, "Fintech's red flags", SOMO, 27 March 2023.

Box 16 Overview of DFI approaches to digital financial services

Few DFIs appear to have addressed the risks associated with digital financial services in their published strategies or approaches, although a focus on increased consumer protection is noted in good practice guidance published by FMO and the Commonwealth Development Corporation (now known as BII) on a few digital risks in early-stage venture capital investments.[293]

- **ADB** assists its government members through technical assistance and policy advice. The Bank helps Governments build regulatory and supervisory frameworks to balance consumer protection and market innovation in relation to digital lending and investment platforms. Key focus areas include financial accounting and reporting systems, professional codes of conduct for market intermediaries and enhancing financial literacy for investors.[294]
- **AfDB** manages the Africa Digital Financial Inclusion Facility.[295] However, it does not focus on the financial sector in its public sector financing[296] and does not specifically address digital transformations in its private sector financial institutions work.[297]
- **AIIB** does not appear to focus on the financial sector or digital financial services.[298]
- **EBRD** has limited emphasis on digital financial services within its financial sector focus.[299]
- The nine focus areas of **EIB** do not include the financial sector.[300]
- **IDB** does not list digital financial services among its current focus areas for its finance work.[301]
- **IDB Invest** has stated that it invests in digital transformation and innovation to achieve greater operational efficiencies in the finance sector.[302]
- The focus of **IFC** on digital financial services has shifted over time as the market has matured and innovation accelerated. IFC has stated that it is supporting "(a) data analytics, leveraging AI and machine learning to develop a more targeted product offering for financially excluded and underserved; (b) process digitization to make FSPs [financial service providers] more efficient and enhance customer experience; and (c) increased consumer protection both with regard to fair and transparent products offers and data protection".[303]

[293] CDC and FMO, "Responsible venture capital: Integrating environmental and social approaches in early-stage investing" (2020).

[294] ADB, *Strategy 2030 Finance Sector Directional Guide: Innovative and Sustainable Finance for Asia and the Pacific* (2022), p. 37.

[295] See AfDB, "African Development Bank provides $1 million for AI-based national customer management systems in Ghana, Rwanda and Zambia", 10 March 2021.

[296] See AfDB, "Sectors".

[297] See AfDB, "Financial Institutions".

[298] See AIIB, "Who we are".

[299] EBRD, *Financial Sector Strategy 2021–2025* (2021).

[300] See EIB, "What we do".

[301] See IDB, "Financial Markets".

[302] See IDB Invest, "Financial Institutions".

[303] See IFC, "Digital Finance" and on its venture capital funding, see "Disruptive Technologies and Venture Capital". See also IFC, "Tech Emerge".

- The **World Bank** notes that in 2020 it was actively working on digital financial services in over 50 countries, through both lending and advisory instruments, on a wide range of digital financial service activities, including from digital identification to payments, banking regulation and digitizing government-to-person payments.[304]
- The **BII** Environmental, Social and Governance Toolkit includes guidance and resources for addressing environmental, social and governance risks in venture capital investments, including digital risks.[305] In its good practice note on E&S approaches in early-stage investing, a section on data privacy, ethical use of data and data security is included.[306]
- **FMO** supports innovation through the promotion and support of fintech and agribusiness.[307]

Based on research undertaken by OHCHR for this report, there seems to be broad awareness among major DFIs of the kinds of risks that may arise in connection with digital financial services and the mitigation measures that may be necessary. However, this awareness does not seem to be consistently reflected in risk management practice in DFI-financed projects (see boxes 17 and 18). The obligation to address risks should be proportionate to the level of risk of the use of AI or other digital technologies, not the size of the provider. Therefore, even small and emerging fintechs supported by DFIs should be expected to be able to address these risks effectively. Given the significant role of DFIs in promoting financial inclusion and supporting small and medium-sized enterprises (SMEs), their approach to managing emerging risks is crucial.

Box 17 Addressing fintech risks

The ADB brief, entitled “Managing fintech risks: policy and regulatory implications”, outlines a number of concerns in relation to financial risks, operational risks, cybersecurity risks and risks to consumers.[308] Proposed responses to consumer risks include the following:

- **Improving data privacy and protection** laws and implementing regulations as applicable to the digital financial services industry, including fintechs.
- **Secure handling and collection of data** utilizing secure protocols (https) while ensuring the transmission and storage of data in encrypted formats. Data should be stored only long enough to satisfy a legitimate business or legal requirement.
- **Informed customer consent**, with clear and simple language about what financial, personal or transactional data are being collected and how the data will be used or shared, with an option to consent or not.

[304] World Bank, *Digital Financial Services* (2020), p. vii.

[305] See BII, “ESG Toolkit for Fund Managers”.

[306] CDC and FMO, “Responsible venture capital: Integrating environmental and social approaches in early-stage investing”.

[307] FMO, “Position statement on impact and ESG and financial intermediaries” (2022), p. 6.

[308] See ADB, “ADB Briefs: Managing fintech risks: policy and regulatory implications” (May 2023); and World Bank, *Consumer Risks in Fintech: New Manifestations of Consumer Risks and Emerging Regulatory Approaches* (April 2021).

- **Awareness of consequences.** Clients need to know about the data trails and transaction histories they create through digital activity, including the potential impact on credit scores, and should have the right to correct errors.
- **Proper internal processes to prevent misuse.**
- **Management and controls for third-party providers** should be the responsibility of the financial services provider. These include lead generators, brokers, agents and data analytic firms. The regulator ensures that outsourcing agreements cover data privacy, use and protection.
- **The use of general data ethics principles**, such as fairness, data minimization, transparency and non-discrimination, can also be operationalized through algorithmic auditing.

In the following boxes, a short selection of MDB projects involving digital financial services, taken from MDB project databases, is provided. The cases are only illustrative, and not necessarily representative; however, they raise questions about the extent to which digital risks of the kind discussed above are identified and managed in practice.

Box 18 Examples of digital financial services projects

- **Policy and regulatory advice.** Some DFIs provide technical assistance for financial sector policy and regulatory reforms aimed at promoting digital financial services and enhancing regulatory oversight. However, project documentation often reveals relatively little discussion of digital risk management measures.[309]
- **Digital transformation of financial services.** Key aspects of digital transformation, including cybersecurity, data protection and data collection, should be central to financial services projects. However, with some exceptions,[310] these aspects are often not highlighted in project summaries.[311]

[309] See, for example, ADB, "Mongolia: Strengthening Banking Sector Stability and Performance", and ADB, "Developing Financial Technology Legal and Regulatory Frameworks for Mongolia", where there is more focus on addressing risks; ADB, "Developing Digital Financial Infrastructure and Enhancing Financial Access for Resilience and Recovery in Asia and the Pacific"; ADB, "REG: Impact Evaluation of Financial Technology Innovations in Selected Developing Member Countries"; ADB, "Improving Finance Sector Know Your Customer Capacity in the Pacific"; World Bank, "Project Information Document (PID) – SADC Transfers Cleared on an Immediate Basis (TCIB) Payment Scheme Project – P176529", which highlights the need for the "protection of identity and personal information … due to potential cyber fraud as part of the E&S risks to be addressed". See also IFC Project Information & Data Portal, "Tunisia Digital Payments Ecosystem Support, 605560, Advisory Services"; and IDB, "Strengthening the Institutional Network of Development Finance Institutions in Brazil for a Digital, Inclusive, Diverse, and Sustainable Recovery".

[310] See IFC Project Information and Data Portal, "Summary of Investment Information: Global Digital Finance Center", which supports the development of a personal data governance guideline for Chinese financial institutions, including support to a pilot. The Global Digital Finance Center is a collaboration between the World Bank and the National Internet Finance Association of China, a self-regulatory organization under the supervision of the State-owned People's Bank of China.

[311] For example, see "IFC Digilab Finance ECA".

- **Financing and advisory services for sensitive financial services.** Even when supporting financial institutions with new credit scoring methods that use personal data or involve potentially discriminatory practices, risks are often not flagged in project documentation.[312]
- **Fintech.** It is expected that project summaries should cover both opportunities and digital risks. However, this rarely seems to be the case. In project summaries, frequently very little information on risks or how they will be managed is disclosed.[313]
- **Funds with a digital innovation focus or component.** Investing in funds that support digital innovations should ensure that asset managers implement digital risk screening and mitigation measures. However, many disclosed documents either completely lack consideration of digital risks or address them only superficially. Investments are often classified as low risk,[314] even for funds involved in AI, big data or educational technology, which have relatively clear risk profiles.[315]
- **Venture capital relating to digital innovations.** DFIs investing in cutting-edge digital finance technology often fail to highlight digital risks or detail prevention and mitigation measures in project summaries.[316] Others identify performance standard issues on labour, but fail to address other risks such as privacy and cybersecurity.[317] Others involving early stage funding for investments including AI and digital-twin technology, AI-based diagnostics and cell/gene therapy are rated as low to medium.[318]
- **Digital banking, such as digital lending platforms and digital payments.** It should be expected that digital banking projects include the consideration of risks such as cybersecurity, data protection, algorithmic fairness in credit scoring and equitable access to finance. However, project documentation often provides limited or minimal coverage of these risks.[319] There also seems to be little discussion of business model risks, in particular whether the business model in question may exacerbate indebtedness.[320]

[312] See, for example, IFC, "Piloting Psychometric Scoring to increase MSME Access to Finance in Senegal and UEMOA"; ADB, "India: Administration of Equity Investment in Satsure Analytics India Private Limited"; IDB Invest, "Social Bond of Diversity and Inclusion – Cooperativa Jardín Azuayo"; and the "IFC Project Information & Data Portal – project disclosures". On the latter project see also Peter Wintermaier, "Kreditech: Loans based on Facebook posts?" Digital Initiative, 12 November 2019, which notes: "One of the major challenges for the company has been the concern about privacy. Essentially, the would-be borrower needs to give Kreditech full access to any online activity without exactly knowing how these datapoints act in conjunction and how the machine learning algorithm makes sense of them. The black-box character of Kreditech's algorithm, which makes credit decisions without obvious causal relationships, still feels odd for consumers. Even the company's experts cannot always explain how the algorithm arrives at the conclusion. This is one of the reasons why Kreditech, as a German company, headquartered in Germany, has still not penetrated the German market, which is particularly cautious about privacy protection. Instead, the company focuses on developing nations where customers have even fewer alternatives".

[313] See, for example, EBRD, "FIF – Go Digital Pilot in BiH – ProCredit Bank II"; and IDB Invest, "Victory Park Capital".

[314] See, for example, EIB, "Seedstars Africa Ventures 1"; EIB "Future Tech (INVESTEU VD) PL"; EBRD "Early-Stage Innovation Facility II"; IDB Invest "Amadeus LAC Sustainable Growth Fund"; IFC Project Information & Data Portal, "Convergence II"; EBRD, "Earlybird Digital East Fund II"; and ADB, "Regional: Investment in Northstar Equity Partners V Limited".

[315] See, for example, IFC Project Information & Data Portal, "Provident Growth Fund II, LP".

[316] See, for example, IDB Invest, "Latin America Venture Debt Growth Fund"; IFC Project Information & Data Portal, "TIDE AFRICA LP"; EBRD, "Earlybird Digital East Fund II"; EBRD "Algebra Ventures II"; IDB Invest, "Amadeus LAC Sustainable Growth Fund"; and IFC Project Information & Data Portal, "Wavemaker Pacific 3 LP". See also EIB, "European Growth Finance Facility", which finances a wide range of digitally enabled products and services. However, sometimes a brief discussion of digital risks has been included: see, for example, EBRD, "Earlybird Digital East Fund II".

[317] See, for example, IFC Project Information & Data Portal, "ISC-AVV", "Janngo Capital Start-up Fund" and "4DX III". See also IFC Project & Data Portal, "Kuku FM", which involves an investment in a digital audio platform for non-music content in India. In the summary, a possible IFC role in building "content filtration methodology and standards" is suggested, however, there is no discussion of creator compensation or generative artificial intelligence issues.

[318] See IFC Project & Information Portal, "Endiya III".

[319] See, for example, IDB "Creditas"; IFC Project Information & Data Portal, "Wave Debt" and "2C2P"; and EBRD "Capital Bank – Digital Bank Facility".

[320] Available on the "How?" tab of the BII "MoneyFellows" project web page. Reference is made only to the positive aspects of digital "buy now, pay later" models, without addressing the potential risks of indebtedness: "…'Buy now, Pay later' (BNPL) products … increase and maintain household well-being and resilience by growing and protecting savings, enabling productive investments, managing cashflows and saving time."

- **Financial inclusion.** Projects aimed at improving financial access for vulnerable populations should address risks and appropriate risk management measures specific to these populations. Instead, several projects reviewed for the present report appear to reflect a more-is-more philosophy and fail to detail how risks will be managed.[321] While some regulatory reform programmes address consumer protection,[322] others appear to overlook concerns about vulnerable populations.[323]
- **Digitalizing SME financing through financial intermediaries.** DFIs supporting the digital transformation of SME financing[324] sometimes provide very little information in project descriptions,[325] making it difficult to assess the consideration of risks, including in sensitive sectors.
- **E-commerce.** When e-commerce is offered directly to consumers, considerations such as data protection and consumer protection should be integrated into project design. However, these aspects are frequently absent from project summaries, preparation documents and E&S reviews.[326]

© Adobe Stock/Generative AI/by pkproject

[321] See, for example, IDB "Digital Payments for an Inclusive Digital Economy" and "Silver Finance: Financial Inclusion for Life"; and AfDB "Mauritania – Financial Infrastructure Modernisation Support Project (PAMIF) – Additional Loan". See also Early Warning System "DWM Displaced Communities Fund (EIB-20220378)", where the end beneficiaries are particularly vulnerable, but there is only a brief project description; and IDB "Génesis Empresarial: Digital Technologies to Accelerate Rural Financial Inclusion", which provides funds to the largest unregulated microfinance institution in Guatemala to launch new digital financial products (nano-credits) and non-traditional finance channels (digital wallets). These new products and channels target unserved lower-income populations, particularly in rural areas and small urban centres. However, there is no discussion of digital risks.

[322] See, for example, ADB, "Indonesia: Promoting Innovative Financial Inclusion Program (Subprogram 2)".

[323] See IDB, "Institutional Support for the Consolidation of the Digital Financial Inclusion Ecosystem in Latin America and the Caribbean".

[324] See IFC Project & Information Portal, "TBC Uzbekistan Equity"; and IDB Invest, "Scotiabank Let's SME – Digital Services for SMEs".

[325] EBRD has an extensive portfolio of SME financing via financial intermediaries, but provides very little information on the project site. See, for example, EBRD "FIF – OTP Bank Serbia – SME", and similarly, IDB Invest, "Republic Bank – Caribbean Partnership".

[326] See, for example, IDB Invest, "Merqueo-Equity" and "Habi – Structured Loan".

Box 19 Examples of digital transformation projects with insufficient consideration of users

- **The IDB Fintech LAC initiative** is aimed at developing, consolidating and integrating a fintech ecosystem in Latin America and the Caribbean. The initiative is focused on promoting policy and regulatory frameworks and strengthening institutional capacities within the ecosystem, with the goal of achieving regional regulatory convergence.[327] However, the description of the fintech ecosystem applicable to the initiative appears to include only cybersecurity risks that affect fintech companies and not digital risks to users.[328] This would seem to be a serious gap given that the project focuses on regulatory reform.
- In **the IDB Invest review of digital transformation for financial inclusion in Latin America and the Caribbean**, cybersecurity issues are looked at, but other potentially relevant digital risk issues, such as biases in automated credit rating system digital risks, appear to be neglected.[329] This omission seems particularly notable given the emphasis in the report on vulnerable populations. Although a commitment to protecting vulnerable groups is highlighted in the blog post announcing the review, the report lacks detailed discussions on necessary protections. Instead, the role of customers as digital advocates for financial institutions is discussed, as is credit analysis involving extensive data scraping, without addressing issues of consent or data protection.[330]
- The **World Bank-financed Second Financial Inclusion Project for Sierra Leone** is aimed at promoting a more inclusive and resilient financial sector for individuals and MSMEs, with a significant digital financial services component.[331] The need to address gender-based violence has assumed increasing importance in the operations of most MDBs, including at the World Bank, following hard lessons at country level.[332] However, this does not yet seem to be consistently reflected in digital transformation projects.[333] Positively, the Sierra Leone project includes a gender-based violence action plan,[334] but all actions relate to the physical dimensions of the project, rather than exploring the online dimensions of harassment and discrimination that may occur in connection with the project or the violence that may occur in connection with accessing the services.[335]

3. HEALTH SECTOR

The digital transformation of healthcare holds significant promise for improving health outcomes. Innovations such as mobile health, health informatics, virtual care, remote

[327] See IDB "Institutional Support for the Consolidation of the Digital Financial Inclusion Ecosystem in Latin America and the Caribbean".

[328] See IDB, *FinTech in Latin America and the Caribbean: A Consolidated Ecosystem for Recovery* (2023).

[329] IDB Invest, Digital Transformation Study for Financial Inclusion in Latin America and the Caribbean (2023), p. 100.

[330] Ibid., p. 63.

[331] See the World Bank, "Sierra Leone Second Financial Inclusion Project".

[332] See the World Bank, "Gender-Based Violence (Violence Against Women and Girls)".

[333] World Bank, *Gender-Based Violence Prevention and Response in World Bank Operations: Taking Stock After a Decade of Engagement, 2012–2022* (2023).

[334] World Bank, *Gender-Based Action Plan for the Sierra Leone Second Financial Inclusion Project (P177947)* (2024). Compare the World Bank report with the 2024 BII publication "How can digital financial services drive women's economic development in South Asia?", in which these issues are highlighted, but there is no guidance on how to address them.

[335] For context, see UN Women, "Leveraging digital finance for gender equality and women's empowerment", Working Paper (New York, 2019), p. 17: "There is an additional layer of risk for women of facing gender-based violence as a direct consequence of owning a phone, exchanging information online and having independent access to new online financial services. Digital services and new technologies not only can widen inequality, they can also increase acts of violence or harassment".

monitoring, smart wearables and data platforms are enhancing medical diagnosis, treatment decisions and personalized care. AI and machine learning further improve predictive and prescriptive analytics, treatment plans and diagnostics. These advancements can accelerate progress towards universal health coverage by increasing service availability, strengthening health systems, reducing costs and improving treatment standards.[336] These digital advancements have been accelerated by the COVID-19 pandemic.

At the same time, health data is one of the highest protected categories of personal data. The World Health Organization emphasizes that health data, while crucial for improving care, must be classified as sensitive personal data requiring stringent security and privacy protections given the potentially serious consequences of disclosure. The Organization also underlines that effective protection of health data requires robust legal and regulatory frameworks to ensure privacy, confidentiality, data integrity and cybersecurity.[337] Despite this, many data protection regimes fall short in practice and enforcement is inconsistent.[338]

Digitalization in healthcare can present significant risks. The personal sensitivity of health data makes it vulnerable to breaches, which are common as a result of malware, ransomware and other cyberattacks.[339] Such breaches undermine privacy rights and erode trust in the healthcare system. As reported recently in the United Kingdom and the United States of America, health data may be shared with technology companies without the consent (or without sufficiently clear consent) of patients.[340] Function creep, where data collected for one purpose are used for another, raises additional concerns. For instance, personal health data collected during medical visits might be repurposed for unrelated uses, such as immigration status checks. The inadvertent disclosure of confidential health data may also result in the stigmatization or discrimination of individuals with particular medical conditions. The use of biometric data in health research[341] and applications adds another layer of concern, with potential misuse for forensic or legal purposes.[342] Issues of informed consent and access by advertisers are also pertinent and pressing.[343] Moreover, the shift to digital-only access to health services can exacerbate exclusion and discrimination, particularly for marginalized groups such as women, migrants and older persons, as a result of existing digital divides.[344]

[336] See WHO, "Harness digital health for Universal Health Coverage", 20 March 2023.

[337] WHO, *Global Strategy on Digital Health 2020–2025* (2021), p. 10.

[338] Privacy International, "The hidden cost of digital health services", 31 October 2023.

[339] Metty Paul and others, "Digitization of healthcare sector: A study on privacy and security concerns", *ICT Express*, vol. 9, No. 4 (August 2023), pp. 571–588; Center for Internet Security, "Data Breaches: In the Healthcare Sector"; and, Nina Sun and others, "Human Rights and Digital Health Technologies", *Health Human Rights Journal*, vol. 22, No. 2 (December 2020), pp. 21–32.

[340] See, for example, Julia Powles and Hal Hodson, "Google DeepMind and healthcare in an age of algorithms", *Health Technology*, vol. 7 (March 2017), pp. 351–367. The case has been subject to ongoing litigation in the United Kingdom; and Maria Ward-Brennan, "NHS: Google faces appeal over patient data deal with London's Royal Free Hospital", CityAM, 21 October 2024.

[341] Kelin and the Kenya Key Populations Consortium, "Everyone said no" Biometrics, HIV and human rights: a Kenya case study" (2018).

[342] Matthew M. Kavanagh and others, "Biometrics and public health surveillance in criminalised and key populations: policy, ethics, and human rights considerations", *The Lancet HIV*, vol. 6, No. 1 (January 2019).

[343] Nada Farag and others, "Mapping the apps: ethical and legal issues with crowdsourced smartphone data using health applications", *Asian Bioethics Review*, vol. 16 (June 2024), pp. 437–470; and Danuta Mendelson, "Legal protections for personal health information in the age of Big Data – a proposal for regulatory framework", *Ethics, Medicine and Public Health*, vol. 3 (2017), pp. 37–55.

[344] Sy Atezaz Saeed and Ross McRae Masters, "Disparities in health care and the digital divide", *Current Psychiatry Reports*, vol. 23, No. 9 (July 2021), p. 61; and Tomas Weber, "Rooting out AI's biases", *Hopkins Bloomberg Public Health Magazine*, 2 November 2023.

Approaches to addressing digital risks in the healthcare sector

DFIs have played a crucial role in financing responses to the COVID-19 pandemic, with a particular focus on the healthcare sector.[345] These institutions continue to provide significant funding, technical assistance and knowledge across the health sector for both public and private entities.

All the reviewed MDBs invest in healthcare, but only a few major health funders have a specific strategy or approach that focuses on digital health (see box 20). Among those that do, attention to the kinds of digital risks identified above varies. The IFC and the World Bank have established the Ethical Principles in Health Care initiative,[346] which includes some principles relevant to the right to health. However, it is unclear whether adherence to these principles is required as a condition of World Bank financing or if adherence is subject to any monitoring.

Box 20 Overview of approaches to digital risks in the digital health sector

- **ADB** has acknowledged that health is a human right and essential to development[347] and its Digital Health Implementation Guide for the Pacific includes a chapter on security, privacy and confidentiality.[348] However, the ADB *Strategy 2030 Health Sector Directional Guide* briefly mentions the opportunities of digitalization, but not critical concerns such as consent, privacy or potential exclusions.[349]
- **IDB** does not prioritize digital health as a core focus area, but recognizes digital transformation as a key opportunity to enhance healthcare systems in the region.[350] The IDB digital health flagship report offers a valuable overview of steps towards digital transformation, and highlights relevant principles and tools in this regard, but it contains only limited discussion of privacy, cybersecurity and exclusion risks associated with digitalization. IDB states that it applies standards for interoperability, cybersecurity and privacy promoted by organizations like the World Health Organization (WHO), the Pan-American Health Organization (PAHO), the International Telecommunication Union (ITU) and the International Standards Organization (ISO).[351] However, the standards are not always evident in project documentation.[352]

[345] See, for example, ADB, "Responding to COVID-19: Lessons from Previous Support to Micro, Small, and Medium-Sized Enterprises" (2020); EBRD Independent Evaluation Department, "Rapid Assessment of EBRD's Solidarity Package", 21 February 2022; Bank Information Center, "Covid-19"; NGO Forum on ADB; World Bank, *The World Bank's Early Support to Addressing COVID-19: Health and Social Response* (2022). The World Bank evaluation shows the extensive contributions of digitalization to the Bank's COVID-19 operations (see pp. 193–194), although, with the exception of India (p. 212), there was very little discussion on the extent to which cybersecurity, data protection or other digital risks were addressed.

[346] See IFC, "IFC's Work in Health".

[347] See ADB, "Health".

[348] ADB, *Digital Health Implementation Guide for the Pacific* (Metro Manilla, May 2021).

[349] ADB, *Strategy 2030 Health Sector Directional Guide: Toward the Achievement of Universal Health Coverage in Asia and the Pacific* (2022), pp. 8–9.

[350] See IDB, "Health"; and IDB, *The Golden Opportunity of Digital Health for Latin America and the Caribbean* (2022).

[351] IDB, *The Golden Opportunity of Digital Health for Latin America and the Caribbean*, p. 11.

[352] PAHO, "8 Guiding Principles of Digital Transformation of the Health Sector: A Call to Action in the Americas" (2021). The eight principles include mainstreaming human rights in all areas of digital health; however, these are not reflected in IDB, *The Golden Opportunity of Digital Health for Latin America and the Caribbean*.

- **IFC** manages a $3.5 billion portfolio in healthcare companies within emerging markets.[353] Through its DigiHealth initiative, IFC provides a comprehensive platform for healthcare providers to plan, finance and implement digital transformation strategies.[354] The initiative emphasizes the benefits of digitalization; however, it does not appear to address relevant digital risks or explicitly align with the Ethical Principles in Health Care Initiative.[355]
- The **World Bank** has a $36 billion global health portfolio;[356] however, digital health is not among its focus areas.[357]

The following boxes provide a small selection of MDB projects involving digital health, taken from the nine MDB project databases. The cases are only illustrative, and not necessarily representative; however, they raise questions about the extent to which foreseeable and potentially significant digital risks of the kinds discussed earlier have been factored into project risk management. For private sector projects, available information is much more limited and digital risks are rarely highlighted, even in the more sensitive digital health subsectors.

Box 21 Examples of digital health projects[358]

- **Supporting health sector reforms with digital transformation.** When DFIs support health sector reforms that include digital transformation, it should be expected that project preparation would assess policy and legal frameworks related to privacy and data protection, evaluate institutional capacity for cybersecurity, and review legal requirements concerning patient consent. However, such analyses were lacking in available documentation for several sampled projects, including ADB health projects in China[359] and Mongolia,[360] and an IDB project in Guyana.[361] A World Bank project in Peru, which included a health information system, addressed software, cloud storage and Internet reliability issues, but did not appear to consider patient data protection.[362] Similarly, a health project in Togo planned an "aggressive membership drive" for biometric registration, but beyond committing to compliance with national data protection law, risks associated with handling sensitive health data were not discussed.[363] The World Bank has supported a wide variety of other Governments in digitalizing their health systems, but relatively few projects appear to address patient privacy issues.[364]

[353] See IFC, "IFC's Work in Health".

[354] See IFC, "DigiHealth: Supporting Digitalization in Healthcare".

[355] Ibid.

[356] See World Bank, "Health: Overview".

[357] See World Bank, "Health, Economic Jobs and Growth".

[358] Danish Institute for Human Rights, "Development Finance for Digitalisation: Human Rights Risks in Sub-Saharan Africa", pp. 16–17.

[359] See ADB, "China, People's Republic of: Strengthening Public Health Institutions Building Project".

[360] See ADB, "Mongolia: Improving Access to Health Services for Disadvantaged Groups Investment Program".

[361] See IDB, "Health Care Network Strengthening in Guyana".

[362] World Bank, "Peru – Integrated Health Networks Project" (2019).

[363] World Bank, *Togo – Essential Quality Health Services for Universal Health Coverage Project* (2021), pp. 18 and 31.

[364] See, for example, the World Bank, "Indonesia: Strengthening National Tuberculosis Response Program"; and "Andhra Pradesh Health Systems Strengthening Project".

- **Lessons learned from health sector digital transformation.** IDB has supported numerous projects focused on digital health transformation across Latin America.[365] While these projects highlight the benefits of digital health, there is often little discussion of necessary safeguards, including with regard to health information exchanges. Although safeguards may be included in supporting tools and guidance documents, if they are not reflected in project documentation, stakeholders are likely to be less aware and less able to trigger any necessary mitigation actions.
- **Developing or expanding medical facilities.** The current generation of E&S safeguards focuses extensively on physical impacts. Hence, risk assessments in projects supporting the construction or expansion of health facilities typically include impacts from construction, resettlement, fire safety, appropriate disposal of medical wastes and labour rights. However, project documentation frequently overlooks the right to privacy and protections due to patients, the core consumers of medical facilities and services.[366]
- **Investing in venture capital funds or health technology funds.** A review of project documentation for venture capital and health technology funds revealed no discussion of digital risks. There was also no indication that DFIs or fund managers required investee companies to have adequate data protection policies in place or to implement privacy by design or other relevant ethical principles. The lack of detailed digital risk management requirements appears to constitute a significant gap in ensuring comprehensive protection in health technology investments.[367]
- **Health products.** Where DFIs support health products that track and monitor sensitive health data, requirements concerning privacy and data protection should be a core part of project requirements. However, these rarely appear to be addressed in project documentation.[368]

Box 22 Case study – ADB e-health project in Tonga

In July 2019, **ADB** approved a $7.5 million grant for the **Introducing eGovernment through Digital Health project in Tonga**. The primary goal of the project is to design and implement a digital health information system to replace the largely paper-based health system in the country.[369] In 2021, the International Organizations Clinic of the New York University School of Law carried out an analysis in order to assess the extent to which the Tonga e-health project met its objectives and addressed relevant digital risks.[370]

[365] See, for example, IDB, "Creating knowledge for the implementation of digital transformation in health and social protection" and "Support the design, implementation and evaluation of digital health transformation operations". The preparatory documentation for the project did refer to one cybersecurity toolkit for the health sector, produced independently (see the IDB Cybersecurity Self-Assessment Tool).

[366] See, for example, IFC Project Information & Data Portal, "Abdali CMC"; "RSE Covid Ciel Healthcare Limited"; "Ayala Corporation Social Bond"; and "Einstein – Cancer Center".

[367] See, for example, AIIB, "Multicountry: Quadria Capital Fund II"; and the IFC Project Information & Data Portal, "Everstone IV"; "Lighthouse IV"; "Quadria Capital Fund II LP"; "1mg"; and "Leapfrog Emerging Consumer Fund IV, LP".

[368] See BII, "Turtle Shell Technologies Pvt Ltd".

[369] See ADB "Tonga: Introducing eGovernment through Digital Health".

[370] New York University School of Law, International Organizations Clinic, "Submission for the Review and Update of the ADB Security Policy Statement" (April 2022); Annex, Digital Risk Case Study – Tonga: eGovernment Through Digital Health (2021), on file with OHCHR.

The analysis indicated a key issue not adequately addressed in the ADB's project appraisal: opportunity costs. The $7.5 million grant prioritized spending on hardware and software upgrades for the health information system and on building the capacity to operate and maintain the digital infrastructure.

Given the small government and limited resources of Tonga, it was argued by the International Organizations Clinic that this allocation of development aid towards digital infrastructure may divert funds from other pressing needs in the Tongan health system, such as recruiting and training medical personnel, constructing new facilities and purchasing medication and supplies. Additionally, while the ADB planned to support the maintenance of the health information system for the first five years, future maintenance costs were expected to be covered by the Ministry of Health of Tonga, potentially straining the health budget. As of 2021, whether these policy choices would be likely to improve healthcare services appeared uncertain.[371]

The analysis also raised a number of other digital risk concerns. It was alleged in the analysis that the ADB's assessment did not consider the possibility that digitalization could reduce the quality of care, and did not sufficiently evaluate the capacity of human resources, hardware or software. The attitudes of healthcare professionals and patients towards digitalization also did not appear to be taken into account. Furthermore, it was alleged by the International Organizations Clinic that the project assessment failed to address the risk of increased exclusion as a result of variable connectivity, low Internet usage and limited digital literacy. Data privacy and access control reportedly received little attention, despite the system's collection of sensitive health data. Finally, according to the International Organizations Clinic, the Bank's analysis did not adequately consider the poor quality of Internet access across the archipelago of Tonga or the potential impacts of natural disasters and climate change on the proposed system.

4. INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES SECTOR

The digital transformation of ICT infrastructure is crucial for global connectivity. SDG 9, Target 9.c includes a call to significantly increase access to ICT and to strive for universal and affordable Internet access in least developed countries by 2020. This target has been missed: half of the global population lacked Internet access at the end of 2019 and access was heavily concentrated in developed countries.[372] The Broadband Commission for Sustainable Development estimates that achieving universal, affordable and high-quality broadband access in Africa alone will require $100 billion in investment to 2030.[373]

Digital risks in the ICT sector are well-known and pervasive.[374] It is vital to address the risks of long-term ICT infrastructure at the outset, given the difficulties of retrofitting effective safeguards once the infrastructure is established. Network providers and equipment vendors are essential to Internet reliability and security, but licensing and contractual arrangements between operators of different components that together enable connectivity are not disclosed.

[371] New York University School of Law, International Organizations Clinic, "Submission for the Review and Update of the ADB Security Policy Statement" (April 2022), p. 14.

[372] See ITU "Facts and Figures 2024 – Internet Use".

[373] Broadband Commission for Sustainable Development, *Connecting Africa Through Broadband: A Strategy for Doubling Connectivity by 2021 and Reaching Universal Access by 2030 – A "Digital Infrastructure Moonshot for Africa"* (2019).

[374] For one overview and explanation of the digital ecosystem, see Global Network Initiative and BSR, *Human Rights Due Diligence Across the Technology Ecosystem* (2022), pp. 10–16.

These licensing and contractual arrangements determine the terms under which services are ultimately supplied to consumers and who can exercise control over the different components of connectivity infrastructure. National legislation in many jurisdictions requires Internet service providers (ISPs) to provide means for national authorities to intercept communications for investigations of criminal activities. However, those same means of interception can also be misused for intrusive state surveillance, compromising privacy and other human rights.[375] It is not uncommon for telecommunications companies to face dilemmas between protecting customer privacy and meeting government demands for data access.

Data-collecting devices such as sensors, facial recognition camera and global positioning systems pose additional risks. These technologies can be used to track and profile individuals in ways that may invade privacy or raise other human rights concerns. For instance, data collected from sensors positioned around a city can be used to track residents' movements in order to create a profile of the overall rhythms of a neighbourhood, or may enable the analysis of sewage for signs of concentrated drug use.[376]

The ever-growing digital services sector raises data governance concerns throughout the data life cycle: collection, analysis, use and deletion. This has triggered a range of legislative responses and softer forms of regulatory action across the globe, engaging a wide range of actors in the digital ecosystem. Despite such initiatives, however, there is an increasing range of actors in the ecosystem whose business model is based on large-scale data mining: using, buying, selling, brokering and scraping data in contravention of ethical principles and human rights law. Information misuse has proliferated as companies compete to commercialize their customers' personal data and privacy. The AI revolution has ignited a growing number of concerns[377] and a plethora of risk mitigation and regulatory initiatives. As AI permeates more and more human activity and decision-making, the scale of impacts rises exponentially. One algorithmic error "can tip the scales for swaths of people".[378] AI risks exacerbate many of the risks discussed earlier in this report, such as turbo-charging discrimination and impacting access to information, as well as creating entirely new kinds of risks, such as the risk of AI overriding autonomy and independent decision-making.[379]

[375] See OHCHR report, *The right to privacy in the digital age* (A/HRC/27/37), para. 47.

[376] See Nancy Scola, "Google is building a city of the future in Toronto. Would anyone want to live there?", *Politico*, July/August 2018; and Laura Bliss, "A big master plan for Google's growing smart city", Bloomberg, 25 June 2019.

[377] See World Bank, *Digital Progress and Trends Report 2023*, chap. 5, p. 85: "AI holds potential to accelerate productivity growth, expand opportunities, improve consumer welfare, and bring vast benefits to the global economy and society. However, the use of AI systems and tools could also cement big tech's market dominance, displace workers, widen inequality, strengthen the state's surveillance abilities, erode privacy, turbocharge misinformation, manipulate democratic processes, and increase security vulnerabilities".

[378] See, for example, Aubra Anthony and others, "Advancing a More Global Agenda for Trustworthy Artificial Intelligence", Carnegie Endowment for International Peace, 30 April 2024, p. 15.

[379] See OHCHR, "B-Tech Project"; and Anna Felländer and others, "Achieving a data-driven risk assessment methodology for ethical AI". *Digital Society*, vol. 1, No. 2 (August 2022), pp. 1–27. See also Jessica Fjeld and others, "Principled artificial intelligence: mapping consensus in ethical and rights-based approaches to principles for AI", *Berkman Klein Center Research Publication*, vol. 2020, No. 1 (2020).

Approaches to addressing digital risks in the sector

DFIs have played a vital role in investing in digital infrastructure and associated digital services, and in providing advisory services to support the development of appropriate regulatory frameworks. Instead of advocating for a slowdown or moratorium on AI that cannot be used in line with international human rights law, several DFIs are helping their member countries and companies prepare for AI, addressing emerging risks and the implications of AI power concentration in the Global North.[380]

Box 23 Overview of approaches to digital risks in the ICT sector

As in the case with other sectors reviewed in this report, some DFIs have a specific focus on the ICT sector and others do not. Digital risks are generally particularly obvious and well-documented in this sector; however, in comparison with the other three sectors reviewed for this report, there seems to be comparatively less attention paid to presenting approaches to the sector as distinct from simply listing the kinds of projects that are financed. There also seems to be comparatively less discussion of ICT-specific digital risks in the various DFI sector overviews and strategies.

- **ADB** finances digital infrastructure (e.g. telecommunications networks, data centres, cloud services, devices and applications) and digital technology industries.[381]
- **AfDB** finances the ICT sector, focusing on digital services and platforms, digital entrepreneurship and skills and digital financial inclusion.[382]
- The **AIIB** digital infrastructure sector strategy covers both hard infrastructure (for connectivity, processing and data storage) and soft infrastructure (services, applications, terminals and devices).[383]
- **EBRD** is investing in the roll-out of essential digital infrastructure as part of its approach to accelerating the digital transition.[384]
- **EIB** finances digital economy projects involving various aspects of ICT infrastructure, equipment, services, applications, research and development.[385]
- **IDB** addresses technology within its innovation, science and technology sector framework.[386]
- The work of **IDB Invest** in this area is categorized under the title "digital economy." IDB Invest works with countries on regulatory frameworks and public investment in telecommunications, media and technology.[387]

[380] See, for example, See World Bank, *Digital Progress and Trends Report 2023*, chap. 5, p. 85; World Bank "Artificial Intelligence (AI) Working Group"; Rabi Thapa, "Developing AI for Development"; and IDB, "IDB Launches Expanded fAIr LAC+ Platform for Responsible AI in Latin America and Caribbean" (November 2023).

[381] See ADB, "Digital Technology".

[382] See AfDB, "Information and communication technology".

[383] AIIB, "Digital Infrastructure Sector Strategy" (2020), pp. 2–3.

[384] EBRD, "The EBRD's digital approach to accelerating the digital transition, 2020–2025", p. 18.

[385] See EIB, "Digital Economy".

[386] IDB, *Innovation, Science, and Technology Sector Framework Document* (July 2022).

[387] See IDB Invest, "Digital Economy".

- **IFC** does not list ICT as a focus sector,[388] but supports innovative technology through its venture capital work.[389]
- The **World Bank** finances broadband connectivity, access and use, digital data infrastructure and services, and cybersecurity.[390]
- **Finnfund** focuses on digital infrastructure and solutions as one of its core sectors for investment. Its digital solutions investments focus on fintech, e-logistics, e-commerce, health technology, agrotechnology and educational technology.[391]

Box 24 Examples of emerging DFI work on AI

- **ADB** has reportedly established an AI cross-department working group.[392]
- **AIIB and AfDB**: no cross-cutting publications or initiatives on AI were found.
- In 2020, **EIB** launched a €150 million financing instrument to support AI companies across Europe.[393] However, the extent to which digital risks are addressed is not clear. In an EIB report on AI published in 2021, only five of 106 pages were dedicated to addressing risks.[394]
- The **EBRD** *Digital Approach: Accelerating the Digital Transition 2020–2025* integrates attention to AI risks and opportunities. However, there does not appear to be much other publicly available documentation on its approach to AI.
- **IDB** is active in developing knowledge products and tools on AI. The fAIr LAC+ initiative of IDB and its innovation laboratory, IDB Lab, provides tools and services to support the responsible use of AI in Latin America.[395]
- **IFC** published a discussion paper on AI in 2021 and also launched a proposal for a technology code of conduct, which, together with a set of practical tools for its operationalization, would assist the corporation's clients engaged in technology intensive projects.[396] However, it is unclear whether there has been any follow-up to this initiative.
- The **World Bank** has been the clearest in highlighting AI risks in its emerging approaches to AI.[397] It reportedly has a wide range of AI initiatives, although there appears to be no consolidated description of how AI risks are being addressed across all the various initiatives.

[388] See IFC, "What We Do – Sectors & Expertise".

[389] See IFC, "Expertise – Disruptive Technologies and Venture Capital".

[390] See World Bank, "Digital".

[391] See Finnfund, "Digital infrastructure and solutions".

[392] See, for example, ADB, *Artificial Intelligence in Action: Selected ADB Initiatives in Asia and the Pacific* (2024). In the publication (p. iv), a cross-department working group on artificial intelligence is briefly described, but then further on, AI initiatives financed by ADB are described without discussion of any preventive or mitigation measures to address artificial intelligence-related project risks.

[393] EIB, "EIB Group provides €150 million to support artificial intelligence companies", 3 December 2020.

[394] EIB, *Artificial Intelligence, Blockchain And The Future Of Europe: How Disruptive Technologies Create Opportunities For A Green And Digital Economy* (2021), pp. 85–89.

[395] See also Edgar L. Cabanas, "The great tech revolution: artificial general intelligence & multilateral development banks" in IDB Invest "Digital Economy", 26 April 2023; and IDB, "IDB Launches Expanded fAIr LAC+ Platform for Responsible AI in Latin America and Caribbean", 22 November 2023.

[396] IFC, *Artificial Intelligence in Emerging Markets – Opportunities, Trends and Emerging Business Models* (2021), chap. 5.

[397] See World Bank, *Digital Progress and Trends Report 2023*, chap. 5.

© Adobe Stock/Generative AI/by Pungu x

The following boxes provide a brief selection of MDB projects involving digital infrastructure and services, taken from nine MDB project databases dealing with both public sector and private sector clients. Given the sector's focus on digital technology, it might be expected that digital risks would attract explicit attention. However, this was not necessarily the case. While there were occasional mentions of data protection, privacy and concepts such as "privacy by design",[398] detailed discussions of digital risks, including data protection and cybersecurity, were not common. Analyses of E&S risks were usually confined to projects with physical footprints.

Larger issues, such as contextual risks for long-term infrastructure projects or data-intensive services involving problematic data extraction practices,[399] were rarely addressed. Concerns about AI risks generally do not seem to have been incorporated into project-level disclosures, although, as noted previously, there are other ways in which DFIs have started to address these issues. As with the other sectors reviewed in this report, project disclosures frequently fail to refer to international standards, principles or norms applied, and the tools used for risk analysis are often not disclosed.

Box 25 Examples of digital infrastructure projects

- **Unaddressed contextual risks.** DFIs are frequently funding digital infrastructure projects, particularly in telecommunications, in very challenging national contexts. Once infrastructure is established, it becomes a long-term fixture. However, critical issues such as market-entry decisions, government regulatory frameworks and policies for handling government requests for surveillance or service restrictions, are often not disclosed or adequately addressed in these projects. This is particularly concerning in fragile and conflict-affected countries, given the dynamic and unpredictable circumstances and higher potential for data misuse. For example:
  - EIB financed the expansion of telecommunications infrastructure in Somalia, aiming to diversify the country's international connectivity and extend broadband networks to underserved areas. While the project description mentioned E&S issues related to construction, it failed to address the contextual risks or the regulatory framework.[400]

[398] See, for example, World Bank, "Privacy by design: current practices in Estonia, India, and Austria" (2018).

[399] See, for example, OHCHR, "B-Tech Project – Human rights risks in tech: engaging and assessing human rights risks arising from technology company business models" (2023).

[400] See EIB, "COVID19 Somalia Telecom Infrastructure Expansion".

- ADB financed a private sector telecommunications operator in Myanmar[401] during a brief period of transition from military rule. The Myanmar Nationwide Data Connectivity Project did not account for the weak regulatory framework or other contextual risks. The more detailed Poverty and Social Impact Assessment (PSIA) mentioned only positive impacts on women and girls arising from increased access.[402] After the subsequent military coup, telecommunications providers faced pressure to comply with data requests from the military, leading some operators (though not the ADB-financed operator) to exit the country as required under their human rights policies.[403]
- IFC invested in Safaricom Telecommunications Ethiopia, the sole winner of the country's unified telecommunication service licence to build, own and operate a nationwide public telecommunication network. The investment, made during the Tigray War,[404] aimed to support the transformation of various SDG verticals through advanced telecommunication services. However, no mention was made of the ongoing conflict and context or its potential impact on the project.[405]

- **Regulatory oversight.** EBRD provided a senior loan to Aztelekom LLC, a State-owned telecommunications company in Azerbaijan, along with technical assistance to revise the sector's legal and regulatory framework. While the review was aimed at strengthening laws and safeguards,[406] it did not address digital risks associated with the sector.

- **Disproportionate and narrow focus on digital connectivity rather than risks.** DFIs have financed numerous digital connectivity projects that are crucial for expanding access. However, these projects often focus heavily on the benefits of digital connectivity without adequately addressing potential negative impacts or digital risks, or the contexts in which they are implemented.[407] E&S reviews typically cover the impacts of physical infrastructure footprints,[408] and while some World Bank projects address regulatory frameworks, they do not always require updates to outdated frameworks, including with regard to data protection.

- **Opportunity costs.** Digital infrastructure projects can be expensive to operate and maintain, requiring skilled staff and long-term service contracts for software and technical updates. Ongoing costs and the political and economic challenges of operating and maintaining digital infrastructure are not always adequately reflected in project planning.[409]

[401] See ADB, "Myanmar: Nationwide Data Connectivity Project".

[402] See ADB, "Ooredoo Q.P.S.C. Nationwide Data Connectivity Project: Initial Poverty and Social Analysis". Compare this with BBI, "Frontiir Pty Ltd", where BII was encouraged by Myanmar-based actors to prompt Frontiir to join the Global Network Initiative as a mitigation strategy to deal with the risky contextual environment.

[403] See, for example, Telenor, "Telenor publishes learning outcomes from Myanmar engagement", 23 May 2023.

[404] See Council on Foreign Relations, Global Conflict Tracker, "Conflict in Ethiopia" (March 2025).

[405] See IFC Project Information & Data Portal, "Global Partners". Safaricom, the largest mobile network operator in Kenya, has experience of the human rights challenges of running networks in Africa during times of heightened conflicts. See, for example, Institute for Human Rights and Business, "Digital dangers – Corporate Responses to Hate Speech in the 2013 Kenya Presidential Elections", Institute for Human Rights and Business (November 2014). The case study referred to in the paper focuses on the initiative of Safaricom to create its own code of conduct to prevent spreading hate-filled messages through its bulk short message service. Compare this with the BII "Global Partnership for Ethiopia B.V.", which recognized some of these risks, but which did not appear to include relevant prevention or mitigation measures.

[406] See EBRD, "Aztelekom LLC".

[407] See, for example, EBRD, "Rural broadband rollout".

[408] See, for example, ADB, "Papua New Guinea: Pacific Telecommunications Modernization Project"; AIIB, "Cambodia: Fiber Optic Communication Network Project"; ADB, "Philippines: Tiger Digital Infrastructure for Rural Connectivity Project"; EIB, "Digital ACP Global Authorization II"; IDB, "Program for the Development of the Federal Optic Network (REFEFO)"; IDB, "Project Oban B-Bond"; IDB Invest, "QMC Regional Facility"; IFC, "Robi Axiata IV"; IFC, "ElCat"; IFC, "Guodong Tower"; and IFC, "Telecom Armenia CJSC".

[409] See box 2 on the subject of digitization as the best choice and see New York School University School of Law, International Organizations Clinic, "Submission for the Review and Update of the ADB Safeguard Policy Statement" (April 2022), pp. 16–17.

Box 26 Examples of digital services projects

- **Facial recognition project rated as low risk.** Facial recognition technology is inherently controversial because of its unreliability, lack of consent in data collection and scope and the potential severity of the (life-long) consequences of data misuse.[410] Some States have banned facial recognition in specific sectors or are calling for stricter regulation of this technology. Despite these concerns, the EBRD equity investment in Alcatraz AI, a company providing facial authentication for enterprise security, was rated as low risk.[411] While there was a brief mention of compliance with the General Data Protection Regulation and ISO 27001 certification (for information security management), the project lacked detailed discussion of the risks associated with facial recognition in security operations or potential mitigation strategies. The project description noted that E&S impacts were limited to labour conditions, cybersecurity and data privacy, all of which were considered manageable through good management practices.
- **Lack of focus on product design and end use.** IFC proposed an investment in a global leader in technology-enabled creative solutions for the entertainment industry, including gender advisory support focused on increasing women's representation in the client's workforce. However, the advisory support apparently did not address gender issues related to the company's products.[412]
- **AI investments with insufficient risk assessment.** An AIIB investment in the Sinovation Disrupt Fund, a venture capital fund focused on AI across various sectors,[413] did not mention the risks associated with AI. Similarly, an EIB co-investment in a venture capital fund investing in AI was presumed low risk, simply because the projects were small.[414] This approach overlooks the potential widespread harm that small AI firms can cause if their products gain market acceptance. An investment by IFC in a private digital insurance service, which used AI to determine coverage, also did not highlight any digital risks or address the risks associated with digitalizing the client's healthcare business.[415]
- **Lack of attention to end use of innovations through financial instruments and grant.** EIB funded four grant-making programmes in Poland, which in turn funded various technologies, including at-home health monitoring and the development of unmanned autonomous vehicles. However, there was no focus on the end use and potential risks associated with these innovations.[416]

[410] See, for example, Joel McConvey, "UK police have used PimEyes facial recognition search tool over 2000 times", Biometric Update, 6 May 2024; and Joel McConvey, "Indian police adopt facial recognition despite risk of massive data breaches", Biometric Update, 6 May 2024.

[411] See EBRD, "VCIP III – Alcatraz".

[412] See IFC Project Information and Data Portal, "DNEG Debt".

[413] See AIIB, "China: Sinovation Disrupt Fund".

[414] EIB, "Environmental and Social Data Sheet" (May 2020).

[415] See IFC Project Information and Data Portal, "What does IFC disclose?"; and ADB, *Artificial Intelligence in Action: Selected ADB Initiatives in Asia and the Pacific* (2024), in which AI initiatives financed by ADB are described without discussion of any preventive or mitigation measures to address AI-related project risks.

[416] EIB, "EU funds co-financing 2014–2020 (PL)", 16 September 2014; and Inteligentny Rozwój, *Lista Projectów* [Smart Development, *List of projects implemented under the Smart Growth Programme 2014–2020*, available in Polish].

© Adobe Stock/by oselote

Box 27 Example of a project supporting better AI

IDB is investing in an algorithmic justice platform designed to identify and mitigate bias and potential discriminatory impacts in decision-making processes that use AI.[417]

C. TRENDS AND CONCLUSIONS

The evidence reviewed by OHCHR indicates that MDBs and other DFIs are encountering significant and increasing digital risk exposure in their portfolios. At the time of writing, digital risks had not consistently been identified and factored into project design, supervision and mitigation and remedial actions, on the basis of clear, transparent and enforceable policy requirements. To the extent that this conclusion is valid, it raises the concern that E&S risks, harms and costs associated with DFI-digital projects may have been, and may continue to be, externalized to communities on a potentially large scale.

More specifically, the review conducted for the present report supports the conclusions set out below.

[417] See IDB, "QuantilAI: Algorithmic Audit", although few details are given. As algorithm audits have matured, so have concerns about their independence and effectiveness. See also Abeda Birhane and others, "AI Auditing: the Broken Bus on the Road to AI Accountability" (January 2024); and Victor Ojewale and others, "Towards AI Accountability Infrastructure: Gaps and Opportunities in AI Audit Tooling" (February 2025).

Lack of consistent, transparent and enforceable requirements to assess and address digital risks

- **DFIs have clearly and consistently identified digital opportunities, but less so digital risks.** As highlighted in the subsection on digital strategies in section A above, many DFIs support digital transformations in the public and private sectors and some are putting digitalization at the very centre of their work. Attention to digital risk varies considerably between DFIs; however, none of the DFIs reviewed in this report yet appear to be taking a proportionate approach to identifying and addressing digital risks.
- **DFIs do not yet have consistent, transparent and enforceable requirements relating to the identification, assessment and addressing of digital risks** for the financing of projects and advisory services with digital components. At the time of writing, this picture was starting to change; however, in the absence of clear, robust and binding digital risk management requirements applicable across all operations and advisory services, DFI financing for digital projects may more likely be associated with irremediable harms. The concerns highlighted further on flow from this premise.

Lack of consistent and transparent consideration of long-term systemic impacts

- **DFIs are funding policies and projects that may ingrain digital risks and impacts for future generations, creating path-dependency and lock-in effects.** DFIs are increasingly supporting digital initiatives and regulatory reforms that are predicated on citizenship, residence or government services that could affect entire populations in host countries. Large-scale systems operate over long time frames to justify the costs, but no system of this kind is infallible, as discussed earlier, even in countries with relatively advanced regulatory capacities.[418] Digitalization in this context gives rise to new risks and can turbocharge exclusion. DFIs are also assisting Governments and private sector clients in rolling out digital infrastructure that is likely to be in place for decades. Poor design choices could unwittingly enable unrestricted Government or private sector access to personal data for the duration of the infrastructure without users' knowledge of such access, opportunities to consent or avenues for redress.
- **Systemic impacts can be hard to identify and, as a result, do not appear to be adequately considered or disclosed across most projects.** DFIs are increasingly funding broad, system-level projects that extend across sectors, such as the digitalization of public administration. Because of their breadth, such projects give the public sector broad discretion about how the project will be implemented as well as how much information about the effects of digitalization will be disclosed to the public. The technologies themselves are often opaque regarding the type of data that are collected and how collection is carried out, how data is processed and analysed, how it will be put to use, who it may be shared with and who will have access. Most impacts will not be obvious, even to the well informed. Such projects by their nature fundamentally alter the relationship between the State and the public and, in doing so, may exert systemic and enduring impacts well beyond the effects of the digitalization of discrete administrative functions. There also appears to be a significant

[418] See, for example, *Report of the Special Rapporteur on extreme poverty and human rights, Digital welfare states and human rights* (A/74/493).

lack of detail in project descriptions about how (broadly worded) project objectives will be accomplished and what technologies will be used.

- **It is often assumed, without questioning, that digital solutions are always the best option.** Technology solutionism, the assumption that development challenges can best be solved through (more) technology and leapfrogging, seems to permeate most DFI digital strategies. Implicitly, if not explicitly, digitalization is taken as the default. This mindset, and insufficient consideration of the project context and alternatives, may inadvertently increase E&S risk exposure. In-depth *ex ante* analysis is needed to determine the best option in any specific context, without automatically tipping the scales in favour of full-scale digitalization.[419] Some nuance and specific contextual considerations are needed in order to understand whether and how digital technology can be leveraged appropriately.

Lack of transparency about principles and standards driving DFIs' approaches

- **Objectives and standards.** DFIs are not always clear about which international standards are applied in project implementation. Given the increasingly contested digital regulatory space,[420] it is crucial for DFIs to have clarity and align with the international human rights framework.
- **Tools and approaches.** Although some DFIs have developed a wide range of publications and tools on digital issues (see section B above), it can be difficult for external stakeholders to understand how and when such tools and approaches are applied, how they may shape financed projects and whether they provide the basis for compulsory digital risk management requirements.
- **Prerequisites for providing financing.** There seems to be very little clarity in digital strategies and project documentation about the prerequisites for financing digitalization projects in particular contexts. For example, should DFIs fund digital identification programmes in countries without appropriate data protection, citizenship rights, independent judiciary or judicial oversight of security forces? Should private sector AI developers be financed if they do not have appropriate policies and procedures to test their algorithms and commitments to ensure the responsible use of the technologies? Should DFIs fund the development of technologies that can be used for surveillance in countries where the repression of political opposition, minorities or other population groups is rife?

Inadequate environmental and social management systems for digital risks

- **Only a subset of digital risks is generally being considered.** Available digital strategies and project documentation indicate that, for the most part, DFIs have tended to focus on only a subset of potentially relevant digital risks, particularly data protection, cybersecurity and the risk of exclusion from services. Privacy is at the core of the digital ecosystem;[421] however, it should not overshadow the wider set of potential impacts outlined in this report.

[419] See box 24 on an ADB e-health project in Tonga.

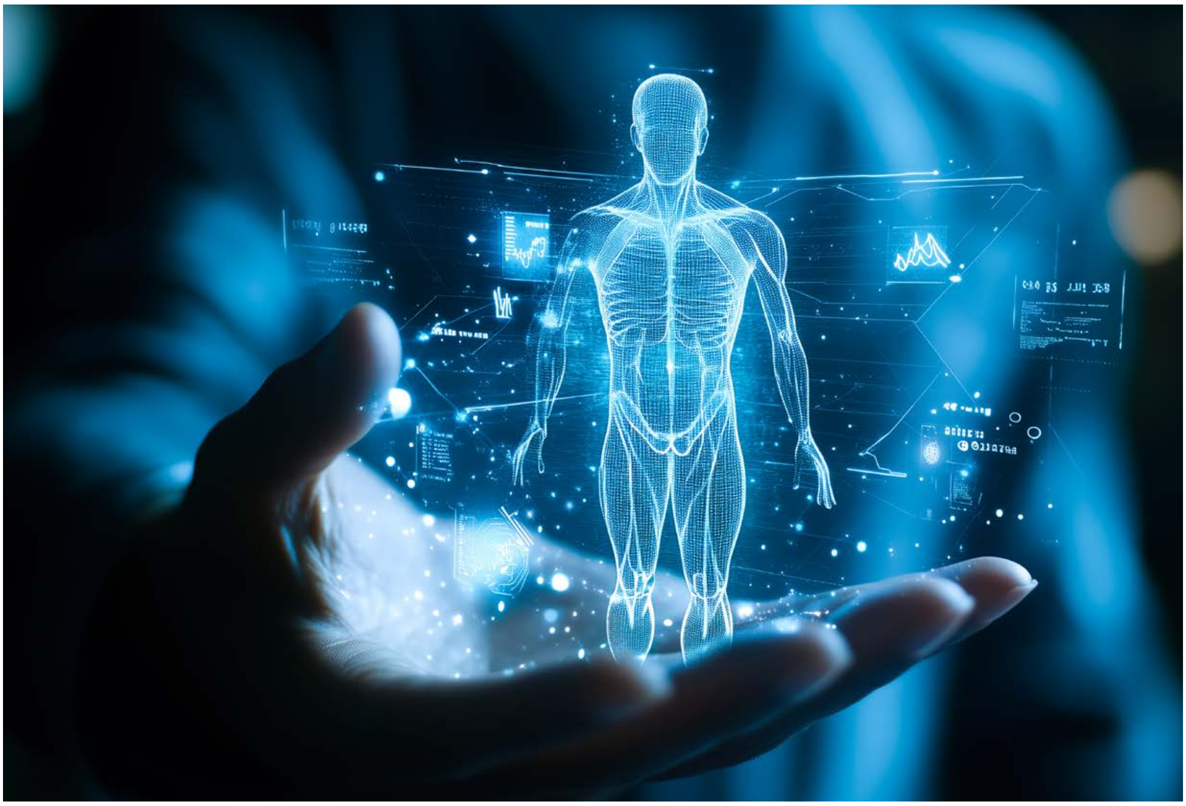
[420] Colum Lynch, "Exclusive: At UN, China seeks greater state control over internet", Devex, 21 May 2024.

[421] For examples of types of adverse impacts on the right to privacy across a wide range of public and private sector functions, see Privacy International, "Submission for the UN report on the right to privacy in the digital age", 15 June 2022; and OHCHR report, *The right to privacy in the digital age* (A/HRC/51/17).

- **There is a lack of publicly disclosed information about digital risks.** Project documentation rarely provides sufficient detail to enable affected individuals to understand if they are at risk and whether proposed mitigation measures are adequate. Consistent with leading practice in MDB public information and safeguard policies, project disclosures should provide adequate information, in a timely fashion and accessible formats, so that affected people can identify concerns at the earliest possible stage, prior to project approval, and irremediable impacts can thereby be avoided.
- **In digital projects, due diligence may not always occur at the most appropriate time to identify risks.** Where DFIs are financing new business models or new start-ups, as many increasingly are, due diligence may be carried out before the start-up is fully developed or launched. In such cases, even if the model, product or approach can be explained to the DFI, it will not have been tested and there may be no evidence of its performance or potential impacts at the time of due diligence. This is particularly concerning with regard to the rapid proliferation of AI-driven projects.[422] Staged due diligence and strengthened monitoring and supervision may be required for these kinds of projects, allowing DFIs to assess potential impacts at a time when the impact of the technology is clearer.[423]
- **There is insufficient clarity on what is required to respond to risks.** Just as there is no routine or standardized approach to identifying digital risks, there appears to be no routine or standardized approach to implementing prevention or mitigation actions. "Digital action plans" may serve a useful function in making digital risks and mitigation response actions clear, concise and actionable, analogous to action plans in E&S safeguards on resettlement, Indigenous Peoples and other issues.
- **There is little or no discussion of stakeholder engagement on digital projects.** Project proponents may have little experience or incentive to identify and meaningfully consult with relevant stakeholders in digital projects, particularly if there is no formal requirement to do so. Effective stakeholder engagement is likely to require new formats and approaches, including with regard to protection against reprisals.
- **Digital risks rarely appear to be addressed in private sector projects.** The documentation available on private sector projects is much more limited than for public sector projects. Only a fraction of the project summaries and E&S documentation reviewed in private sector projects raised any concerns about digital risks. Improved transparency practices are needed on this important issue.

[422] Center for Financial Inclusion, *Investing in Equitable AI for Inclusive Finance: A Risk Management Guide for Impact Investors* (2023), p. 5.

[423] In the view of OHCHR, as a matter of policy, any proposal for a phased approach to E&S safeguard implementation should be defined narrowly and carefully, and be subjected to a high standard of justification. For example, categorical carve outs for E&S safeguards in conflict settings or for complex operations should be avoided.



© Adobe Stock/Generative AI/by Nanthiwan

Lack of awareness, expertise and internal capacity

Notwithstanding their rapidly expanding digitalization portfolios, regulatory advisory work and other activities, most DFIs seem to be at an early stage of their digital journeys, with relatively limited engagement with digital risks at the project level, beyond those which have gained commercial attention. The development of necessary internal awareness and technical capacities to effectively support and supervise clients and consultants is in most cases a work in progress, as reported by various DFIs themselves.[424] The internal capacity-building challenge is particularly pressing in rapidly evolving fields such as AI.

[424] See, for example, "The EBRD's approach to accelerating the digital transition, 2021–25", p. 3. EBRD notes that it is on a digital journey and that it is growing its capacity and expertise, but nonetheless (p. 18) lists a range of regulatory advisory projects in which it is involved. See also EBRD, "Understanding Digitalisation: Case Study of the Kafr El-Sheikh Wastewater Expansion Project" (2023), pp. iv and 12, where it is noted that "the EBRD's relative inexperience in explicitly supporting digitalisation was visible in this case study" and that "the Bank's partners also observed how the Bank developed its own, initially rudimentary, digital capacity and skills", while it is also noted in a second, related project there was evidence of bank learning. Similarly, ADB stated that it has only "started to explore data privacy, security, and ethics in response to demands from DMCs and the Board of Directors" and that it has a new interdepartmental working group to explore improved approaches to risk assessment and ethical concerns related to digital technologies and their impact for ADB operations. See ADB, "Strategy 2030 Digital Technology for Development Directional Guide: Supporting Inclusive Digital Transformation for Asia and the Pacific" (2022), pp. 11–12 in this regard. The internal capacity-building challenge is clearly a pressing one in view of the complexity, high stakes and potentially irremediable impacts of structural and regulatory reforms associated with digitalization. See also AIIB, *Digital Infrastructure Sector Analysis: Market Analysis and Technical Studies* (2020), p. 9; and World Bank, *Mobilizing Technology for Development*, chap. 3.

Accountability gaps

- **Unclear accountability.** In disclosed documentation, there is often limited discussion on accountability for adverse impacts on stakeholders beyond standard language on roles of project-level grievance mechanisms and DFIs' own IAMs. However, these mechanisms face serious challenges in dealing with harms arising from digitalization projects (see below). Where projects involve multiple actors in the digital ecosystem,[425] responsibility for adverse impacts may be unclear and a willingness to take responsibility even less clear.
- **Lack of appropriate expertise and mechanisms to deal with the uniqueness of some digital harms.** Digital harms differ from harms associated with projects with physical footprints in various ways, as previously discussed. Existing accountability mechanisms may not be appropriately structured and staffed to deal with these kinds of harms. Neither IAMs nor project-level grievance mechanisms have the expertise and skillset to deal with such harms, presumably because they have not yet been required to do so.[426] Fresh thinking is needed on how to conceptualize and make remedy meaningful and operational in the context of harms arising from digital projects, and on the role that the larger remedy ecosystem could play in this regard.
- **Opaque technologies obfuscate accountability.** As discussed earlier, technologies used in DFI-supported projects often lack transparency regarding the type of data collected, methods of collection, data processing and usage, and with regard to the operative algorithms or databases used to train algorithms. This lack of clarity is itself a serious barrier to accountability as it blurs the lines of responsibility.[427]
- **Complex ecosystems obscure accountability.** The reuse and repurposing of data and technologies are at the core of digital innovation, but in common with the opacity of some of the technologies themselves, this could undermine accountability by obfuscating who is responsible for their use.
- **Mismatch in time frames for the materialization of harm.** Digital harms may take time to materialize as a system, product or service is used. The admissibility criteria of accountability mechanisms may need to be revised to take account of this fact. The deadline for submitting complaints should be set according to the time frame within which impacts actually materialize, rather than being tied to project closure or any other fixed cut-off date.

[425] Global Network Initiative and BSR, *Human Rights Due Diligence Across the Technology Ecosystem* (2022).

[426] See Rabi Thapa, "Developing AI for Development", 9 April 2024, in which it is described how some IAMs are starting to use AI to help process complaints, but not about how AI impacts of projects can be dealt with.

[427] Victoria Adelmant and others, *Digitalization as Development*, pp. 22–23 and 67.

© Adobe Stock/by visoot

CHAPTER III
RECOMMENDATIONS – RESPONDING TO THE ANALYSIS

DFIs are carrying out a wide range of initiatives to integrate and elevate digital approaches in their work with private and public sector clients, and are supporting an even wider range of projects through advisory services and financing. OHCHR recognizes the tremendous benefits that digitalization brings and the role that DFIs play in this process, bringing much-needed finance and knowledge to their public and private sector clients. Continued innovation and intensified support will be needed, given the pace of technological change, to ensure that digital development produces consistent positive outcomes for people and the planet.

A. RECOMMENDATIONS FOR ENHANCING THE GOVERNANCE OF DIGITAL RISKS

The expansion of DFI digital portfolios implies the multiplication of a wide range of digital risks. DFIs are increasingly providing technical support to help clients address these risks and a few have begun updating their E&S safeguard policies to this end, although this is often limited to specific digital risks *ex ante* rather than being driven by a contextual and project-specific risk identification process. The attention given to digital risks varies across DFIs and, to some extent, across sectors. Based on the evidence available to OHCHR, to date, risk management for projects with digital components does not yet appear to have been carried out in a consistent and transparent manner.

The findings generated by the present report point to the need for a more intentional, transparent and systematic approach to digital risk identification in DFI-financed projects, and to the consistent application of tailored prevention, mitigation and remedial measures, underpinned by independent accountability. More specific recommendations in relation to this subject are detailed below.

1. BASELINE ASSESSMENT AND STOCKTAKE

DFIs are engaged in a wide range of activities in the digital sphere, as noted repeatedly throughout this report. However, it is very difficult to gain a clear overall picture. Given that the financing of and the support given to digital activities seems set to expand, it would seem prudent and opportune for each DFI to carry out a baseline assessment of digital risks in their portfolios and an institutional stocktaking of the effectiveness of their existing policies, procedures, practices and projects in anticipating and managing a wide range of digital risks and impacts. Such a process should ideally draw on any internal evaluations focused on the impact of digitalization and be the subject of consultation with IAMs and external stakeholders.

2. BALANCED DIGITAL STRATEGIES

DFIs face real challenges in the digital sphere in fulfilling the "do no harm" dimension of their mandates. More balanced strategies appear to be needed, setting out clearer boundaries with regard to what kinds of projects will and will not be supported and how digital risks will be addressed. A balanced strategy would clarify how project benefits will be realized in accordance with an institution's mandate, while risks are identified and mitigated, to ensure the fulfilment of project-level and institutional goals.

Addressing risks is indispensable but not straightforward. As noted by the World Bank Independent Evaluation Group, "Addressing DTT [disruptive and transformative technologies] risks and adhering to the do no harm principle may require the Bank Group to navigate sensitive ethical and political issues and advise clients on them".[428] A wide range of risk factors, operational challenges and dilemmas faced by DFIs in the context of digitalization, which should inform the objectives, tone and content of DFI digital strategies, have been documented in the present report.

The dilemmas include:

- How should institutions deal with requests from sovereign borrowers that have neither the commitment nor the capacity to implement appropriate safeguards to protect users from misuse? It is one thing for DFIs to support appropriate health and education programmes in authoritarian settings where financing provides critical services directly to populations; however, it is quite another matter for DFIs to use public funds to finance technologies that can, even if inadvertently, become tools of government oppression.
- How should DFIs respond to the rising and challenging demand for digital sovereignty[429] in its different forms, helping countries make appropriate choices on matters such as strengthening data governance and protection and regulating data flows on which the digital economy depends, while respecting digital rights?
- How should DFIs respond to demand from clients for AI-driven solutions, given the particular uncertainties and potential systemic risks that may be involved?
- How should DFIs deal with dual-use items and what guardrails would be appropriate in this context? For example, DFIs mandated to support development and the SDGs should not be supporting dual-use items that can be used for military applications. But how clear are those lines and what kind of oversight and accountability mechanisms should apply?
- How should DFIs weigh up potential changes in Government, particularly in fragile and conflict-affected settings, when planning and financing longer-term projects, such as large-scale digital identification programmes, e-government platforms and telecommunications infrastructure? It has been estimated by the World Bank that 60 per cent of the world's extreme poor will live in countries affected by fragility, conflict and violence by 2030.[430] Given the potentially vast changes that some digital projects entail,

[428] World Bank, *Mobilizing Technology for Development*, p. xvi.

[429] See, for example, ECDPM, *Global Approaches to Digital Sovereignty*.

[430] See World Bank, "Fragility, Conflict & Violence".

careful assessment is needed of the long-term consequences for the given country, taking into account political volatility and potential consequences of regime change.[431]

These are complex issues, but without clear guidelines set out in strategies, the public will have no sense of what principles and decision-making criteria will be applied to projects and programmes to be supported, and what types of issues are being considered in particular contexts. Such questions require transparently reasoned and thoughtful guidance based on alignment with global standards.[432] The ground-breaking work of DFIs and other partners in developing a framework for ethical and responsible artificial intelligence[433] may provide inspiration in this regard.[434]

Recommendation

DFI digital strategies should specifically identify and address digital risks alongside digital opportunities, in order to signal to staff, clients and stakeholders that institutions take these risks seriously and will require that the risks are addressed as part of their support.

3. CLEARER EVIDENCE AND PREREQUISITES FOR INVESTMENT AND ADVISORY SERVICES

As noted above, DFIs face many operational challenges and dilemmas in their ever-growing digital portfolios. Staff, clients and stakeholders need clearer criteria about what DFIs will and will not support through financing and advisory services. In some cases, these decisions will be driven by concerns that certain digital products or services or digital transformation actions are simply too risky. In other cases, contextual risks may be the deciding factor. OHCHR understands that thinking and guidance development is already under way in some DFIs, although emerging guidance is not always available to the public. Alternatively, even where relevant guidance is made public, it may not always be possible for external stakeholders to understand what tools are being used by particular DFIs in any given context.

DFIs and their clients should be encouraged to develop a more detailed evidence base before, during and after the implementation of a digital project. Given the dynamic and often disruptive character of digital innovations, evidence of what works and what does not in various contexts will be an ever-evolving challenge. At the time of publication, as noted, the justifications in project documentation for many of the projects reviewed are not always supported by clear and convincing evidence: for example, claims may be made about reducing corruption through digitalization without any baseline work showing the levels of corruption and which aspects of that corruption could be tackled by a proposed digital system. A lack of research, baseline work and ongoing monitoring means that neither DFIs nor the clients nor

[431] See the references in footnote 112.

[432] ECDPM, *Global Approaches to Digital Sovereignty*.

[433] See box 27 on AI.

[434] Edgar L. Cabanas, "The great tech revolution: artificial general intelligence & multilateral development banks"; and Rabi Thapa, "Developing AI for development".

stakeholders have appropriate analysis of the actual impact of these projects, measured against their theory of change. While DFIs are ramping up their knowledge products on digitalization more generally, this emphasis on a knowledge-led approach also needs to be reflected at the project level.

When putting in place appropriate parameters for their digital financing and advisory services, it would be desirable for DFIs to:

- **Update exclusion lists to account for digital risks.** DFIs use exclusion lists to identify projects that they will not finance. Many of the exclusions are based on international law standards. Many exclusion lists have not been updated for years,[435] with the exception of new exclusions for coal projects in some lists in line with the Paris Agreement on climate change. There are currently no exclusions for any kind of harmful digital products and services. Exclusion lists are a blunt instrument and might be seen as antithetical to expectations that DFIs should remain engaged as far as possible and build and exercise all available forms of leverage for positive E&S outcomes.[436] Nevertheless, there may be particular digital risks that are so inherently problematic or potentially harmful from a human rights perspective, and whose impacts are so challenging to prevent or mitigate, that an outright exclusion is warranted. A ban on the use of facial recognition technology in particular circumstances may be one example, following emerging practice in some countries.[437] Certain artificial intelligence uses, such as those in the European Union Artificial Intelligence Act, that are considered "unacceptable risks" might also be proscribed.[438]

Box 28 Example of an updated exclusion list

BII has a specific fund exclusion policy (applicable to funds and their portfolio companies) on the following:

- AI, where it poses unacceptable risk as defined in the European Union Artificial Intelligence Act;
- Social media targeting children and other vulnerable people, and dating applications, given the significant gender-based violence and harassment and child exploitation risks associated with the latter.[439]

[435] For example, the exclusion list of IFC dates to 2007. See IFC, "IFC Exclusion List (2007)".

[436] See, for example, OHCHR, Guiding Principles on Business and Human Rights, principle 19; OECD, *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct* (Paris, 2023); and OECD, *OECD Due Diligence Guidance for Responsible Business Conduct* (Paris, 2018). The EBRD *Environmental and Social Policy* (2024) reflects clear requirements for building and exercising leverage in the case of labour impacts in supply chains (para. 45).

[437] See, for example, Lu-Hai Liang, "Brazilian groups call for ban on facial recognition", Biometric Update, 16 October 2024; and Kate Conger and others, "San Francisco bans recognition technology", *New York Times*, 14 May 2019.

[438] See European Union Artificial Intelligence Act, paras 29–44. The Act prohibits the deployment "of certain AI systems with the objective to [sic] or the effect of materially distorting human behaviour, whereby significant harms, in particular having sufficiently important adverse impacts on physical, psychological health or financial interests are likely to occur." Other prohibitions include social scoring AI: classifying people based on behaviour, socio-economic status or personal characteristics; biometric identification and categorization of people; real-time and remote biometric identification systems, such as facial recognition. Exceptions may be allowed for law enforcement purposes in "exhaustively listed and narrowly defined situations, where the use is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks."

[439] Summary of information provided by BII in September 2024, on file with OHCHR.

- **Develop clear decision criteria and processes for digital projects ("no project" scenarios, red flags and escalation scenarios).** These could include:
  - **Digital alternatives analysis.** Guidance on carrying out an analysis at the earliest stage of a project to determine if digital is the best option in a particular context (see box 2).
  - **Red flags for digital risks.** These would signal the need for intensive pre-project appraisal in order to understand the risks and long-term consequences of projects in particular contexts and to put in place appropriate prevention and mitigation measures. For example, funding digital ID projects in contexts where discrimination against particular population groups is deeply entrenched and funding AI systems that may create unacceptable risks.[440]
  - **Escalation criteria.** These would signal where more extensive analysis and senior management judgement calls are warranted. This could in turn prompt new approaches or definitions of high-risk projects in various sectors. For example, projects that would fundamentally transform the way the State interacts with the public, such as through e-government technology in a high-risk context.
- **Develop prerequisites for support.** Based on the research undertaken for this report, it is not clear to OHCHR if any DFI has articulated and consistently applies specific prerequisites for supporting digital projects, such as the existence of effective data protection laws and data protection authorities (in the case of sovereign borrowers) or data protection policies (in the case of private sector clients). Moreover, with the exception of the World Bank ID4D legal assessment tools,[441] it is not always clear how the effectiveness of data protection laws, policies and institutions should be assessed and whether DFIs have relevant tools or analysis frameworks for other relevant areas. Where clear prerequisites are not in place at the time of project appraisal, particularly strong justification should presumably be required to proceed with the project based on assessments of anticipated project benefits, the severity (involving scale, scope and remediability) of any human rights risks and impacts, and the leverage options available to the DFI, individually and collectively, to effectively prevent and mitigate identified risks within a reasonable time frame.[442]
- **Support clients in developing stronger evidence bases that guide the digitalization choices in proposed projects.** Expected impacts need to be actively monitored alongside proactive identification of new harms as projects progress.

[440] See the European Union Artificial Intelligence Act, paras. 29–44, for additional examples.

[441] See, for example, the World Bank IBRD IDA, *ID Enabling Environment Assessment (IDEEA) Guidance Note* (2018).

[442] See Guiding Principles on Business and Human Rights, principle 19. The reasonableness (or otherwise) of the mitigation time frame should depend on the severity of the identified risks.

Recommendation

DFIs should develop clear guidance for staff on the points above to support them in making difficult decisions in fast-moving areas of digital development. Where potential harms to people are particularly severe (in terms of scale, scope and irremediability) and where there would appear to be no viable prospects for mitigation, consideration should be given to incorporating these risks within exclusion lists.

4. APPROPRIATE DIGITAL SAFEGUARDS

As discussed earlier, the current generation of E&S policies does not provide much policy guidance to help either DFIs or their clients identify, address and account for digital risks. Existing safeguards simply were not designed to address the new kinds of challenges that digital transformation presents. At the time of writing, ADB and EBRD had shown themselves to be first movers in addressing this gap, by integrating data protection, privacy and cybersecurity in their updated safeguard policies. However, in light of the analysis in this report, OHCHR suggests that more comprehensive, multifaceted approaches to digital risk management may be necessary.

Based on the research undertaken for this report, to ensure that digital risks are more consistently and effectively addressed, OHCHR recommends that a three-tiered approach be taken to the adaptation of DFI E&S safeguards in order to appropriately address digital risks. Before detailing these proposals, it is first necessary to consider why digital-specific safeguards are indispensable.

Case for specific safeguards responsive to digital risks

There are several main reasons why E&S safeguard policies need to be specifically tailored to account for digital risks. These are set out as follows.

DFIs may have a range of policies, procedures and tools that guide their digital work apart from E&S safeguards. However, generally speaking, these policies, procedures and tools are:

- Not specifically focused on the assessment and management of the E&S impacts on stakeholders of DFI-financed projects and advisory services.
- Not always made public, which means stakeholders have no means of knowing how project-related decisions affecting their rights and interests are made, the conditions that are applied to DFI financing and the requirements clients are required to meet.
- Not subject to the IAMs of DFIs or other mechanisms for ensuring accountability and remedy for impacts on stakeholders.[443]

[443] Some DFIs, such as the World Bank and EBRD, have also set up grievance redress mechanisms that seek to address complaints from stakeholders through a management-led process as an alternative to complaint-handling through an IAM. The accountability architecture in any context needs to be consulted on publicly and thought through carefully in order that the various components operate efficiently and equitably from the perspective of project-affected people and are not in tension.

Subject to limited exceptions, the current generation of E&S safeguards are not fit for the purpose of dealing with digital risks and impacts, as illustrated in the analysis in chapter II, because:

- They do not identify digital risks as issues to be assessed and managed, as seen from the project analysis (see chapter II), which means that they are often not identified and managed by either E&S teams or investment teams.
- Digital risks and impacts are very different from risks and impacts arising from traditional investment projects (see chapter I). Safeguards largely emerged from experience concerning projects with more tangible physical footprints, such as dams, mines, agriculture and large-scale infrastructure and to a great extent still bear that legacy today.[444] Simply adding a reference to "data protection" or "digital" to existing safeguards is not enough to reverse-engineer existing E&S safeguards to effectively assess, mitigate and remedy a broad range of digital risks.
- Current E&S safeguards do not have appropriate indicators for categorizing digital risks (see section A of chapter II). Current classification systems are ill-suited to assigning appropriate risk categorization. Under most existing safeguard systems, projects with potentially significant human rights impacts across large sectors of the population (such as projects concerning digital identification) may well be classified as low-risk projects because they do not have a significant physical footprint. The tendency to categorize ICT projects as low-risk (category C) projects is evident even in the application of more recent safeguards.[445] Innovative digital products and services developed by micro-entrepreneurs can have a very significant impact if their products are widely used. Contrary to other types of projects, the size of the enterprise is not a reliable indicator of the size of the impact. Moreover, approaches based unduly on sector characteristics may lack adequate nuance.[446]
- Contextual risk assessment practices under existing E&S safeguards are still in their infancy. The contextual risks for digital products or services are likely to be very different from those involved in E&S risk assessments for more traditional investment projects.
- Risk assessments need to be calibrated to consider a whole new set of digital risks in both direct and financial intermediary projects.
- Digital projects require different types of prevention and mitigation and remedial measures than those stipulated in the current generation of E&S safeguards.
- Digital projects require different approaches to supervision: conventional E&S monitoring reports and site visits are unlikely to effectively address digital impacts for projects with a significant digitalization component or focus.

[444] Sometimes project teams are identifying digital risks as social risks and disclosing them. See, for example, World Bank, "Jordan – People-Centric Digital Government Program for Results" (Washington, D.C, 2024), p. 19, in which weak protection of personal data is identified as a direct social risk. However. practice is uneven, even among the DFIs that have so far paid more attention to these issues.

[445] For example, the IFC "Guidance note on financial intermediaries" (September 2023), table 1, p. 5, notes that for equity investments in venture capital funds, the fund must screen an investee company involved in non-information-technology-related activities (manufacturing, logistics, agriculture, etc.) against key requirements of the IFC Performance Standards, but that for "IT-related activities, the assessment focuses on PS2 (labor and working conditions)". See also DFC, "Environmental and social policy and procedures" (July 2020), sect. 2.6, in which "telecommunications projects not involving new physical infrastructure" are classified as category C, suggesting a focus only on the physical footprint of these projects rather than their broader connectivity purposes and associated risks and impacts.

[446] DEG, AfricaGrow and Steward Redqueen, *Responsible Investment in Technology*, sect. 2.2.

- The prevailing conception of "affected stakeholders" is too limited for digital projects. Most existing E&S safeguards reflect a geographic limitation as to who is and who is not a project-affected stakeholder, defined in relation to a physical project location.
- Different approaches and expertise will usually be required. Digital processes and risk factors may be highly technical, opaque, complex and/or interlinked, and may be buried in coding language that only experts can understand. DFI staff will need to have appropriate expertise in order to be able to ask the right questions and provide effective support to clients.

There are several reasons for adopting a fit-for-purpose set of safeguards that addresses digital risks. Annex I outlines a possible structure of updated safeguards that address digital risks. In the view of OHCHR, specific digital safeguards would:

- Provide clarity, consistency and transparency about what DFIs are doing to identify and manage digital risks.
- Be sufficiently flexible to cover a wide and growing range of digital risks and respond to the rapidly evolving character and dynamism of the digital landscape. The purpose would not be to constrain adaptation to new developments, but instead to ensure that DFIs and clients are taking a balanced approach to engaging with both risks and opportunities.
- Provide much needed guidance and a clear mandate to DFI staff to address digital risks.
- Provide accountability to shareholders in this fast-expanding field of DFI operations.
- Be risk based (in common with existing safeguards and general practice on managing digital risks), meaning requirements would correspond to risks, bearing in mind the often far wider scale of risks as identified in section C of chapter I (on how digital risks differ from E&S risks).
- Consolidate within a single policy framework the multiple approaches currently being taken, while encouraging the development and deployment of complementary tools as needed.
- Describe the various forms of leverage (contractual and otherwise, individual and collective) that should be built and deployed to require clients to address digital risks.
- Prevent DFIs inadvertently contributing to harms (including, at times, severe and pervasive harms) through lack of awareness or consistent attention to these issues.
- Define the standards to which DFIs and clients will be held accountable.

Such fit-for-purpose safeguards would also benefit from closer alignment with the United Nations Guiding Principles on Business and Human Rights. As indicated in the introduction to the present report, the relevance of human rights to digital risk management has procedural as well as substantive dimensions, relevant to all stages of the investment project cycle. E&S safeguards of bilateral and multilateral DFIs are beginning to align with the Guiding Principles, the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct and related regulatory requirements at the regional and national levels. However, across the board, many critical gaps still continue to exist.[447] Closer alignment between DFI safeguards and the

[447] For a more comprehensive discussion, see OHCHR, *Benchmarking Study on Development Finance Institutions' Safeguard Policies*.

Guiding Principles and related standards may strengthen digital risk management in a range of important ways, including the following:

- Digital risk management would be genuinely risk-based throughout the whole value chain, not only focused on upstream supply chains, but also including downstream users and consumers of technology. Upstream supply chains should not be limited to consideration of "primary suppliers".[448]
- E&S risk assessments would prioritize "severity" of risk, which is defined in the Guiding Principles and the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct as "scale, scope and irremediability".
- Contextual risk assessments for digital projects would explicitly take into account internationally recognized human rights and national and legal frameworks.[449]
- Digital risk management would explicitly take into account the involvement of clients and DFIs in impacts, or in other words, the extent to which actions or omissions of the DFIs and/or the clients caused or contributed to an adverse impact, or alternatively the extent to which impacts are directly linked to the products or services of the DFI or clients through a business relationship.[450]
- The responsibility to address digital impacts would not be limited to the extent of the existing control of the DFIs and/or the clients, but rather, would be predicated on a requirement to build and exercise all available leverage, individually and collectively, to address those impacts.[451]

[448] At the time of writing, the EBRD *Environmental Social Policy* (2024), constituted "best practice" in this regard. At least for "core" suppliers (EBRD, "Environmental and Social Requirement 1" (2024) para. 21), requires "significant" E&S risks to be prevented or mitigated and impacts remediated, without any necessary limitation to primary suppliers. Certain digital risks (notably privacy and data protection) are explicitly within scope: EBRD *Environmental Social Policy*, para. 2.13; and EBRD, Environmental and Social Requirement 1, para. 17 and sect II: definitions. Moreover, the EBRD *Environmental Social Policy*, para. 2.5, and EBRD, "Environmental and Social Requirement 1", paras. 1 and 3, explicitly require that human rights risks and impacts should be addressed.

[449] The ADB *Environmental and Social Framework* is a good example. In common with the EBRD *Environmental Social Policy*, digital risks are to some extent explicitly within scope of the ADB Environmental Social Framework. In the ADB's Policy, para. 24 (viii), it is required that risk classification take into account "digital risks for which the host country may have limited legal and data privacy; and regulatory framework, institutional capacity and understanding, that may have potential for significant E&S impact." Contextual factors according to the ADB Policy, para. 24 (x) and (xii), include, respectively, "civic space and freedoms of expression, association and assembly" and "information relevant to host country obligations under applicable international agreements". The latter requirement indirectly imports a potentially wide range of digital risk information from the United Nations human rights system.

[450] EBRD, "Environmental and Social Requirement 1" (2024), para. 21, provides that the supply chain risk management system (or client's Environmental and Social Management System) "will take into account: … (b) whether the client caused, contributed or is directly linked to these risks and impacts…". See International Climate Initiative (IKI), "Safeguards Policy of the International Climate Initiative" (January 2023), pp. 9–10, of the Government of Germany, which explicitly requires that the lender's involvement in impacts be taken into account, in addition to that of the client, thereby aligning more directly with the Guiding Principles on Business and Human Rights and the responsible business conduct standards, and, in principle, offering a more robust framework for remediation. Also in the "Safeguards Policy of the International Climate Initiative", pp. 9–10: "In accordance with the UNGPs, the due diligence process distinguishes respective actors in line with the level of involvement in the 'responsibility chain' in possible adverse impacts on the environment and people. A distinction is made between three levels of involvement… [cause, contribute, and direct linkage, in line with the Guiding Principles]. An actor's due diligence obligations differ in line with the level at which the actor is involved in the occurrence of damage…As the providers of the funding, the responsible ministries and ZUG are involved in potential adverse impacts primarily at the level of "direct link" and to a lesser extent at the level of the contribution. This is because the responsible ministries and ZUG maintain business relations with implementing organizations which can cause damage or contribute to damage via their activities or omissions in the context of a supported project. They can contribute to possible adverse impacts if they fail to comply with their due diligence obligations as they review and monitor the safeguard standards throughout the project cycle".

[451] See, for example, EBRD, "Environmental and Social Requirement 2: Labour and Working Conditions", 2024, paras. 45–47, which contains requirements (limited to labour impacts) that clients build available leverage and exit projects responsibly.

- Any residual impacts from digital projects would need to be remedied, not merely compensated or offset, through a robust and comprehensive approach that takes into account all relevant parties' involvement in those impacts.[452]

What could a stand-alone digital safeguard look like?

OHCHR proposes a three-tiered approach to adapting existing E&S safeguards to the demands of digital risk assessment and management:

- Adapting sustainability policies (which are the requirements applicable to DFIs) to include specific requirements for digital risks;
- Adapting existing performance standards (which are the requirements applicable to clients) so that the digital risk issues embedded within existing E&S standards are identified, addressed and mitigated;
- Adding a new digital-specific performance standard, applicable to clients, that relates to digital components of projects.

A three-part structure of this kind is outlined in annex I. OHCHR recognizes that this is only a schematic proposal intended to prompt further discussions among DFI management, shareholders and other stakeholders about the most appropriate form of policies to guide this growing area of DFI activity. In line with the practices of the leading MDBs, a broad, multi-stakeholder approach will be necessary when developing a revised set of safeguards.

OHCHR also recognizes the lengthy preparatory and consultation processes that are needed for DFIs to undertake updates of their safeguard policies and that these policies typically have a long lifespan and are not always easy to amend. OHCHR also notes that these processes present challenges in the context of evolving and sometimes contradictory national, regional and international legal frameworks. The recommendations on the potential role E&S safeguards offered in the present report should not distract from the need to take other necessary measures to manage and disclose management of digital risks in the interim.

Recommendations

DFIs should update and adapt their board-approved E&S safeguard policies to reflect the demands of digital risk assessment and management, taking a three-tiered approach as outlined in annex I.

This would entail:

- Adapting sustainability policies (containing the requirements applicable to DFIs) to include specific requirements for digital risks;
- Adapting existing performance standards (containing the requirements applicable to clients) so that the digital risk issues embedded within existing E&S standards are identified, addressed and mitigated;

[452] For a fuller discussion of this issue see OHCHR, *Remedy in Development Finance: Guidance and Practice* (2022).

- Adding a new digital-specific performance standard or requirement, applicable to clients, that relates to digital components of projects.

Until E&S safeguard policies are updated, clear and transparent guidelines (which may include directives and procedures) should be developed in order to require the assessment and management of a wide range of digital risks in the interim. This may include moratoriums in relation to certain types of projects. OHCHR recommends that interim guidelines be publicly disclosed.

Updated E&S safeguard policies should include rigorous requirements for "contextual risk assessment", which should explicitly influence project E&S risk classification. In line with leading practice among MDBs, contextual risk factors should include the legal, regulatory and institutional framework for digitalization, "civic space and freedoms of expression, association and assembly" and "information relevant to host country obligations under applicable international agreements".[453]

The specific requirements of updated E&S safeguards should explicitly be aligned with the Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct, which are increasingly reflected in regional and national regulatory frameworks and set higher standards than most DFI E&S safeguard policies on due diligence and risk management throughout the value chain, including downstream impacts on users and consumers of digital products and services.

5. APPROPRIATE RISK MANAGEMENT APPROACHES AND TOOLS

As noted in chapter II (section 5), several DFIs, particularly the leading MDBs, have developed a wide range of tools covering many different digital topics, including digital identification, cybersecurity and digital maturity preparedness for the digital economy. However, not all tools that play an important role in shaping the management of digital risks and impacts on stakeholders appear to be publicly disclosed.[454] Also, importantly, the analytical outcomes of the application of these tools are not disclosed in a systematic way in project documentation.

[453] See the ADB *Environmental and Social Framework* (E&S Policy) (2024), paras. 24 (viii), (x) and (xii), respectively. Contextual and general restrictions on civic space not only limit the possibilities of affected stakeholders to freely express their opinions, free of reprisals, about projects with digital components, but may also indicate a greater risk that digital tools or infrastructure financed by the Bank may be used for purposes other than those stated in the project, such as to enable illegal surveillance or perpetrate reprisals against human rights defenders. More comprehensive recommendations for DFIs related to the assessment of contextual civic space restrictions in the context of development projects can be found in the following reports: Coalition for Human Rights in Development, "Financing Repression" (2024), pp. 46–49; Coalition for Human Rights in Development, *Wearing Blinders: How Development Banks are Ignoring Reprisal Risks* (2022), pp. 51–53; and Coalition for Human Rights in Development, *Misplaced Trust: Why Development Banks Should Not Rely on their Clients to Address Reprisal Risks* (2023), pp. 50–51.

[454] For example, it is noted by BII that as part of its E&S due diligence processes, the BII environmental, social and governance team applies an enhanced and contextual risk tool to identify risks that require due diligence beyond a standard E&S due diligence scope. Screening and scoping guidance provided by this tool include risk themes such as data protection and cybersecurity risks and AI use risks. Summary of information provided by BII, September 2024, on file with OHCHR.

What appears to be needed is a suite of tools (updated as necessary) appropriate to public and private borrowers that would enable DFI teams and clients to screen and assess the full range of digital risks and impacts and design appropriate prevention, mitigation and monitoring measures. Enhanced monitoring and enhanced implementation support to clients seem particularly important given the novel and dynamic nature and unpredictable evolution of many digital risks and impacts. Digital-specific E&S safeguards would mandate the use of these tools. Similar to the experience of other sectors, such as agriculture, health and infrastructure, a range of tools might be used to identify risks and develop appropriate responses, given the breadth of digital transformation initiatives.

DFIs have been instrumental for decades in developing risk and impact assessment tools in the E&S space on a wide range of issues.[455] As such, DFIs should be encouraged to lead in developing broad risk and impact assessment tools for digital impacts,[456] aligned with globally agreed standards. The standards should include the international human rights framework, which is the subject of tool development among numerous DFIs (see box 8),[457] as well as digital-specific standards such as National Institute of Standards and Technology and International Organization for Standardization standards, modified as needed in order to reflect the mandates and stewardship roles of DFIs. Equally, the tools and frameworks developed by DFIs to identify the positive impact of investment projects may need to be adapted to reflect the specificities of digital projects and to enable rigorous evaluation of their development impacts.[458]

The rapid and unpredictable evolution of many digital technologies will no doubt generate an expanding industry of tool development. E&S safeguards, with finite scope and lifespans of at least several years, cannot possibly address all needs. Careful reflection is needed on what core requirements should be explicitly included in safeguards and how safeguard requirements should integrate or interact with the relatively fast-moving world of digital risk tool development elsewhere. Guidance notes on particular issues, technologies and kinds of projects, which can be updated more regularly and flexibly than board-approved safeguards, could play a particularly valuable role in the interpretation and application of core E&S safeguard requirements.

Recommendation

DFIs should invest further in the development of tools for digital risk impact assessment and management, building on emerging digital risk management experience and the long-standing experience of these institutions in developing other kinds of E&S tools (see boxes 7 and 8). These tools should be designed to operate in conjunction with upgraded E&S safeguards that specifically address digital risks.

[455] For example, DFIs are actively involved in the annual conferences of the International Association of Impact Assessment, where a full day is usually dedicated to DFI issues. See, for example, IAIA24 "Proceedings".

[456] See, for example, Danish Institute for Human Rights, *Guidance on Human Rights Impact Assessment of Digital Activities*.

[457] Finnfund commissioned a human rights assessment of its digital sector investments in 2023, but the assessment is not publicly available. Summary of information provided by Finnfund, September 2024, on file with OHCHR.

[458] See, for example, the IFC, "Anticipated Impact Measurement and Monitoring".

6. STRENGTHENING TRANSPARENCY

The World Bank and other leading MDBs have pioneered the development of robust public information policies for international organizations. However, restrictive disclosure practices constitute a serious obstacle to effective digital risk management, particularly for private sector financing institutions.

The research undertaken for this report revealed a lack of adequate public disclosure about digital dimensions of projects sufficient to enable stakeholders to be conscious of risks and initiate necessary avoidance or mitigation measures. The picture varies between DFIs and is generally worse for private sector financing institutions. Even for obviously risky private sector digital projects, such as those involving AI for sensitive issues, facial recognition technologies or health data, there was often nothing in the project disclosures to indicate that digital risks had been considered. Certain projects reviewed by OHCHR did disclose an analysis of specific digital risks at the project appraisal stage; however, practice is not consistent. This state of affairs seems unlikely to improve, in the view of OHCHR, until there are clear and specific disclosure requirements, backed by appropriate expertise and resources.

The latency, complexity and potential pervasiveness of digital risks seem to require a step-change in disclosure practices. Without significant advances in transparency, stakeholders will continue to be unaware of salient risks and the associated harms, and costs may be externalized on a large scale.

Recommendations

DFIs are encouraged to:

- Disclose a description of their risk management approach for digital issues, including their risk appetite in relation to these risks as part of their financing or advisory services in their annual audited financial statements and the accompanying Management Discussion and Analysis statement, which provide an overview of risks to project outcomes.
- Update and disclose exclusion lists, red flags and any accompanying tools that are likely to have a significant impact on stakeholders' rights, in order to provide clarity to staff, clients and all affected stakeholders.
- Issue requirements for the systematic public disclosure of the nature of the digital system deployed and associated digital risks and management measures for relevant projects in updated E&S safeguards and access-to-information policies. Consistent with best practice, any exceptions to disclosure should be narrowly defined, such as cases where the disclosure of a client's cybersecurity weaknesses may expose it to further risks.
- Improve project databases to make searching for digital and venture projects straightforward, so that institutional policy performance can be assessed. Provide clarity on the landing pages of project databases about what types of projects are included and what types are not (for example, providing clarity on whether technical assistance, trust funds and/or support to multi-stakeholder initiatives are included or not).

- Make clearer, consolidated information on digital work available, facilitated by a dedicated webpage that consolidates strategies, tools, guidance, publication and news on digitalization.
- Provide a clearer evidence base for choices made on digital projects through ex-post evaluations and other learning tools. Similarly, DFIs should be encouraged to make E&S monitoring data and reports publicly available.

7. REIMAGINING STAKEHOLDER ENGAGEMENT

In digital projects, stakeholder identification can be far more challenging than in traditional projects with a clearer physical footprint and where proximity is a defining variable. Even in traditional projects, depending on the DFI, the track record of stakeholder engagement is highly variable.[459] However, for digital projects where users, affected stakeholders and local communities may be widely dispersed across geographies, new tools might be required to identify users and impacts on users and non-users alike, and affected stakeholders might need new options to self-identify. In addition, project proponents may have little experience, receive no adequate guidance and be under no contractual obligation to identify and engage with relevant stakeholders in relation to project design and E&S risks.

Successful stakeholder engagement in this context will require new approaches and formats.[460] In many cases, in the context of digital transformations, engagement with all affected stakeholders will not be feasible. But meaningful engagement could be contemplated with a representative mix of stakeholders, including those well informed about digital risks and others who are not. This would ideally include technical experts (for example, experts in health data for health digitalization projects), while also ensuring that the potential impacts of digitalization projects are explained and understood by other (non-technical) stakeholders.[461] Civil society groups, particularly those with expertise in digital rights and experience in operating in similar contexts in other countries, can provide much-needed insight into the nature of potential harms from different types of projects. This may help local stakeholders and project proponents to design more effective preventive and mitigation measures in advance.[462] Given the technically complex and often invisible nature of digital harms, local groups may not otherwise have the knowledge or experience to engage with many digital risks until the resulting harms have already materialized.

OHCHR is not aware of any specific DFI guidance on stakeholder engagement for digital projects. To a significant extent, existing DFI guidance appears to be focused on or framed by experiences in applying the current generation of E&S safeguards.[463] Practice in the private

[459] Shortcomings in information disclosure and stakeholder engagement have been among the most common causes of complaint to the IAMs of MDBs. See, Piper Goeking, "Understanding community harm part 1: consultation, disclosure, and due diligence", Accountability Consol, 1 May 2021.

[460] See the five suggested practices for improving the quality of technology company interactions with external stakeholders described in OHCHR, "B-Tech Project – Five practices to improve stakeholder engagement in tech company due diligence" (March 2023).

[461] See, for example, the World Bank, "End-user perspectives on Fayda ID from marginalized and vulnerable groups".

[462] See, for example, the list of civil society organizations participating in the annual RightsCon conference.

[463] The MFI Working Group on Environmental and Social Standards published a useful guide on stakeholder engagement in 2019, but this does not address engagement with stakeholders where there is a significant digital component. See IDB and others, "Meaningful stakeholder engagement: a joint publication of the MFI Working Group on Environmental and Social Standards" (2019).

sector and among civil society organizations may provide inspiration for DFI guidance on engaging with digital stakeholders.[464]

Finally, the problem of reprisals is a serious impediment to stakeholder engagement in any context. Numerous DFIs and IAMs have adopted statements, policy commitments and strengthened safeguards on reprisals against people who raise concerns about DFI-funded projects. However, it appears that none of these tools has yet to address the rapid growth of online threats, such as malicious cyberattacks, online censorship, arbitrary or unlawful online surveillance, harassment, smear campaigns, disinformation and doxing. This would seem to be a key area of attention in forthcoming updates of DFI E&S safeguard policies.

Recommendations

DFIs are encouraged to:

- Develop or adapt new tools and approaches to identify and meaningfully engage with stakeholders in digital projects, targeted both at institution staff and clients.[465] Such tools should be adapted to the digital environment and could take into account the extensive work undertaken by DFIs to engage with stakeholders during the COVID-19 pandemic.
- Develop or adapt new tools and approaches to meaningfully engage stakeholders, including international civil society and other experts. Transparency, coupled with an openness to engage and answer questions about projects particularly at the early stages of pre-project appraisals, seems particularly important given the rapid pace of change in this area of work.
- Update approaches to protection against reprisals for online participation. This is an area where reprisal guidance should be updated. Clear requirements, including for DFIs themselves, will be needed in updated E&S safeguards, accompanied by detailed procedures, in the view of OHCHR, if implementation is to be taken seriously. DFIs need to take on clearer responsibilities for assessing and responding to reprisal risks, and should implement reprisal-sensitive engagement with project-affected people and civil society organizations working to promote human rights potentially impacted by these projects, given that clients often have conflicts of interest in doing so and are often the source of the threat.[466]

[464] See OHCHR, "B-Tech Project – Five practices to improve stakeholder engagement in tech company due diligence" (March 2023); and European Center for Non-Profit Law and Society Inside, "Framework for meaningful engagement: human rights impact assessments of AI", 8 March 2023.

[465] See the five suggested practices for improving the quality of technology company interactions with external stakeholders described in OHCHR, "B-Tech Project – Five practices to improve stakeholder engagement in tech company due diligence" (March 2023). See also IDB and others, "Meaningful stakeholder engagement: a joint publication of the MFI Working Group on Environmental and Social Standards" (2019).

[466] Specific recommendations related to the assessment of retaliation risks and the implementation of reprisal sensitive engagement can be found in Coalition for Human Rights in Development, *Uncalculated Risks* (2019), pp. 99–101; Coalition for Human Rights in Development, *Wearing Blinders: How Development Banks Are Ignoring Reprisal Risks*, pp. 51–53; and Coalition for Human Rights in Development, *Misplaced Trust*, pp. 50–51.

8. STRENGTHENING ACCOUNTABILITY

Accountability is at the core of DFI value propositions.[467] Accountability entails the performance of clearly defined responsibilities as well as answerability and remedy when things go wrong.[468] Numerous barriers to accountability for harms arising from digital projects exist. The lack of clearly defined E&S digital risk management responsibilities is a fundamental obstacle to accountability. Achieving remedy can be elusive in the best of conditions in the context of traditional DFI-supported projects with a relatively well-defined physical footprint,[469] and presents greater challenges still in the context of digital projects.

Recommendations

There are a number of actions that could be taken to strengthen accountability for digital projects and advisory services, including:

- **Developing fit-for-purpose client grievance mechanisms.** Client grievance mechanisms are not generally well suited to addressing grievances concerning human rights risks and impacts related to digital technologies. This is the case even for companies in the digital technology sector, which have been under pressure to address and provide remedies for digital harms for years.[470] New explicit requirements, specific expertise and procedural adaptations will be needed in order to make available redress mechanisms fit for this purpose,[471] while taking into account relevant experience elsewhere, such as the grievance processes and mechanisms under the General Data Protection Regulation[472] or other similar national experiences.[473] At the same time, advances in digital technologies provide great potential in terms of digital evidence that might support complaints.

[467] See, for example, the World Bank, "External review of the board approved reforms to the inspection panel toolkit and the creation of the World Bank accountability mechanism", 30 January 2024: "Accountability is at the core of the World Bank's value proposition as premier development finance institution".

[468] See, for example, OHCHR and the Center for Economic and Social Rights, *Who Will Be Accountable? Human Rights and Post-2015 Development Agenda?.*

[469] See OHCHR, *Remedy in Development Finance: Guidance and Practice*.

[470] See, for example, Ranking Digital Rights, "The 2025 RDR Index: Big Tech Edition", where big tech and large telecommunications companies are ranked on human rights, including on remedy; and OHCHR, "B-Tech Project – Access to remedy and the technology sector" (2021).

[471] See Women's Digital Financial Inclusion Advocacy Hub, "Advancing Women-Led MSMEs through Digital Financial Inclusion: How policies, products, and grassroots actions enable women entrepreneurs to thrive with digital financial services" (June 2024), p. 14: "Accessibility of complaint management and dispute resolution is another big issue for many customers, especially women. Grievance redressal procedures and recourse systems should be free to access and user-friendly. FSPs should prioritize analyzing gender-disaggregated data in order to make informed decisions and ensure these systems are inclusive of women".

[472] See, for example, the European Union network of data protection authorities that hear complaints about data protection (European Commission, "Information for individuals").

[473] There is also a wider global network of data protection authorities. See Global Privacy Assembly.

- **Strengthening the accountability ecosystem for addressing and remedying digital harms at the national level and integrating attention to digital risks into broader rule of law, justice and security reform work.** There may be a wide range of actors involved in protecting against or adjudicating digital rights violations at the national level in any context, including national data protection authorities, consumer protection authorities, national human rights institutions and so forth. DFIs in a position to do so should consider how they may support this wider accountability ecosystem. Broader initiatives on rule of law and security sector reform should include not only incorporating digital transformations into their systems, but also addressing their role in protecting from harms.[474]
- **Developing fit-for-purpose IAMs.** Just as DFI teams will need to build expertise and capacity (see subsection 9), IAMs teams will require the expertise to assess and address complaints dealing with digital technologies.
- **Developing clearer links to IAMs.** Only one case involving a digital project has been filed to any of the nine IAMs (in August 2024).[475] There may be a range of reasons for this: a lack of disclosure and a consequent lack of awareness among those affected of digital risks and impacts; a lack of connections between stakeholder groups, given that users may be geographically dispersed, depending on the type of project; and, a lack of awareness or disclosure of information about the option to raise complaints with IAMs. DFIs and clients should be required to disclose the option of filing complaints with IAMs, and mechanisms should be encouraged to expand their outreach activities to include actors dealing with digital technology impacts on users and communities.
- **Extending IAM time frames for submitting complaints.** Most IAM procedures include strict time limits within which project-affected people must submit complaints. The most recent policies (at International Finance Corporation/Compliance Advisor/ Ombudsman and Green Climate Fund/Independent Redress Mechanism) require complaints to be submitted within two years from the date of project closure or when harm is detected, whichever is the later date. Digital impacts may take years to materialize and require specific expertise to uncover and address. Hence, it is vital that the admissibility requirements of IAMs are defined by reference to the date of the detection of harm, rather than to the project closure or any other fixed cut-off date.
- **Revising the admissibility criteria of IAMs to include more systemic risks and the different forms of digital harms discussed in this report.**

[474] See footnote 205.

[475] The World Bank Inspection Panel registered a complaint in August 2024 that involves digital dimensions (see "Serbia: Public Sector Efficiency and Green Recovery DPL (P164575)"). Otherwise, based on Accountability Counsel's Accountability Console, there have been 1,955 complaints to date involving the nine current IAMs, but none have involved projects that are demonstrably digital (such as having the word "digital" in the project title). Only three complaints had "technology" in the title. One of these three complaints involved "ICT" and concerned a procurement matter. The World Bank, *Annual Report FY23: Grievance Redress Service* (Washington, D.C., 2024) notes that two complaints were heard about digital development, but a search through the very brief information provided on each complaint shows that the complaints were related to procurement or integrity issues.

9. CULTIVATING EXPERTISE AND SUPPORTING CAPACITY DEVELOPMENT

As noted above, most DFIs are still at a relatively early stage of building their digital expertise and capacities. The picture is a varied and dynamic one, accelerated by the demands of responding to the COVID-19 pandemic. However, digital capacity development does not yet seem to be a key focus in most E&S departments, which are often under-resourced and struggle to deal with their existing priorities.

Nevertheless, anecdotally, it seems that the E&S departments of certain DFIs are beginning to engage with a range of digital risks, such as those relating to platform workers, fintech and consumer protection. Investment departments dealing with digitalization commonly carry out due diligence across a range of digital risks, but do not necessarily communicate this due diligence to E&S departments, given that digital issues currently are not within the scope of most E&S departments. Moreover, investment departments are not charged with the same mandate and do not have the same clearance function as E&S departments on risks affecting people and the environment. In the view of OHCHR, breaking down organizational silos to promote better internal collaboration may help strengthen due diligence processes.

Given other pressures on DFI deal teams and clients, and given the novel, challenging and dynamic nature of digital risks and impacts, it is unlikely that these issues will be dealt with effectively or consistently unless or until there are clear and specific requirements to do so, approved by the executive boards of DFIs and supported by appropriate expertise and resources.

Recommendations

- DFIs should build the capacity and expertise of their E&S safeguard teams to strengthen stewardship and supervision of digital projects.
- DFIs should strengthen coordination of digital expertise across different organizational functions in order to enable 360-degree appraisal of projects.

B. CONCLUDING REMARKS

Digital technology is undoubtedly a game changer for development. The economic and other benefits of digitalization may be transformative. However, the central challenges are how to understand the implications and consequences of digital technology choices in particular social, political and cultural contexts, and how to more effectively identify and manage E&S risks (including human rights-related risks) in practice.

The dominant narrative on digitalization in development is a very positive one, as noted in the present report; however, undue techno-optimism may inadvertently minimize attention to risks. Nevertheless, the research and consultations carried out for this report have revealed a wide range of initiatives undertaken by bilateral and multilateral DFIs to analyse and address privacy, data protection, cybersecurity and certain other digital risks. The examples documented in this report are only illustrative and will quickly date. However, it is hoped that the documented practices will provide inspiration for more effective and consistent digital risk management approaches across the board, among DFIs and their sovereign and private sector clients.

Notwithstanding the many promising initiatives documented in the present report, it remains a matter of serious concern that digital risk management approaches at the project level have not been integrated effectively within the E&S safeguard policies of DFIs. At the time of writing, ADB and EBRD had taken initial steps in this direction, by integrating a certain number of digital risks within the scope of their updated E&S frameworks. However, across the board, there is much more to be done to ensure that a fuller range of potential digital risks and impacts are brought within the mainframe of DFI project risk management policies, and are translated into clear and consistent requirements for DFIs and clients respectively across all phases of the project cycle. There is nothing inherent in the nature of digital risks that should warrant their exclusion from the scope of safeguards: rather, the challenge is to articulate the role of safeguards in the context of a larger suite of policies, tools and approaches, through which the dynamism and other distinctive characteristics of digital risks and impacts can be more transparently and consistently addressed.

As is noted in this report, safeguard policies are in most cases the main board-approved instruments governing E&S risk management in DFI-financed projects. Safeguard policies establish clear, transparent, differentiated and contractually enforceable requirements for DFIs and clients, tailored to all phases of the project cycle. Such policies are backed by independent accountability, which enables access to remedy for project-affected people and helps to minimize negative externalities of projects and to strengthen lesson learning and feedback loops from operations to policy. Safeguard policies are also usually the product of public consultation processes, which confers legitimacy, strengthens ownership and trust, and ensures that a wide range of stakeholders' views and perspectives are reflected. Safeguard policies and the principle of independent accountability appear to be facing serious pressures in the face of recent MDB reform initiatives.[476] To ignore safeguard policies, in the digitalization context or otherwise, may further undermine them.

The breadth and complexity of the digital development field, and the diversity in DFI mandates, policies and approaches, means that it has not been possible to deal with all issues in the required depth in the present report. The clearest example of this is in relation to the management of AI risks in DFI-financed projects, which in the view of OHCHR, would be a compelling subject for a separate report. Deeper exploration of digital risk management in venture capital funds would also seem to be warranted, along with more a comprehensive discussion of rule of law prerequisites for digital identification and DPI projects, and at a more fundamental level, how "thinking infrastructurally"[477] could help to embed digital risk management within a deeper appreciation of project context and longer-term systems thinking.

[476] See, for example, Suma Chakrabarti and Chris Humphrey, "Rebooting the World Bank", Project Syndicate, 28 November 2022.

[477] See Benedict Kingsbury, "Infrastructure and InfraReg: on rousing the international law 'wizards of is'", *Cambridge International Law Journal*, vol. 8, No. 2 (December 2019), pp. 171–186, in which the author argues for "thinking infrastructurally" in international law to account for the ways in which "infrastructures", by which is meant "a set of relations, processes and imaginations" can have regulatory effects. By extension, it has been argued that infrastructural thinking "can illuminate ways in which digitalization projects connect with, become embedded in, are built on top of, and are dependent upon other infrastructures, and, in turn, can create new infrastructures with their own politics and publics. It requires us to take account of the wider social, technical, cultural, legal, institutional, political, and economic realities and practices that will shape the way a technology will operate – and it orients us firmly towards the future". See also Victoria Adelmant and others, *Digitalization as Development*. For an illustrative discussion, see Jean-Christophe Plantin and others, "Infrastructure studies meet platform studies in the age of Google and Facebook", *New Media & Society*, vol. 20, No. 1 (January 2018), pp. 293–310.

© Adobe Stock/Generative AI/by Yuliia

ANNEX I
WHAT A DIGITAL SAFEGUARD COULD LOOK LIKE

This report suggests the need for a more systematic, transparent and robust approach to managing digital risks in DFI operations. Chapter II, section A, puts forward that the E&S safeguard policies of DFI could, and should, play a central role in this regard, for several reasons: E&S safeguard policies establish transparent and binding requirements for DFI due diligence and client E&S risk management, specific to the different stages of the DFI project cycle. Moreover, E&S safeguards are usually the product of public consultation processes, approved by the executive boards of DFIs, and are backed by independent accountability. The safeguard policies of the leading MDBs have also indirectly influenced national laws and policies on E&S issues, in addition to having direct project-level impacts.

Chapter III, section A of this report recommends that E&S safeguard policies are updated and adapted to address digital risks according to a three-tier approach: (a) adapting sustainability policies (applicable to DFIs) to include specific digital requirements; (b) adapting existing performance standards (applicable to clients) so that the digital risk issues embedded within existing E&S standards are identified, addressed and migitated; and (c) adding a new digital-specific performance standard, relating to clients, that applies to digital components of projects.

In the following pages, ideas about what could be covered in each part of the E&S safeguards are set out, intended as a starting point for further reflection and discussion. Each DFI will need to address how to best address digital risks appropriate to its own safeguard system, although given the diversity and dynamism of the digital risk landscape, particularly in the context of AI, it seems clear that simply adding "digital" or "data protection" to existing E&S risk management requirements will not be sufficient.

Given the complexity and rapid evolution of digital technologies, it also seems reasonable to assume that no single set of E&S safeguards could be expected to anticipate and effectively address all needs. Rather, a reasonable ambition may be for (board-approved) E&S safeguards to reflect essential minimum due-diligence and risk-management requirements, while challenges pertaining to particular technologies may be addressed in documentation such as guidance notes, which can be fleshed out and updated more flexibly.

OHCHR recognizes that this is only a schematic proposal. However, its modest aim is to stimulate more detailed discussions among DFI management, shareholders and other stakeholders about the most appropriate form of policies to guide this growing area of DFI activity.

HOW COULD EXISTING E&S SAFEGUARDS BE ADAPTED TO ADDRESS DIGITAL RISKS?[478]

Digital-specific sections of sustainability policy applicable to DFIs

- **Objectives**
  - Digital-specific commitments that set out a general approach to digitalization (including respecting human rights)

- **Bank requirements**
  - Risk classification: Tiered digital-specific risk classification that avoids the systematic categorization of digital as low risk. Tiering tied to the scope and scale of the impacts, taking account of the differentiated nature of the digital impacts, rather than being driven by the nature of the project.
  - Project conceptualization stage: For projects with potentially systemic risks, wider scoping, investigation and consideration of the underlying foundations of the digital ecosystem and the project's potential impact, particularly the potential harms to users and non-users of the systems.
  - Due diligence: Digital-specific due diligence, including digital specific contextual analysis
  - Information disclosure: Digital-specific information disclosure
  - Consultation and participation: Digital-specific consultation and participation with affected stakeholders defined and identified to correspond to digital risks, rather than proximity to a project
  - Monitoring/supervision: Digital-specific supervision and relevant reporting requirements geared towards relevant digital disclosures
  - Grievance mechanisms and accountability: Specific provisions for digital-related complaints

- **Updated exclusion list** to cover inherently or systemically problematic or dangerous impacts that cannot be prevented or mitigated

Adaptation of existing performance standards/requirements applicable to clients

These are illustrative examples of the kind of issues that could arise, some of which are already being covered in practice:

Performance Standard 1 on assessment and management. Assess digital risks and where risks relate to topics already covered by existing performance standards, cross-reference to topic-specific performance standards (or to the performance standard that covers digital projects more generally).

Performance Standard 2 on labour and working conditions. Gig workers, data enrichment workers, health and safety (for example, screen time, psychological support for content moderators and monitoring at work)

Performance Standard 3 on resource efficiency pollution prevention. Sourcing of critical minerals for digital infrastructure, water and energy use, e-waste disposal

Performance Standard 4 on community health, safety and security. Product safety, incitement to violence against community members

[478] OHCHR gratefully acknowledges the collaboration with the Danish Institute for Human Rights in developing its Digital Safeguard recommendations.

Adaptation of existing performance standards/requirements applicable to clients

Performance Standard 5 on land acquisition and involuntary resettlement. Displacement and impacts of digital infrastructure, including power sources (such as for data centres), loss of customary land rights and access through the digitization of land records and rights

Performance Standard 6 on biodiversity. Displacement and impacts from digital infrastructure, waste and impact on indigenous knowledge

Performance Standard 7 on Indigenous Peoples. Stereotyping, cultural rights, digital ownership, control and stewardship by Indigenous Peoples

Performance Standard 8 on cultural heritage. Loss of cultural heritage, cultural appropriation and the potential for digital technologies to distort or misrepresent cultural identities, exploitation of traditional knowledge without consent

Performance Standard 9 on vulnerable and marginalized groups. Online human rights defenders, exacerbating vulnerability and marginalization through online actions, technology-facilitated gender-based violence, deepening the risk of statelessness

Performance Standard 10 on stakeholder engagement. Identifying and engaging affected stakeholders in digitalization projects, digital reprisals, emphasizing the importance of consultations with experts and global civil society (given the widespread lack of knowledge and transparency concerning digital impacts)

Digital-specific performance standard applicable to clients

- **Introduction**
  - Contextual information and justification for stand-alone digital safeguard requirements

- **Objectives**
  - To recognize technology, data and technology change as essential to sustainable development
  - To recognize that technologies, data and technological change will be responsibly managed throughout their life cycles, especially in light of potential developments and disruptions
  - To prevent DFI-financed digital projects having adverse impacts through use or misuse
  - To provide transparency about the potential and actual impacts of digital products and services and how they will be managed, outlining principles underlying a risk management approach for responsible management of technology, data and technology change throughout the technology life cycle, including identification, assessment and supervision
  - To clarify application of a risk management approach in start-up and venture contexts, as risks and impacts may be asymmetric to the company's stage of development

- **Scope of application**
  - Tiered approach depending on the level of risks associated with the digitalization
  - Through different financing modes, including financial intermediaries
  - Defining affected stakeholders to include users of digital products and services

Digital-specific performance standard applicable to clients

- **Requirements**
  - **Policy commitments.** Clients to adopt policy commitments specific to the type of project and its associated digital risks and to the level of transparency about how the risks are being managed
  - **Identification of risks and impacts.** Use of digital specific assessments proportionate to the level of risk, such as data protection impact assessments, algorithm impact assessments, algorithm audits and human rights impact assessments, for higher-risk activities
  - **Application of appropriate principles.** For example, do no harm, rights-respecting, privacy by design, data protection principles, non-discrimination, safety and sustainability, including by reference to internationally accepted principles and standards[479]
  - **Management systems and management plans.** Reference to accepted digital risk management frameworks and specific actions to prevent and mitigate identified risks organized into a digital action plan. The risk management structure may overlap, be coordinated with or may in part be separate from the client's E&S management system, and should be tailored to client and context
  - **Coverage of core issues in every management system.** For example (a) privacy, data protection, data security; (b) risks associated with automated decision-making and machine learning; and, (c) risks of exclusion
  - **Organizational capacity and expertise.** Requirements on appropriate digital expertise, scaled to the level of digitalization
  - **Monitoring.** Requirements to monitor the impacts of projects and the use of products and/or services
  - **Stakeholder engagement.** Adapted requirements to reach stakeholders affected by digital products or services, including protection against retaliation
  - **Remedial measures.** Fit-for-purpose grievance mechanisms and remedial measures proportionate to the number of stakeholders who may be affected and suitable to provide redress for digital specific harms

[479] See, for example, "Principles for Digital Development".

ANNEX II METHODOLOGY

SCOPE

The scope of the present report encompasses DFIs that finance both private and public sector clients, including bilateral and multilateral banks.

- **Multilateral development finance institutions**: ADB, AIIB, AfDB, EBRD, EIB, IDB, IDB Invest, IFC and the World Bank.
- **Bilateral DFIs**: BII, DEG, Finnfund, FMO, JICA, Swedfund and DFC.

The mixed-method research methodology on which this report is based is comprised of five main elements:

- **Desk research and three comparative reviews of DFI-financed projects with a digital component.** The first project database analysis, focused on the ICT sector, was carried out in early 2023 at the University of St. Gallen. A second analysis, focused on Sub-Saharan Africa, was made available to OHCHR by the Danish Institute for Human Rights.[480] A third database analysis, covering nine MDBs and four sectors, was carried out between November 2023 and January 2024 by former IDB E&S specialist Amalia Palacios (OHCHR digital risk-mapping exercise, see next section).
- **Documentation review** of DFI strategies, selected tools and publications highlighted on websites and in evaluations and E&S safeguards.
- **Consultations** were carried out with DFIs, civil society organizations, academics, specialists and other key stakeholders. This included in-person interviews in Washington, D.C. in May 2023 with IFC and IDB, and a series of online meetings and webinars that took place between May 2023 and October 2024 with DFIs, civil society organizations and technical experts.
- A **short questionnaire** was distributed in August 2024 to all nine multilateral DFIs and the bilateral DFIs covered in this report, which attracted five responses.
- **Review of academic literature** on DFIs and digital issues from academics, with a particular thanks to the International Organizations Clinic at the New York University School of Law.

[480] OHCHR is grateful to the Danish Institute for Human Rights for providing access to its database of projects, reviewed in the Institute's briefing note, entitled "Development finance for digitalisation: Human rights risks in sub-Saharan Africa" (March 2023).

OHCHR DIGITAL RISK-MAPPING EXERCISE

All the multilateral DFIs and a few of the bilateral DFIs included within the scope of this report maintain comprehensive project databases on their respective websites, which contain details about ongoing, forthcoming, concluded and terminated projects.

The analysis was undertaken from the perspective of people potentially affected by digital impacts from DFI-supported projects. Hence, it focused on appraisal documentation, including but not limited to E&S documentation, made publicly available through the respective DFI project portals. This is the documentation that is intended to provide potentially affected stakeholders with advance notice of potential risks in order that any concerns can be raised in advance of project approval. The amount of information made available varies between DFIs.

Financing agreements are the dispositive tool to create binding requirements for clients and thus a powerful source of leverage for DFIs. However, within applicable resource and time constraints, it was not possible to review financing agreements on more than a selective basis. Transparency is a barrier in this regard: ADB, IDB and the World Bank make legal agreements systematically available; however, the other MDBs discussed in this study do not.[481] Private sector contracts are not disclosed at all.

The view taken by OHCHR is that financing agreements should not be the sole source of information to potentially affected stakeholders about digital risk management requirements in projects. Project summary disclosures and E&S disclosures have been developed and adapted over time to serve this role. By contrast, the technical content of legal agreements can be difficult for most people to comprehend. Moreover, arguably, contractual conditions are not actionable by stakeholders in the same way that non-compliance with E&S safeguards are under an IAM system. Hence, while legal agreements are important, they should not be the only answer for stakeholders.

The emphasis of OHCHR's research was on projects that are active, including those which had been approved for adoption at the time of writing, but have not yet entered the implementation phase. In most databases, except for AfDB, it was possible to search by sector.

The study is not intended to be all encompassing or definitive in terms of the issues covered, or necessarily representative of all the kinds of digital risks that may arise in connection with DFI-financed projects. Rather, the analysis was largely illustrative, aiming to identify noteworthy features, gaps and trends in the emerging digital risk management landscape. With regard to the OHCHR digital risk-mapping exercise, a survey analysis was conducted on the project portfolios of nine DFIs to assess digital components/activities and understand how human rights/digital risks were being considered. Approximately 3,450 projects were preliminarily screened and reviewed, searching for "digital" elements/components within four different pre-selected main sector categories/thematic areas defined as "sector focus (OHCHR)" because of their relevance and potentially related "digital" risks. For each of the nine MDBs, a dataset of listed projects was downloaded/extracted from the banks' online databases (official websites).

[481] For a comparative analysis of DFI transparency practices, including but not limited to E&S issues, see Publish What You Fund, "DFI Transparency Index 2023" (2023).

To download the list of projects for later analysis, pre-identified filters (time period and project status) were selected and applied while downloading and building each DFI dataset. Details of the criteria/filters used for each DFI are summarized in the following table.

Table 1
Criteria applied to extract project lists and data by DFI

DFI	Time period		Project status
	From	Until	
World Bank	1 Jan 2019	14 Nov 2023	Active
IFC	1 Jan 2019	20 Nov 2023	Active
IDB	1 Jan 2019	13 Nov 2023	Active
IDB Invest	1 Jan 2019	22 Nov 2023	Active
AIIB	1 Jan 2019	24 Nov 2023	Approved
ADB	1 Jan 2019	23 Nov 2023	Active
AFDB	1 Jan 2019	23 Nov 2023	Active
EIB	1 Jan 2019	23 Nov 2023	Approved
EBRD	1 Jan 2019	24 Nov 2023	Active

All downloaded databases were consolidated into a unified spreadsheet, featuring nine tabs/sheets (each one including all listed projects extracted from the main database of each DFI).

Table 2
Key terms used to search for projects in DFI databases

Main sector category	Key terms and search words used when identifying digital projects
ICT infrastructure	▪ "Digital" + xx (digital innovation, digital transformations, etc.) ▪ "E-…" (e-commerce, etc.) ▪ Tech/technology/technologies ▪ AI/artificial intelligence ▪ IT/information technology ▪ Hardware/software ▪ Machine learning ▪ Mobile
Finance	
Health	
Public administration	

Table 3
Search terms most frequently found in digital projects in DFI databases

Main sector category	Search terms frequently found in digital projects
Found in most digital projects/all sectors	▪ Digital innovation ▪ Digital communication ▪ Digital platforms ▪ Digital transformation ▪ Smart technologies
ICT	▪ Infrastructure: digital infrastructure and telecommunications infrastructure (e.g. 5G mobile network, data centres) ▪ Digital technologies: digital skills, AI/machine learning, digital markets, digital equipment, etc.
Finance	▪ Fintech (digital finance tools for supporting public development banks, digital markets and digital finance) ▪ SME support (with digital finance tools, venture capital, e-commerce supporting start-ups and promoting digital entrepreneurship systems) ▪ Digital (social) payments (integration of mobile and cashless transactions) ▪ Regulatory advice (focused on developing digital finance tools and promoting digital ecosystems)
Health	▪ Digital health and e-health: infrastructure and equipment for smart health facilities ▪ Telemedicine and health surveillance systems: using digital platforms for public health, healthcare accessibility and preventive measures (COVID-19 pandemic) ▪ Digital transformation: digital equipment/digital tools including digital medical records, teleconsultations and mobile health platforms
Public administration	▪ E-government: digital identification, taxation systems, cybersecurity, digital public sector reforms ▪ Digital public services: digital tools to improve service delivery, fiscal management, regional governance ▪ Cybersecurity: smart/digital governance and digital security measures, judicial and public sector digital transformations ▪ Digital tools: used for policy development, fiscal management and project monitoring in public administration ▪ Regulatory advice: including open government data, government reforms and e-education

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

Office of the United Nations
High Commissioner for Human Rights (OHCHR)
Palais des Nations
CH 1211 Geneva 10, Switzerland
Telephone: +41 (0) 22 917 92 20
Email: ohchr-infodesk@un.org
Website: www.ohchr.org

ISBN: 978-92-1-159365-5

9 789211 593655