



Learning Lab Series

Understanding Digital Risks:

*Protection of forcibly displaced and host communities
and realising the benefits of the digital economy*

ILO-UNHCR



Learning Memo

Understanding digital risks:

*Protection of forcibly displaced and host communities and
realising the benefits of the digital economy*

Learning Lab #3

Wednesday 4 October 2023

Understanding Digital Risk

- ▶ **Digital risk is a comprehensive concept:** it can be understood as the potential harms arising from and encountered through interactions between people navigating the Internet, hardware, software, various locations, discourses, practices, and power relations. Moreover, it is intersectional, and thus influenced by factors such as race, gender, age, sexuality, citizenship, and status.
- ▶ **Digital risk assessment framework:** This framework untangles the various dimensions in which digital risk manifests, categorising them into four key areas:
 - **Infrastructural risks:** Encompass a spectrum of challenges within energy systems, communication networks, national and international legal frameworks, and institutional structures at the national level.
 - **Access-based risks:** Entail diverse considerations, including device affordability, accessibility, battery charging, cultural stigmas, availability of training centres, and proficiency in internet navigation skills.
 - **Service-based risks:** Potential digital harms introduced by platform service providers, often stemming from inadequate governance models, platform design and suboptimal usability. In the case of digital labour platforms specifically, additional risks related to precarious work conditions, lack of protections, algorithmic bias and unregulated collection of data.
 - **Use-based risks:** Arise when individuals utilizing digital technologies jeopardize themselves or others through actions like age verification evasion, clicking on suspicious links leading to scams, disseminating misinformation, grooming, cyberbullying, hate speech, harassment, etc.

Digital risks faced by refugee populations

- ▶ **Common and specific threats:** Refugees face a dual challenge in the digital realm, encountering both common risks shared with host communities and distinct threats specific to their situation. Tailored online scams exploit vulnerabilities with false promises of aid or resettlement. Furthermore, refugees are at risk of being identified due to their social media activity, which can be exploited.
- ▶ **Risks vary within refugee communities:** Risks within refugee communities can vary based on factors such as gender, age, and digital skills and literacy. For example, young women, girls, and boys may face a heightened risk of being targeted by online traffickers and cyber bullying.
- ▶ **Online and offline risks:** Online risks can translate into various offline dangers, ranging from financial fraud to physical harm. Online recruitment scams, for instance, may contribute to diverse forms of human trafficking. In the context of the gig economy, workers engaged in services such as deliveries and home aid persons may face tangible physical risks.

Digital risks when working on online labour platforms

- ▶ **Regulatory gaps pose risks:** New online work models, like the gig economy, often lack adequate regulations and safeguards. Workers, including refugees, may encounter discrimination from employers, endure unfavourable labour conditions, and have limited negotiating power for pay terms. Limited access to ownership of personal devices hampers refugees from utilising cybersecurity and privacy features offered by online work platforms.
- ▶ **Payment risks:** Concerns arise regarding non-payment for work done on online labour platforms in general, with refugees at higher risk of exploitation due to language barriers, lack of legal protection, and unfamiliarity with local labour laws. Identity issues further complicate the use of payment platforms like PayPal or bank transfers.
- ▶ **Explosion of AI poses risks:** With the increasing use of AI and the subsequent demand for cloud work and microwork, concerns about the working conditions in this labour sector are growing. American lawmakers just last month reached out to nine different tech companies, including Amazon, Google, and OpenAI, to inquire about the working conditions of those that they employ to train and maintain their AI systems.
- ▶ **Well-being risks:** Platform work, which often spans various time zones, compels individuals in less favourable time zones to work at night. This not only jeopardises their physical well-being but also disrupts their time with family and friends, significantly impacting social interactions. Refugees face higher risks of exploitation and poor working conditions due to the opacity of platform terms, language barriers, and inadequate documentation.

Mitigation of digital risk

- ▶ **Mitigation strategies of digital risk:** Effectively managing digital risk requires tailored mitigation strategies aligned with specific risk categories.
 - **Infrastructural risks mitigation:** Mitigating infrastructural risks requires collaborative efforts involving policymakers, regulators, national infrastructure providers, and development actors, to address shortcomings at a macro level.
 - **Access-based risks mitigation:** Addressing access-based risks calls for localized interventions, such as forging partnerships with local training providers and managing relationships with device distributors and community-based organizations working with refugees and host communities.

- **Service-based risks mitigation:** Managing service-based risks should primarily involve shaping the design and business models of digital platforms, requiring direct engagement with platform providers and collaboration with regulators.
 - **Use-based risks mitigation:** Mitigating use-based risks often demands direct engagement with digital technology users. This may include implementing training and awareness raising to empower people with information on how to safely navigate the online world of work.
- ▶ **Primary stakeholders engaged in managing digital risk:** For effective mitigation, a multi-stakeholder approach is needed. Key actors in this endeavour include:
- **The UN system and other developmental partners** offer technical guidance to nations in establishing regulatory frameworks for heightened oversight of digital risks.
 - **The private sector** assumes a pivotal role by constructing inclusive and secure digital platforms, enabling users, and including refugees to adeptly navigate privacy and security concerns.
 - **Researchers** play a vital role in comprehending the swiftly evolving landscape of technologies like generative AI, discerning both opportunities and risks.

Key resources

- ▶ Howard (2023): [The Ukraine War & Cyberattacks Targeting Refugees and Humanitarian Organizations](#)
- ▶ CSIS (2023): [Safeguarding the Digital Landscape: Online Opportunities & Threats for Displaced Ukrainians](#)
- ▶ EU-ILO (2022): [Digitalization and Employment](#)
- ▶ UNCDF (2022): [The role of cybersecurity and data security in the digital economy](#)
- ▶ UNHCR (2022): [Digital Transformation Strategy](#)
- ▶ Sayegh (2022): [Dark Web Of Cybersecurity Concerns Rising With Gig Economy](#)
- ▶ ILO (2022): [The Algorithmic Management of work and its implications in different contexts](#)
- ▶ UNHCR (2021): [Connecting With Confidence: Managing Digital Risks to Refugee Connectivity](#)
- ▶ ICTworks (2021): [12 Ways to Manage Digital Risks to Refugee Community Connectivity](#)