Combatting Corruption: Digital Transformation

Guidance Note - DG INTPA G1

This note is an excerpt of longer guidance currently in development, exploring anti-corruption in different sectors.

Through Global Gateway, the EU is strengthening connections between Europe and the world and helping partner countries address the digital divide and further integrate into the global digital ecosystem. Digitalisation is bringing fast change that affects our labour markets and daily life. With the Communications on Shaping Europe's digital future and the 2030 Digital Compass Decade, the EU has put forward a human-centric approach to digital transformation. Through European Declaration on Digital Rights and Principles for the Digital Decade from 2022, EU commits to strengthening the democratic framework for a digital transformation that benefits everyone and improves the lives of all people living in the EU.

On the one hand, digital transformation enables possibilities to enable private sector development and investments, enhance citizen engagement, government efficiency through e-governance, and communication. Additionally, it can offer opportunities to tackle corruption, e. g. by using technology to follow financial flows and improve tax collection. Corruption is more pronounced in cash-based economies and it is precisely for anti-money laundering purposes that many Governments are trying to reduce the circulation of large notes.

On the other hand, it brings risks, including inequity in access to connectivity, due to digital literacy disparities and potential violations of personal data privacy, online fraud, illicit financial flows, as well as the potential impact of disinformation on democratic process, and harassment and intimidation of i.a. political opponents, consequently, deepening divisions among citizens and posing a serious threat to national security.

Corruption Risks and Mitigation

While many look at the bright side of how digitalisation and new technologies assist in the fight against corruption, there is a lack of knowledge about specific mechanisms of how corruption manifests in digital transformation and what the mitigations are for the corruption risks in the digital economy sector.

Main challenge for analysis of corruption risks is the complexity of a sector that is not limited to national borders. There are at least three effects of digital transformation associated with corruption: (i.) Digital technologies **enable corruption** (e. g. money laundering and other forms of illicit

financial flows through cryptocurrencies and cash-less transactions); (ii.) Worsening of corruption through the creation of digitally moderated **opportunities and networks**; (iii.) Conventional forms of **corruption shift to other, new, unanticipated forms** of corruption that are difficult to tackle (corrupting public opinion by bots, skewing e-voting, e-petitions, etc.).

Governments' digitalisation – The public sector's digitalisation entails the smarter use of new technologies and data analytics, e. g. digitalising paper-based processes, automate bureaucratic procedures, introducing e-gov services and interoperable digital systems. Most importantly, governments' digitalisation requires complementing measures regarding the careful and secure management of data and mitigation of risks to data privacy and cybersecurity.

Despite the potential to fight corruption by reducing discretion, increasing transparency, and enabling accountability by digitalised services and limiting human interactions, the public sector still faces conventional corruption risks in decision-making, public procurement, and public service provision.

These risks can affect e. g. contracting, designing, and developing technology and information systems, e-voting systems and public service provision in e-gov services, and manifest in forms of kickbacks, overpricing, and under-delivery.

Resources for further reading:
OECD Open Government Toolkit Open government - OECD.
UK Government Open Policy Making Toolkit.
The Governance Lab at NY University has formulated eight recommendations for open and engaged policy-making.
The latest TI report 'Exporting Corruption' (2022) assesses the foreign bribery enforcement of the OECD Anti-Bribery Convention (adopted 1997) and identifies a range of inadequacies in legal frameworks, and enforcement systems.
OECD provides further resources, such as its paper on Preventing Corruption in Public Procurement, and its Anti-Corruption and Integrity Hub.
IACA's and UNOPS free online training on 'Fraud and Corruption Prevention in Public Procurement'.
UNODC provides University Modules for Anti-Corruption training, also on public procurement as part of its Module 4 Public Sector Corruption.
The IMF outlines in its Working Paper from May 2022 a methodology and results in assessing corruption risks in public procurement and their impact on relative prices, using large databases on government contracts and tenders.
The Open Contracting Partnership has developed a wealth of resources on open contracting, including specifically for extractive industries and its joint global analysis with the Natural Resource Governance Institute (NRGI) which identifies 16 better practices covering each stage of the contracting process including over 30 real-world examples from Australia, Chile, Ghana, Lebanon, Mexico, etc.

U4's Anti-Corruption Resource Centre provides information on Procurement. Hivos has produced an advocacy toolkit for opening up contracting.

Corruption risks through artificial intelligence (AI) – Corrupt AI is defined as inter alia the abuse of AI systems by (entrusted) power holders for their private gain. There are at least three categories of corruption risks: (i.) AI system is intentionally designed for corrupt purposes, (ii.) training data or algorithm of existing AI systems are manipulated to achieve corrupt goals, and (iii.) an AI system is applied and repurposed for corruption.

Examples are the generation of hyper-realistic deep fakes to discredit and intimidate (political) opponents, designing an AI system for computational propaganda (e. g. social media bots), trained AI systems with not full representative data increasing potential discrimination (e. g. admission to schools, provision to health services) based on gender, race, income, or nationality.

Resources for further reading:
Driving and enabling factors of AI-related corruption risks are comprehensively compiled in the TI-Working Paper "The corruption risks of artificial intelligence" by Köbis et al. (2022). The authors also list in the same working paper some possible mitigation strategies such as independent audits, quality checks, and raising transparency and accountability.
OECD provides an overview on AI Principles, which was initially adopted in 2019 and updated in May 2024, supporting AI actors in their efforts to develop trustworthy AI and provide policymakers with recommendations for effective AI policies.
UNESCO provides Recommendation on the Ethics of AI, which was adopted by all 193 Member States in November 2021, allowing policymakers to translate core values and principles into action respecting data governance, environment and ecosystems, gender, education, research, and health and social wellbeing.

Cryptocurrencies as enablers of corruption – Cryptocurrencies have a complex impact on development, as they offer potential benefits such as financial inclusion and access to capital, but also pose diverse risks. Additionally, their decentralized nature has made them appealing to legitimate businesses and criminal elements, enabling illicit finance and corruption.

According to the findings of the Occupational Fraud 2022 Report from the Association of Certified Fraud Examiners (ACFE), 8% of fraud cases worldwide in 2021 involved the use of cryptocurrencies – 48% of these cases related to payment of bribes and kickbacks.

Resources for further reading:
EU Regulation on markets in crypto-assets was adopted in May 2023, and has been implemented as of August 2024, aiming to support innovation and fair competition by creating a framework for issuance, and provision of services related to crypto-assets as well as to ensure a high level of consumer and investor protection and market integrity.
Several attributes of cryptocurrencies and conditions related to the operations enable corruption, including mitigation strategies are provided by U4-TI analysis Cryptocurrencies, Corruption and Organised Crime from 2023.
The Basel Institute on Governance provides different recommendations on this issue, e. g. Combating virtual assets-based money laundering and crypto

enabled crime: Recommendations of the Tripartite Working Group on Criminal from 2021, or Seizing the opportunity: 5 recommendations for crypto assets-related crimes and money laundering from 2022.

Corruption Analysis
Understanding the enablers and drivers of corruption in the digital sector is critical to designing appropriate direct or indirect interventions to fight corruption.

The overall political economy analysis for the digital sector must account for several questions regarding e. g. role of digital economy sector, access to internet, degree of digital literacy, and available infrastructure for governmental and open data in a country. The answers to these questions might help to avoid unintended consequences of the anti-corruption interventions.

The following three complementary approaches are often employed: (i) Political Economy Analysis (PEA) includes stakeholder mapping and exploration of the structure as well as the 'rules of the game'; (ii) Systems Analysis covers the

> **EU Tools**
> Based on Article 21 of the Treaty on the EU (TEU), as a priority in its external action the EU promotes human rights, democratic governance, the rule of law and the fight against corruption policies. More generally, in its external actions, the EU supports legal and policy reforms to build anti-corruption institutions as well as oversight bodies, and to strengthen civil society, human rights defenders, whistleblowers, and independent media as watchdogs against corruption. Any anti-corruption analysis can complement and be supported by existing EU tools, including Conflict analysis and EU early warning systems, Gender analysis, Risk Management Framework, Budget support, Human Rights & Democracy country strategies. Note also the recent EU Handbook of good practices in the fight against corruption and the currently discussed joint proposal for adjusting the horizontal, thematic framework for the Common Foreign and Security Policy (CFSP) sanctions toolbox, to be able to target serious acts of corruption worldwide, to complement EU internal and external policy actions to fight corruption.

procedures and routines within a system to understand drivers and causal loops; (iii) Analysis of Social Norms and Perceptions, including gender, focuses on expectations and perceptions of what is acceptable behaviour.

Resources for further reading:
OECD public integrity maturity model – self-assessment tool for national and subnational governments and public sector organisations.
U4 The basics of corruption risk management, U4 Anti-corruption resource centre, and TI Anti-corruption Knowledge Hub provides wide range of resources. Specifically for the digital sector, U4 provides in its paper Blockchain as an Anti-Corruption Tool case examples and introduction to the technology.
AUS administration's Good Practice on PEA, UK administration's Understanding PEA, UK AID's Beginner's Guide to PEA and USAID's Applied PEA, the Corruption, Justice and Legitimacy Program (tools and guides), general guidance is provided by USAID Anti-Corruption Assessment Handbook.
The paper Are emerging technologies helping win the fight against corruption? By Adam, I (Elsevier, 2021) provides a review of the state of evidence.