Barey Ibrahim Korone receives cash assistance from Oxfam. The programme targets drought affected families in Wajir, Kenya and provides money electronically via their mobile phones. © Billy Owiti/Oxfam. November 2022

Chapter 7: Data and Digitalization

Summary: Chapter 7

Data and Digitalization

Key findings

- ✓ The use of digital payments is increasing.
- ✓ More action is needed on data responsibility.
- ✓ Cybersecurity is a risk that few talk about in the humanitarian space.
- ✓ Biometrics are better understood than before; blockchain pilots have expanded and multiplied.
- ✓ The concepts of interoperability and portability continue to be explored.
- ✓ Technology for remote targeting and accountability can complement existing CVA processes but can also amplify risks and introduce new ones.
- ✓ There are high levels of investment in Management Information Systems by the largest organizations.
- ✓ Artificial Intelligence provides new opportunities and risks.
- ✓ Skills gaps and underinvestment are impeding digital developments in many humanitarian organizations.

Strategic debates

- [?] Can technology increase recipient choice?
- [?] How can new technologies be piloted without increasing risks to vulnerable communities?
- [?] Can CVA and payment technologies support locally-led response?
- [?] What are the cybersecurity risks faced by CVA stakeholders?
- [?] How can humanitarian organizations and the private sector work together better in relation to CVA?

Priority actions

- [!] **Humanitarian organizations should** embrace the opportunities presented by developments in the digital payments space which can offer recipients a choice of CVA delivery mechanisms, as well as allowing faster and more efficient disbursements.
- [!] **Humanitarian organizations should** recognize that successful technological innovations are more likely to scale if they are drawn from communities and the programme teams who regularly interact with them.
- [!] **Humanitarian coordination channels should** harness existing data responsibility guidance and support its uptake in CVA. **Humanitarian organizations should** prioritize the implementation of guidance to ensure effective management of data and mitigation of risks.
- [!] **Humanitarian organizations should urgently** make investments to ensure strong digital skills and understanding across their staff teams. Cyber-security capacity needs to be developed by staff involved at each stage of the CVA project cycle. Recipients should be supported to understand digital risks and how they can be mitigated.
- [!] **CVA implementers should** work together to advocate to governments and regulators for improvements to policies and regulations that impact CVA recipients.
- [!] **Humanitarian organizations should** always consider a multi-channel approach when deploying any technology, giving recipients choices in the ways they interact with programme systems and processes.
- [!] **Humanitarian organizations and the private sector should** agree on approaches and develop a roadmap that will support interoperability and portability initiatives.
- [!] **Donors should** continue their efforts to catalyze action to improve data responsibility.

Increasing use of digital payments

There has been a significant increase in the use of digital payments since the *State of the World's Cash 2020* report. This has resulted in faster payments, larger scale responses and a greater push into hard-to-reach areas. The humanitarian sector is leveraging digital payments to explore giving recipients choice. At the same time, the digital payments space has been undergoing rapid change and is a challenging space for many to navigate, 'characterized by a high level of uncertainty and competition'[1].

What are digital payments?

"Digital payments (or e-transfers) refer to electronic transfers of money or e-vouchers from the implementing agency to a recipient. They provide access to cash, goods and/or services through mobile devices, electronic vouchers, or cards (e.g., prepaid, ATM, smart, credit or debit cards). Digital payments/e-transfers are umbrella terms for e-cash and e-vouchers[2]."
(CALP Glossary, 2023)

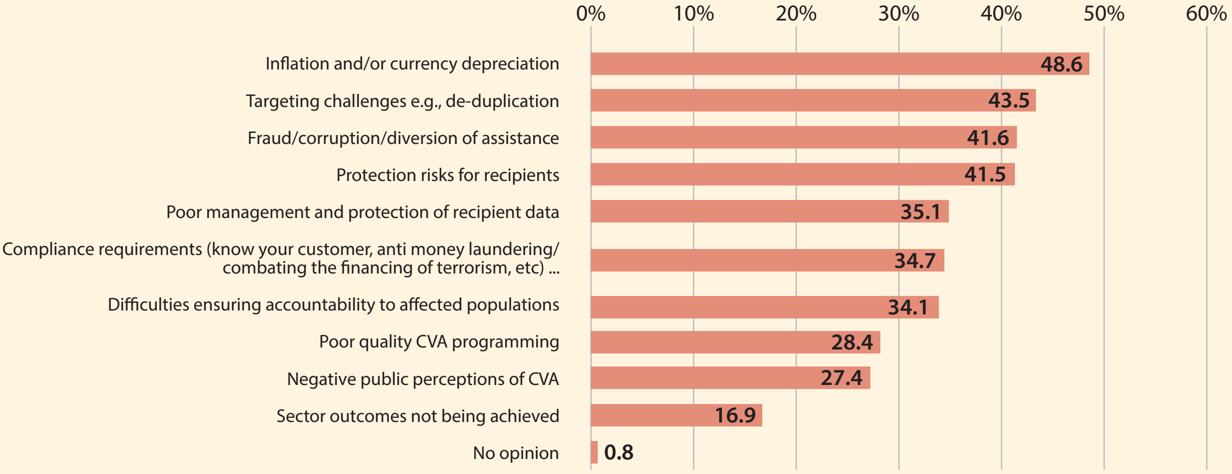
For many organizations, the COVID-19 pandemic and regulatory changes accelerated the move to digital payments and the use of mobile money grew in many countries[3]. By 2022, there were 1.6 billion registered mobile money accounts worldwide.

This trend was also seen in the humanitarian space. For example, WFP in Somalia piloted moving CVA recipients from e-vouchers to mobile money in late 2020[4]. By 2022, 63% of their recipients received payments via mobile money[5]. To encourage such change, some donor policies now indicate a clear preference for mobile money. For example, DG ECHO's cash policy supports 'digital by default' unless financial infrastructure is limited, analogue methods offer better value[6] or where recipients express a preference for a particular delivery mechanism. It also stresses that mobile payments need to be considered through the lens of 'do no digital harm'.

While digital transfers can be fast once systems are well established, research in the Horn of Africa highlighted that **a major factor limiting the speed of a CVA response is the time taken to establish contracts with financial service providers** (FSPs)[7]. Various avenues have been explored in different contexts to address this.

GRAPH 7.1

What are the highest risks associated with CVA that need to be addressed?



Standing contracts with multiple FSPs could enable organizations to respond faster across various locations. However, this is challenging in terms of: (a) procurement and maintenance of contracts, (b) technically, if Application Programming Interfaces (APIs) are used to send data and requests (since each require an expensive and often-unique set-up process and need expert maintenance), and (c) FSPs' profitability concerns if they need to respond to numerous requests for proposals for services that may never be utilized and so no revenue is earned.

Aggregator

"An entity that consolidates financial transactions for processing, for example enabling the flow of payments between payers and recipients across ***multiple financial service providers (FSPs)****. Aggregators provide systems integration by connecting FSPs to third-party systems. They may also provide additional services such as notification of successful payments, reconciliation, and receipts."*
(CALP Glossary, 2023)

Numerous stakeholders, including donors,[8][9] Cash Working Groups (CWGs),[10] UN bodies[11] and research institutions, have promoted joint procurement[12][13]. The UN has taken this forward, with the UN Common Cash Statement (UNCCS) reporting[14] progress on collaborative procurement. This includes piggybacking contracts, collaborative contract clauses and joint procurement, with 25 countries leveraging 'common procurement, inclusive of other agencies beyond UNCSS, to simplify cash delivery from the perspective of people in need'[15]. Outside the UN, this approach has not been widely adopted between NGOs aside from the commonly cited example of the Common Cash Facility in Jordan – a collaboration which also involved UN bodies and the Jordanian Government[16].

Several organizations, including IFRC and WFP, are exploring global payment solutions, including via aggregators, to enable scalable, faster, and more efficient distribution of CVA[17][18]. Such solutions could also allow recipients to choose their cash delivery mechanism and provider e.g., using an existing or preferred bank, mobile money account, or cash-out agent, rather than agencies determining choices. Global and regional aggregators can simplify CVA implementers' access to multiple local and international FSPs, which are essential for the final delivery of CVA. However, some raise concerns that this may disempower in-country relationships with FSPs and make it more difficult to negotiate specific services or lobby for the expansion of services in underserved communities.

Some issues related to digital preparedness are also explored in Chapter 5 on Preparedness and capacity.

The move towards digital payments has enabled greater speed and scale of response but has also brought new challenges as humanitarians seek to understand a complex and fast-moving world of payments, regulated by a patchwork of global and national legislation. With funds crossing international borders, CVA implementers contend with the financial sector de-risking phenomenon, where banks refuse to deal with certain customers, countries, or transactions rather than manage the risk associated with the relationship[19]. In many cases, **funds moved for CVA disbursements have received greater scrutiny than some other humanitarian transfers**[20] as the final recipients are a multitude of individuals, rather than individual companies supplying goods with readily available contracts and company registration documents to assess. In contexts with higher risk jurisdictions, systems such as F4ID's LOTUS20, which make payments to vendors for the goods chosen by recipients, offer a possible solution as vendors can more easily and effectively[21] be subject to KYC or sanction checks than multiple individuals.

Each solution requires trade-offs between choice, efficiencies, speed, the ease with which regulations are managed and so on. Alongside all this, major questions around data responsibility need to be addressed.

Data responsibility, more action needed

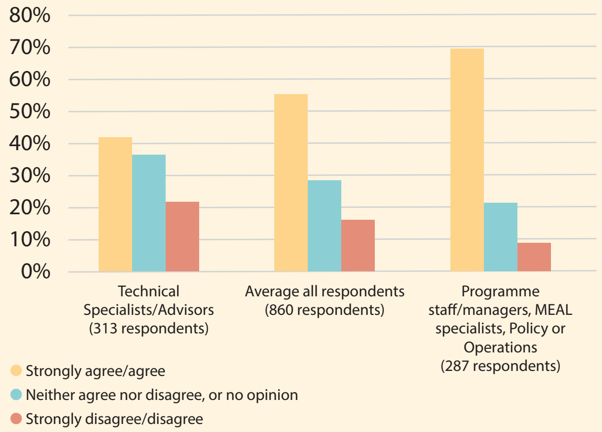
Fifty-five percent (55%) of survey respondents thought that CVA implementers managed and protected recipient data effectively. Another 16% disagreed and 29% neither agreed nor disagreed, or had no opinion. This paints a relatively positive picture of the state of humanitarian data responsibility. Yet these results need to be treated with caution.

Data responsibility

"Data responsibility goes beyond data privacy and data protection (the process of safeguarding important information from corruption, compromise, or loss) to include principles, processes and tools that support the safe, ethical, and effective management of data. CVA involves the collection, sharing and use of potentially sensitive data (which if improperly accessed could lead to harm to person(s) and/or negatively affect organizations) about crisis-affected people, communities, locations, and humanitarian interventions, hence incorporating data responsibility throughout the programme cycle is important." (CALP Glossary, 2023)

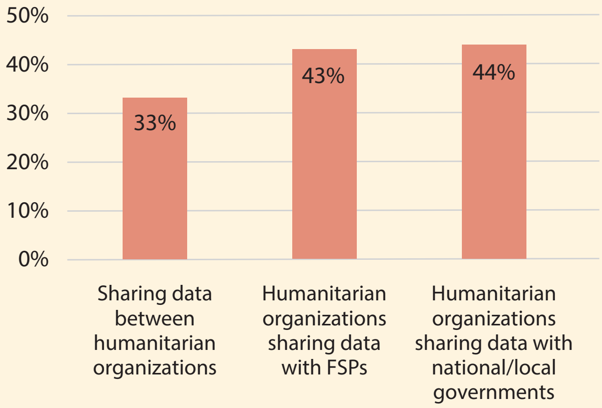
GRAPH 7.2

Organizations involved in CVA programming are managing and protecting CVA recipient data effectively, breakdown in role



GRAPH 7.3

What are the biggest challenges for improving the management of recipient CVA data?



CVA technical specialists, advisors and researchers responded to the survey more negatively than those with operational or programmatic roles. The disparity in responses suggests there are important differences in understanding the level of risk or the effectiveness of current mitigations (See Graph 7.2). **Overall, irrespective of role, nearly half the respondents felt that data responsibility was not effectively mainstreamed across teams implementing CVA**.

Sharing data with other organizations is a necessity in most CVA distributions. Data must be shared with FSPs to make payments, with other humanitarian organizations to support coordination, with governments to link with social protection programmes, and with third-party monitors for accountability purposes. Yet, many respondents perceived data sharing to be a challenge for improving the management of recipient data (see Graph 7.3).

In recent years, valuable sector-wide guidance on CVA and data responsibility has been generated or refreshed (see Box 7.1) to enhance the protection of CVA recipients and support a more efficient, collaborative, and data-driven approach. In each case, organizational roles and responsibilities are articulated and the examples shared to help implementers contextualize and operationalize the guidance.

BOX 7.1

Guidance on CVA data responsibility

- 2020: ICRC published an updated Handbook on data protection in humanitarian action[22].
- 2020: OCHA's Centre for Humanitarian Data, CALP and NORCAP released a Guidance Note on Data Responsibility in CVA[23] to support implementers in applying global frameworks and guidance.
- 2021: CALP released a Data responsibility toolkit[24] specifically for CVA implementers to include data responsibility into each stage of the programme cycle.
- 2023: Humanitarian Data and Trust Initiative published a principled framework to create a common understanding of how to balance the risks and benefits when sharing data between humanitarian organizations and donors[25].
- 2023: OCHA's Centre for Humanitarian Data published a guidance note on the implications of cyber threats for humanitarians[26].
- 2023: IASC released an updated Operational Guidance for Data Responsibility in Humanitarian Action setting out responsibilities at three levels, System-Wide, Cluster/Sector and Organization[27] and focusing on establishing an Information Sharing Protocol (ISP) to raise awareness of and embed data responsibility at the outset of an emergency.

BOX 7.2

Mosaicking – An emerging threat

Mosaicking 'occurs when multiple datasets are linked to reveal significant new information. While such information could be used to gain insight, it could also be used by bad actors to do harm'[28]. Combining humanitarian and social protection data to reveal new information is creating new data responsibility threats. As organizations publish more information online under Open Data strategies, and humanitarian and social protection systems are sharing data to work collaboratively in supporting communities, the likelihood of data being misused increases.

For example, transaction data of pre-paid ATM cards, commonly used in CVA distributions, could be combined with the location of religious buildings to identify people who are frequently near mosques at prayer time. Similarly, food purchase data could reveal dietary patterns, indicating a specific religious or ethnic affiliation. When assessing the Humanitarian Data Exchange (HDX) platform, the Centre for Humanitarian Data team found that: 'The challenge is to understand when this can occur and what to do about it'[29]. The ICRC recommends that organizations look beyond the humanitarian data ecosystem and consider what public or private data stakeholders might have access to before sharing[30].

The necessity of sharing data and the fact that CVA programmes produce a lot of data at each step in the programme cycle means that CVA implementers are often at the forefront of data responsibility discussions which can lead to the perception that cash is held to a higher standard[31] than other modalities. Yet, **much as CVA actors often take a lead role on data responsibility – this is an issue for the entire humanitarian sector and, as such, decisions need to be taken to govern the whole system not just one part of it**.

While strong guidance now exists there seems, as some survey respondents perceived, to be a gulf between the guidance and the realities of implementation in different contexts. As a result, the IASC Deputies asked the Cash Advisory Group (CAG) to identify gaps and risks. The CAG has tasked a Data Responsibility Working Group[32] Task Team to explore the issue and propose strategies for the safe, ethical, and effective data management in the delivery of CVA.

> *"… humanitarians are being expected to hold some of the most sensitive data in the world of the most vulnerable people in the world and have the resources of mall cops to protect against the cyber hacking equivalent of Delta Force."*[33] V. Elliott quoting N. Raymond (February 2022)

Cybersecurity is a risk that few talk about in the humanitarian space, though there have been a few publicly reported large-scale cybersecurity attacks on humanitarian CVA distributions and Management Information Systems (MIS). For example, in July 2019, hackers broke into numerous UN systems, downloading staff records and contract information[34]. In January 2022, hackers accessed records of 515,000 people who had interacted with ICRC[35]. In July 2023, the Norwegian Refugee Council reported a cyber-attack on a database containing personal information of thousands of project participants[36]. It is possible, indeed likely, that there have been other breaches, leaks, and hacks which have gone unreported or unnoticed. With the rise of malicious actors using cyber-attacks alongside conventional warfare in conflicts, it may be that CVA distribution systems are impacted either directly or indirectly, potentially disabling systems when they are most needed[37]. For example, Kenya's Safaricom's M-Pesa system, which is widely used to deliver CVA,[38] was impacted by a cyber-attack in July 2023 as part of a wider attack that affected many national systems. While there have been no reports to suggest that CVA payments were impacted, the potential is evident raising questions about the degree to which humanitarian organizations have effective mitigation and management plans for such eventualities.

Reflective of such risks, OCHA's Centre for Humanitarian Data released a guidance note finding that cybersecurity preparedness was limited in the humanitarian sector[40]. It outlined implications for humanitarians, provided definitions, detailed common vulnerabilities, and explored the impact it could have on humanitarian organizations' ability to deliver support in line with humanitarian principles.

Malicious actors can attack recipients directly, as well as through humanitarian actors. Mobile phones used by most CVA recipients are budget devices that lack the Secure Elements[41] chips found in higher-end devices which serve to secure sensitive information such as banking access credentials and biometrics. Equally, feature phones and 2G networks have security problems stemming from weak cryptography. A review of mobile money apps found that six out of seven had easily exploited critical vulnerabilities[42], though ironically legacy systems can offer protection as hackers focussed on the cutting edge lack the ability to access them[43]. The security features of low-end mobile phones may improve as new products come to market. Geo Phone, for example, is working to produce the first entry-level smartphone with Secure Elements that would give people access to robust security on a sub-US$50 device[44].

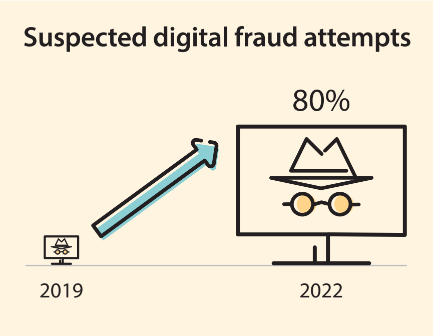
BOX 7.3

Technology to watch

If people in remote areas had access to internet-connected smartphones they could more easily be included in CVA programmes, receive funds and feed into programme design. However, reaching vulnerable populations in remote areas can be unprofitable for telecom companies using traditional mast systems.

Recent tests in Switzerland[45] and Texas[46] have confirmed the feasibility of using Low Earth Orbit (LEO) satellites to provide connectivity to standard smartphones. Such technology, combined with mobile money systems and effective regulation could allow CVA programmes to reach rural or shock-affected areas.

The GSMA plan to publish work in 2023 on LEO satellites in humanitarian settings.



Globally, suspected digital fraud attempts increased by 80% from 2019 to 2022 with bad actors focussing on organizations with direct access to money and on consumers who were engaging with organizations digitally[47]. **CVA distributions are often well-publicized in advance, and often involve people with varying levels of digital literacy who may have limited experience in avoiding digital scams** and may only have one or two avenues to raise concerns – which can also be hijacked[48]. Risks related to scamming within the CVA space have received little attention, perhaps because of the low individual transfer values and fact that money is spent out quickly. Yet scamming does seem to be a potential risk given overall increases in digital fraud. For example, Safaricom, whose mobile money M-Pesa system delivers a significant portion of humanitarian CVA in Kenya, had a class action lawsuit filed against it in 2023 for failing to tackle rising levels of fraud[50]. CVA was not implicated in this lawsuit, but it does highlight the vulnerability.

Cybercrime causes an erosion of trust and confidence in digital CVA systems that the implementation of effective legal and regulatory requirements can counter[51]. A positive correlation between high mobile money regulatory index scores and mobile money adoption and usage evidences this[52]. In addition to national regulation, to support an effective regulatory environment, GSMA offers mobile money operators a certification process to demonstrate 'that a provider has taken steps to ensure that customers' funds are in safe hands, that their rights are protected, and that a high level of customer service can be expected'[53].

Biometrics, better understood

Biometrics have supported the move from in-kind assistance towards CVA[54], with humanitarian organizations looking to biometrics, 'to eliminate fraud, reduce duplication, meet the assurance requirements and encourage confidence in States receiving vulnerable refugees for resettlement'[55]. Equally, the move towards digital payments has exposed organizations to obligations presented by international regulations that may be, in part, resolved by biometric-based identity systems.

The COVID-19 pandemic prompted a move from touch biometrics[56] towards those that could be done at a distance including iris, palm, and voice[57] and early pilots of voice biometrics were successful[58] in providing remote verification. UNHCR linked their Biometric Identity Management System (BIMS) to the Global Distribution Tool (GDT) which is used to generate payment lists and 'track the admission, verification, and collection of assistance'[59].

Views about biometrics have evolved as the benefits and the risks have become better understood. In 2015, Oxfam reversed its moratorium on the use of biometrics allowing their use 'when specific principles of responsible use' had been met[60]. In 2019, ICRC announced they would only collect biometric data in a limited number of cases, such as for travel documents, reunification of families, where it was 'in the best interests of the persons concerned' and where data would not be held centrally[61]. In 2022, WFP queried whether distribution processes needed the 'enormous' and 'rich' personally identifiable information that biometric data contains to ensure the accuracy of distributions. They also questioned whether biometrics had garnered oversized importance in humanitarian operations[62]. At the same time, research has found that the 'risks and harms (of biometrics) are not fully accounted for'[63] in humanitarian programmes and that greater risks are borne by the data subjects, than the organizations implementing the systems[64].

While loss or misuse is a risk and concern for all personal data, for biometric data the concern is elevated. If a malicious actor steals a password to your email account, they can create havoc but passwords can be changed. Your biometrics cannot be changed. High-profile humanitarian data breaches involving biometrics include Afghanistan where biometric data was collected with the support of Western donor governments, and then accessed by the Taliban to target people[65]. In Bangladesh data collected from people of the Rohingya ethnic group was shared with the Myanmar government[66] without the group's informed consent. A 2020 'audit highlighted multiple risks associated with the roll-out of SCOPE and biometrics in Yemen, including that WFP had to agree to technical arrangements and stipulations that "biometrics data shall be retained in a joint server room" with the effect that potentially sensitive data could come into the hands of de facto authorities'[67].

Issues related to data responsibility and the opportunities biometrics present for interoperability are considered in other sections of this chapter.

Blockchain pilots have expanded and multiplied

> *"Web3 technologies including blockchain-based solutions and cryptocurrencies have not lived up to their promise in the humanitarian sector, in part because they involve applying technical rather than systemic solutions to deep-rooted problems of social and economic inequality."* (Dr Margie Cheesman, Lecturer in Digital Economy, King's College London)

Humanitarian organizations have continued to pilot Distributed Ledger Technology (DLT) in many contexts including blockchain-based e-voucher programmes in Ecuador and Kenya[68], QR code payment systems in Bangladesh[69] and Nepal[70] and a recipient deduplication system in Ukraine[71]. Stablecoins – cryptocurrencies tied to fiat currencies and designed to overcome the volatility of others – have also seen more use in the humanitarian space in recent years. People in Afghanistan have used stablecoins to receive funds from overseas when international banks stopped facilitating transfers to the country[72]. While UNHCR has used stablecoins to send money to internally displaced persons and other war-affected people in Ukraine, which they could convert to fiat currency at MoneyGram locations across the country and across borders[73].

Experiences from such interventions vary. CARE Ecuador found that recipients and vendors were initially distrustful of digital currencies. They overcame this by working with a trusted local partner demonstrating that the technology worked. Oxfam's work in Vanuatu found 'modest cost-savings and significant time-savings'[74] in operational activities compared to previous similar responses where cheques were used, though they struggled to demonstrate greater efficiencies because of challenges related to the reliance on existing FSPs. Some research has found that benefits attributed to distributed ledgers such as security, auditability and interoperability and cost-effectiveness can also be derived from centralized databases[75], while other research suggests that such untested technologies often pass on risks to recipients without the offer of choice or alternatives[76].

Alongside new pilots, some ongoing initiatives have expanded. Oxfam's Unblocked Cash project which provided e-vouchers on a blockchain has expanded from supporting 35,000 households in Vanuatu to also being piloted in Papua New Guinea, Venezuela and, in future, in the Solomon Islands[77]. WFP's Building Blocks system, used to distribute e-vouchers and deduplicate recipients, has expanded from a 100-person pilot in Pakistan to supporting more than a million people in Jordan, Bangladesh, Lebanon, and Ukraine[78].

As distributed technology ledger systems continue to be tested, it remains to be seen which use case may provide valuable solutions within the CVA space.

Data interoperability and portability

The twin concepts of interoperability and portability continue to be explored, with the drive coming from donors and implementers. Demand from recipients may increase as they become aware of the potential benefits[79], for example, removing the need to register with multiple agencies and easier referrals to organizations providing non-CVA services.

For humanitarian organizations, the potential of system interoperability to enable deduplication of recipients gained interest, in contexts such as the refugee response in the Greek islands, the port explosion in Lebanon and responses in Syria and Turkey, where traditional area-based coordination techniques (which mitigate duplication) were not possible and where alternative data sources (e.g., tax ID) were not available.

Donor interest in interoperability is high. DG ECHO released a policy framework for humanitarian digitalization in 2023[80] which highlighted interoperability as an area of focus following on from the Donor Cash Forum Statement and Guiding Principles on Interoperability of Data Systems in Humanitarian Cash Programming[81]. In addition, DG ECHO funded two consortia, the Collaborative Cash Delivery (CCD) Network and Dignified Identities in Cash Assistance (DIGID) consortium which were tasked with exploring interoperability and portability from governance and technical angles.

Both CCD and DIGID's work have included landscape mapping reports and fora, creating consistent terminology, and introducing key concepts that allow stakeholders to explore the opportunities that portability and interoperability present. CCD explored opportunities of copying data stewardship models used in healthcare i.e., entities that hold data on behalf of others and allow access, normally for public, educational, or charitable aims. However, they found the data steward role to be incompatible with organizational mandates and the realities of the humanitarian sector[82].

> *"[Data portability] … by definition requires multiple participating organizations, not just internal policy and process. Most staff usually do not see the potential of wider ecosystems of data, since their focus is of necessity primarily within their own organizations; and the nature of grant-based projects means that they have limited incentive to engage with wider initiatives, absent either personal interest or a specific mandate from their organization. As a result, most organizations still have a general approach of locking down their data rather than sharing it, especially as the potential harms and potential value of data both become clearer."* (Paul Currion, CCD Network)
>
> *"[Interoperability] … remains an ambition among donors, that at an intellectual level makes sense, but it is deprived of any incentives/drivers to make it a reality on the ground."* (KII)

BOX 7.4

DIGID's Interoperability Initiative[83]

DIGID's Interoperability Initiative identified four interoperability scenarios as part of a process to create a roadmap for a way forward.

1. Deduplication of people, families, or households.
2. Sharing data on which organizations can provide what kind of support to whom.
3. Sharing data on a person with a partner, donor, or government.
4. Sharing data on a person with a payments or messaging provider.

To assist in coordination and deduplication efforts that interoperability could, in time, resolve, WFP offered their Building Blocks blockchain platform to organizations responding in Ukraine[84]. The platform offers a deduplication process based on tax IDs – where organizations could upload registration data to determine if another organization was already supporting the intended recipient. Currently operating using two nodes, run by WFP and UN Women, the ambition remains to have this as a decentralized, member-owned and operated platform. Some CVA implementers chose not to adopt the solution, a decision attributed to blockchain technology not being fully understood[85], while others questioned the transparency of the selection process over alternative technologies. In common with other deduplication efforts, the issue remains that while the technology may be able to identify a duplicated individual, CVA implementers must still determine if that person is eligible for support from more than one agency, as CVA can be distributed to achieve multiple objectives over different time periods[86]. This determination often requires agencies to share data on eligibility criteria and decide if one or both need to act which complicates the process and can lead to delayed cash distributions[87][88].

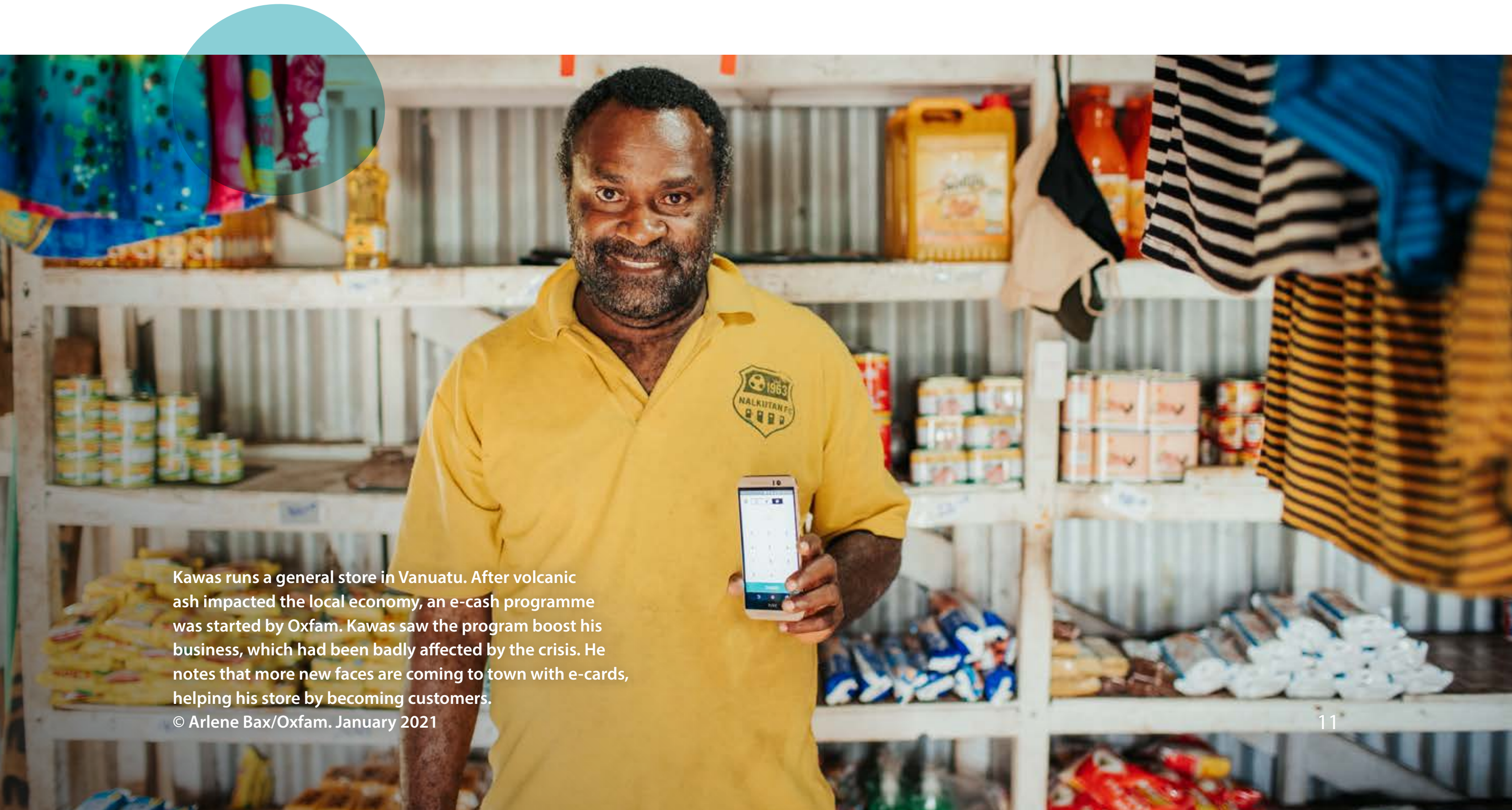
For some, questions about interoperability raise questions of power. As more organizations have focused on cash disbursement, the differentiation between them is reducing and mandates blurring. Bilateral interoperability exacerbates this dynamic as one organization loses control to another whose MIS is selected as the primary data registry. Such issues suggest that governance, legal, political, and organizational mandate barriers to interoperability are more difficult to surmount than the technical ones.

Digitalization of remote targeting and accountability

Using technology for remote targeting and accountability can complement existing CVA processes without placing additional burdens on recipients but it can also amplify existing risks or introduce new ones.

Remote targeting methods promise to increase the speed of response and improve the ability to provide support in hard-to-reach areas but, depending on the method and context, they can increase or reduce inclusion errors[89]. For example, if an approach relies on ownership of a mobile phone, those without a phone could be excluded, conversely in contexts where in-person targeting options are limited, remote targeting increases inclusion. WFP Chad, for example, found that the local authorities validated 90% of a vulnerable village list identified by satellite, and concluded that the approach was efficient[90]. They also noted it was a cost-efficient and effective tool but should not replace field surveys and validation workshops as not all vulnerabilities could be identified using remote sensing technology. Equally, in Florida, GiveDirectly used their remote targeting approach as 'a supplement to other models', not a replacement, since it allowed them to respond six times faster than previous disasters but excluded some individuals. For future responses they plan to offer complementary channels such as, 'open web-based applications, in-person operations, and collaborations with local partners'[91].

Digital self-registration platforms, often an element of remote targeting processes, can speed up registration but may exclude some people such as those with disabilities, those with lower levels of digital literacy or those without connectivity. They can also lead to an increased need for deduplication processes as recipients may submit multiple registrations, often in error rather than in a deliberate attempt to receive multiple payments[92].



Kawas runs a general store in Vanuatu. After volcanic ash impacted the local economy, an e-cash programme was started by Oxfam. Kawas saw the program boost his business, which had been badly affected by the crisis. He notes that more new faces are coming to town with e-cards, helping his store by becoming customers.
© Arlene Bax/Oxfam. January 2021

BOX 7.5

Examples of remote targeting and registration

- GiveDirectly used mobile phone Call Detail Records and machine learning in Togo to identify large numbers of people in need quickly[93].
- Mercy Corp's Lebanon Crisis Analytics Team used night-time lights data to identify economically vulnerable areas[94].
- Several organizations, including the Government, UNICEF, NRC, and WFP, created self-registration processes in Ukraine allowing 2.64 million people to be registered in 4 months[95].
- GSMA's Mobile for Development team combined cell tower records, topographical data, and population data to identify communities without phone reception[96].
- WFP Chad used satellite products to measure climatic indicators such as rainfall, temperature, and vegetation greenness to project food insecurity to be used for geotargeting[97].
- GiveDirectly used AI and satellite imagery in the US to quickly identify buildings damaged by Hurricane Ian, then overlaid government poverty data to identify areas of 'high-poverty and high damage'[98].

BOX 7.6

Using digital platforms to enhance targeting and accountability

Norwegian Refugee Council partnered with communications company Twilio to create a WhatsApp and SMS-based chatbot for people who left Ukraine and were living in Poland or Romania[99]. Potential recipients could complete a questionnaire to determine their eligibility for aid, provide information about their circumstances and requirements, and use the same system to lodge complaints[100]. Once approved, people could access funds from a MoneyGram agent and have access to a helpline to resolve any issues.

In Bulgaria, the IFRC linked their AccessRC app with WhatsApp and Viber-based chatbots, updating people on the status of their application and communicating with people on channels they were already using[101].

Digitalization of CVA accountability mechanisms can enhance both the benefits and risks for affected people[102]. It can provide better data for analysis, scale and more consistent workflows but can also exclude people with lower levels of digital literacy, without devices or connectivity and can lead to higher levels of mistrust compared to face-to-face channels[103]. Using mixed approaches can mitigate such risks. For example, Jireh Doo Foundation in Nigeria countered this by combining a system of telephone boxes where people could leave audio recordings with traditional suggestion boxes, toll free phone lines and community meetings[104].

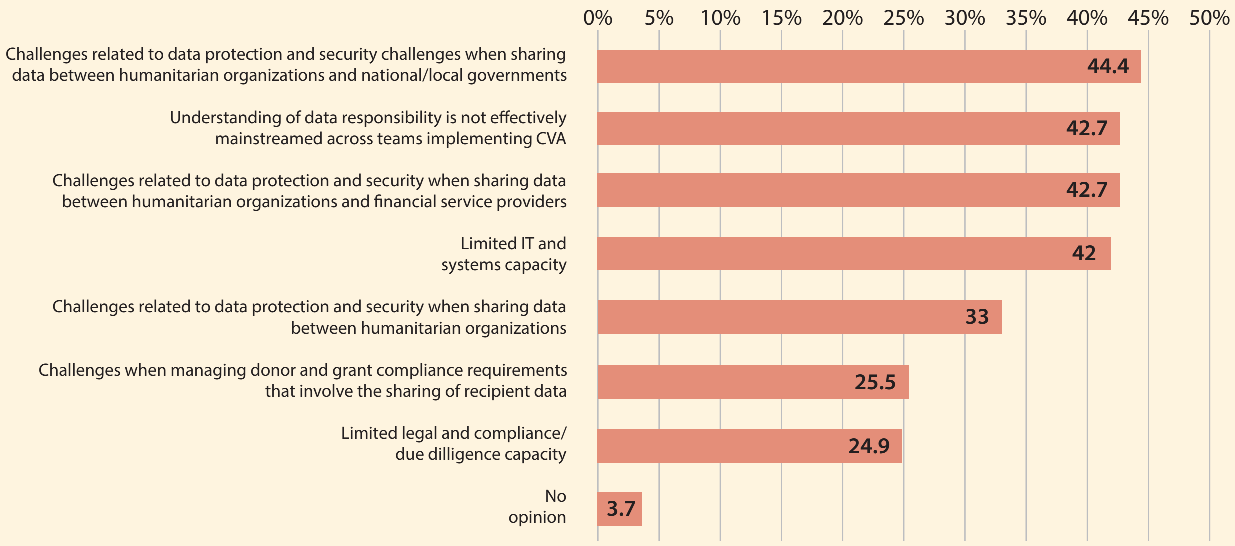
As with the digitalization of other processes such as targeting and payments, the use of digital accountability technologies is highly context-specific, and a mix of online and offline channels is important to reach as many population groups as possible[105].

High levels of MIS investment by the biggest players

MIS are expected to keep recipient data secure, while also making it accessible for analysis, be interoperable with other databases, allow payments via APIs with FSPs, deal with complex federated organizational structures and provide accountability to funders. Systems that meet all these demands require significant investment to develop and maintain and this investment has been inconsistent between large and small organizations. At one end of the spectrum, the larger UN and Red Cross CVA implementing organizations have developed their own data collection and management platforms, with WFP's SCOPE for example, costing US$47.3 million between 2013 and 2020 at HQ level alone[106]. Equally, some INGOs have developed or purchased MIS for use across all their CVA programmes, for example, World Vision International has developed the Last Mile Mobile Solution (LMMS), Concern Worldwide has deployed RedRose and GiveDirectly uses Salesforce. Many other organizations, including national NGOs rely on Open Data Kit (ODK) for data collection and Microsoft Excel for processing, then emailing payment lists to FSPs.

GRAPH 7.4

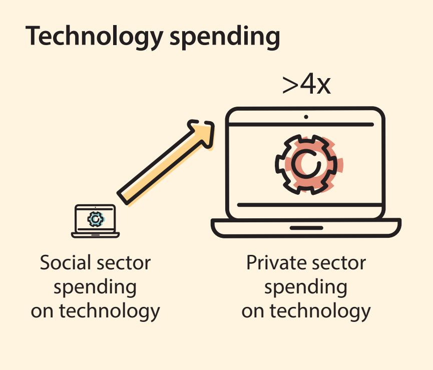
What are the biggest challenges for improving the management of recipient CVA data?



Focus group participants explained that API connections to FSP's systems promised to improve data security and increase the speed of payments. However, CVA implementers have found that field teams or FSP representatives often cannot solve the issues that arise from making these connections, and instead require the involvement of software developers – this often causes delays and offers little immediate benefits to recipients. They also reported that API connections require a significant upfront investment and needed to be justified as innovative, as they wouldn't be accepted based on a cost-benefit analysis.

RedRose's (ODK-based) system achieved prominence when they announced the signing of an agreement with the Ministry of Social Policy of Ukraine to distribute payments[107], supplementing their operations in 40 other countries. Several companies are now offering MIS solutions for CVA, each with their own focus, such as AIDONIC, GeniusTags, BeDataDriven's ActivityInfo, F4ID, CGA Technologies, UMOJALABS, and AIDKIT. No single system has been broadly adopted and each system has its own data structure and processes.

Beyond ODK's open-source mobile data collection platform, which is widely used to collect CVA registration data, CVA implementers have not taken up open-source MIS software solutions. One reason seems to be that, while open-source solutions remove the need for costly licenses, they still require money and expertise to implement. In addition, organizations are finding it more difficult to demonstrate platform stability and manage procurement than is the case for propriety software purchases from a particular vendor[108]. A collaboration between the World Bank, openIMIS and GIZ to release an open-source software package[109] to administer social protection and CVA programmes may begin the standardization and widespread adoption of a single MIS system, though the costs and complexity of hosting it may preclude its adoption by smaller NGOs.


Technology spending
>4x
Social sector spending on technology
Private sector spending on technology

An underlying issue seems to be humanitarian organizations' relatively low investment in IT. Private sector spending on technology is likely to be at least four times that of the social sector[110] with global non-profits surveyed spending just 2% on IT. This may be attributed to organizations being unable to spend time-bound project grants on IT investment, but also likely results from a thinly stretched and risk averse IT capacity when it comes to scoping, procuring, and managing systems.

Low-code solutions offer an attractive proposition for some. Staff can build and maintain such solutions with a medium level of digital literacy, increasing the chance of sustainability when developers leave, the funding cycle rolls on, or systems are handed over to governments. Some believe that as staff, who are closer to recipients, can develop solutions, they are more likely to be contextually appropriate and be designed to meet the recipients' needs. In this case, the platform owner – which tend to be large multinational entities who create new features within existing, often relatively inexpensive per user license fees – maintains system stability and security. However, some concerns remain about data security, data territoriality, long-term existence of the platforms and how to choose from a bewildering array of solutions.

Artificial Intelligence – new opportunities and risks

A recent academic review found that the 'adoption of innovative tools (in the humanitarian space) has demonstrated underwhelming results compared to the exponential growth of CVA'[111]. Artificial Intelligence (AI) may prove to be different.

Humanitarians are slowly beginning to use AI more widely outside of specialized pilots. For example, a poll of 151 people involved in the humanitarian sector found that 77% had not begun using AI, but 66% were interested[112]. The 23% using AI tools were doing so to help with transcription, translation, summarizing research sources, improving writing, generating how-to videos, and evaluating complex ideas.

AI offers clear opportunities for increasing efficiency and effectiveness of CVA, presenting alternative and faster ways of targeting, enhanced feedback loops, data analysis to improve anticipatory action, and much more.

At the same time, there are well documented concerns that AI systems focusing on the analysis of past data might continue to reproduce errors and inaccuracies and perpetuate historical inequalities, biases and unfairness[113]. These concerns are not unique to the humanitarian sector, but populations already impacted by conflict and crisis could be at even greater risk from such bias. A Red Cross review highlighted that AI had achieved mixed results in solving issues in the humanitarian sector[114], echoing the sentiments of several key informant interviewees who said that technology alone cannot solve societal, governance or human issues.

While it is hard to anticipate how AI will evolve in the sector in the coming years, given the fast pace of developments, we can anticipate that it will soon start to impact all areas of CVA. As reflected elsewhere in this and Chapter 5 on Preparedness and capacity, there is need for humanitarian agencies to upscale resourcing of technically astute professionals to ensure that opportunities are taken but, at the same time, risks are meaningfully mitigated.

Implications for the future: Areas for strategic debate and priority actions

Areas for strategic debate

Our analysis highlighted the following considerations to inform further thinking and progress in this area.

- **How can technology increase recipient choice of CVA delivery mechanism?** Recipients of humanitarian CVA often have few opportunities to make decisions about the design of the programme that supports them. Being able to choose their preferred cash delivery mechanism e.g., mobile money, cash-out agent, pre-paid debit card or bank account ensures recipients have agency over at least that aspect of the programme. However, some feel that single transfer mechanisms offer great efficiency savings, and this overrides choice. Equally, KYC, AML and sanctions regimes also create challenges. With progress in payment technologies, including the use of aggregators, the possibility of choice and efficiency becomes increasingly achievable.

- **How can new technologies be piloted without increasing risks to vulnerable communities?** Piloting innovative technologies helps to understand their benefits and risks, but humanitarian organizations need to carefully consider exposing vulnerable people to additional risks and explore alternative trials first. Piloting of DLT technologies has allowed for private sector engagement, access to non-traditional funding sources and an opportunity for humanitarian organizations to demonstrate innovation but few pilots have progressed to scale and the benefits to vulnerable populations have not always been clear. AI risks replicating offline biases and problems in an online world – at an incredible speed and scale – automating decision-making processes that recipients already feel excluded from and providing results that may be impossible to justify[115]. The significant body of work that exists outlining the risks and benefits can inform decisions on biometric deployment, and these decisions can be made in collaboration with governments, recipients, community groups and humanitarian response mechanisms while considering humanitarian principles. It is vital that humanitarian organizations have staff with the necessary levels of digital skills and clear processes for assessing and managing opportunities and risks.

- **How should CVA and payment technologies be used to support a locally-led response and a range of operational models?** MIS are encouraging consolidation of CVA distributors and centralization of recipient data and global payment framework agreements. Investments in MIS have been focussed on developing in-house data management capacity within large organizations which has left smaller organizations using a fragmented set of non-standardized proprietary solutions or basic tools that hamper their ability to analyze data safely and effectively or explore innovations such as connecting to FSPs' APIs. The centralization of recipient data in international hubs increases the negative impact if data is compromised. Global payment framework agreements promise a faster response but – at country-level – risk disempowering relationships, reducing investment and removing decision-making. In-country payment agreements present their own challenges. Multiple CVA implementers may overwhelm a small number of FSPs with time-consuming procurement processes in the aftermath of a shock. Pre-positioned contracts reduce the immediate burden on FSPs but may result in unused contracts if no shocks occur, resulting in FSPs developing procurement fatigue.

- **What are the cybersecurity risks faced by CVA stakeholders?** Distributing billions of dollars of CVA through a multitude of channels, governed by a patchwork of rules and regulations to vulnerable communities, is a potentially attractive target to those threatening cybersecurity. Cyber attacks are likely underreported – with the risk that CVA stakeholders may not fully understand current threat levels. This is likely to hamper effective planning.

- **How can humanitarian organizations and the private sector work together better in relation to CVA?** Humanitarian organizations and the private sector both continue to cite differences that hamper their ability to sit together and solve problems in a sustained way. The private sector is calling for a partnership approach, where problems can be solved together, but the tender processes and contracting on a project-by-project basis keeps them at arm's length. Recognizing and capitalizing on the differing core strengths of humanitarians and the private sector, for example, by updating procurement processes to reflect the digital services being procured, will allow the CVA space to scale faster and offer a better service to recipients.

Priority actions

In relation to the strategic debates above and other key findings in this chapter, the following are recommended as priority actions for stakeholders.

- **Humanitarian organizations** should embrace the opportunities presented by the progress in the digital payments space. This will allow them to offer choice of cash delivery mechanism to recipients, as well as allowing faster and more efficient disbursements.

- **Humanitarian organization leadership** should recognize that successful technological innovations are more likely to scale if they have been drawn from communities and the programme teams who regularly interact with them. Empowering and resourcing these groups to co-design the next set of innovations will maximize their impact.

- **Humanitarian coordination channels**, such as the Data Responsibility Working Group (DRWG), **should harness the existing data responsibility guidance and support its implementation** in CVA programmes, by curating resources that plug the gap between global guidance and implementation. **Humanitarian organizations should prioritize the implementation** of this guidance to ensure effective management of data and mitigation of risks.

- **Humanitarian organizations** should urgently make investments to ensure strong digital skills and understanding across their staff teams. This should be done within a broad range of roles including programme and community engagement, plus operational roles such as procurement and payments. Humanitarian organizations should develop the cyber security capacity of staff involved at each stage of the CVA project cycle. Recipients should also be supported to understand the digital risks they face and how they can be mitigated. This can be done in conjunction with digital literacy programmes led by governments, FSPs and financial inclusion initiatives.

- **CVA implementers** should work together to advocate to governments and regulators for improvements to regulations and policies that impact CVA recipients nationally, regionally and internationally. CVA implementers should recognize their advocacy power in making sizeable, regular, and high-profile transfers.

- **Humanitarian organizations** should always consider a multi-channel approach when deploying any technology. Recipients should, wherever possible, be given a choice in the ways they interact with programme systems and processes including registration platforms, eligibility determination, cash distribution and accountability channels.

- **Humanitarian organizations and the private sector** should collaboratively agree on approaches, such as creating standardized data models and metadata processes, developing a roadmap that will support interoperability and portability initiatives, reducing the centralization of recipient data and aligning information management efforts with the locally-led response agenda.

- **Donors** should continue their efforts to catalyze action to improve data responsibility by supporting a coordinated and consistent approach to the sharing of humanitarian data and encouraging inter-sectoral collaboration.

ENDNOTES

[1] Monich, A., Pablo, V. H-N & Raju, R. (2023) The stagnation of innovation in humanitarian cash assistance. Journal of International Humanitarian Action. 8, 4. https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-023-00136-3

[2] CALP (2023) Glossary of Terms. https://www.calpnetwork.org/resources/glossary-of-terms/

[3] Raithatha, R., Awanis, A., Lowe, C., Holliday, D. and Storchi, G. (April 2023) The State of the Industry Report on Mobile Money. GSMA. https://www.gsma.com/sotir/

[4] WFP (September 2020) Mobile Money in Mogadishu: A new way of strengthening food security. WFP. https://medium.com/world-food-programme-insight/mobile-money-in-mogadishu-a-new-way-of-strengthening-food-security-866f5ad5ab17

[5] OCHA (August 2020) Cash Based Programming in Somalia, HDX dashboard. https://data.humdata.org/visualization/somalia-cash-programing-v3/

[6] DG ECHO (022) DG ECHO Thematic Policy Document No 3 Cash Transfers. https://ec.europa.eu/echo/files/policies/sectoral/thematic_policy_document_no_3_cash_transfers_en.pdf

[7] McDowell, S., Crew, R. and Yusuf, B. (2022) The Changing Landscape of Cash Preparedness: Lists, Risks and Relationships. CALP. https://www.calpnetwork.org/publication/the-changing-landscape-of-cash-preparedness/

[8] DG ECHO (2022) DG ECHO Thematic Policy Document No 3 Cash Transfers. DG ECHO. https://ec.europa.eu/echo/files/policies/sectoral/thematic_policy_document_no_3_cash_transfers_en.pdf

[9] DG ECHO (2019) Joint Donor Statement on Humanitarian Cash Transfers. DG ECHO. https://www.calpnetwork.org/publication/joint-donor-statement-on-humanitarian-cash-transfers/

[10] ELAN DRC (2020) Cash Assistance Procurement in the DRC: Recommendations to humanitarians. ELAN DRC. https://www.humanitarianresponse.info/es/document/cash-assistance-procurement-drc-recommendations-donors-elan-rdc-2020

[11] UNHCR (2021) Guidance for Collaborative Procurement for Humanitarian Cash Transfers. UNHCR. https://www.unhcr.org/media/guidance-collaborative-procurement-humanitarian-cash-transfers

[12] Better than Cash Alliance (December 2018) Cash Digitization—UN Collaboration, Coordination, and Harmonization Opportunities. https://www.betterthancash.org/explore-resources/cash-digitization-un-collaboration-coordination-and-harmonization-opportunities

[13] ASI (2020) Cash Assistance in DRC: Evaluation of Procurement Procedures and Constraints. Study. Adam Smith International. https://static1.squarespace.com/static/5bc4882465019f632b2f8653/t/5e96c555445bca269b02f0ed/1586939241401/Cash+Assistance+Procurement+study-FV.pdf

[14] OCHA, UNHCR, UNICEF and WFP (2021) UN Common Cash Statement Progress Report. OCHA, UNHCR, UNICEF and WFP. https://reliefweb.int/report/world/un-common-cash-statement-progress-report-september-2021

[15] Ibid.

[16] UNHCR and CALP (2023) Jordan: Common Cash Facility Factsheet: A Partnership for Coordinated Cash Assistance. UNHCR and CALP. https://reliefweb.int/report/jordan/jordan-common-cash-facility-factsheet-partnership-coordinated-cash-assistance

[17] Oliveros, J. and Leghari, T. (2022) Global Payment Solutions for Humanitarian Cash Assistance. IFRC. https://cash-hub.org/wp-content/uploads/sites/3/2022/11/IFRC_GlobalPaymentSolutions_EN_LR.pdf

[18] WFP (2023) Payment Aggregators for Cash Based Transfers Expression of Interest. WFP. https://www.ungm.org/Public/Notice/195472

[19] Moret, E. (2023). Safeguarding Humanitarian Banking Channels: How, why and by whom? NRC. https://www.nrc.no/globalassets/pdf/reports/safeguarding-humanitarian-banking-channels/safeguarding-humanitarian-banking-channels.pdf

[20] Newhouse, N. (July 2021) Screening Recipients of Humanitarian Cash and Voucher Assistance: Necessary precaution or wasted resources? CALP. https://www.calpnetwork.org/blog/screening-recipients-of-humanitarian-cash-and-voucher-assistance-necessary-precaution-or-wasted-resources/

[21] O'Leary, E. (May 2021) COVID-19, Sanctions, Counterterrorist Financing and CVA. CALP. https://www.calpnetwork.org/blog/covid-19-sanctions-counterterrorist-financing-and-cva/

[22] ICRC (2020). Handbook on Data Protection in Humanitarian Action. ICRC. https://www.icrc.org/en/data-protection-humanitarian-action-handbook

[23] OCHA, CALP and NORCAP (2020) Guidance Note on Data Responsibility in Cash and Voucher Assistance. OCHA, CALP and NORCAP. https://centre.humdata.org/guidance-note-data-responsibility-in-cash-and-voucher-assistance/

[24] Raftree, L. & Kondakhchyan, A. (2021) Data Responsibility Toolkit: A guide for CVA practitioners. CALP. https://www.calpnetwork.org/publication/data-responsibility-toolkit-a-guide-for-cva-practitioners/

[25] OCHA, ICRC and Federal Department of [Swiss] Foreign Affairs (2023) A Principled Framework for Responsible Data Sharing Between Humanitarian Organizations and Donors. OCHA, ICRC and Federal Department of [Swiss] Foreign Affairs. https://centre.humdata.org/a-principled-framework-for-responsible-data-sharing-between-humanitarian-organizations-and-donors/

[26] OCHA (2023) Guidance Note on the Implications of Cyber Threats for Humanitarians. OCHA. https://centre.humdata.org/guidance-note-on-the-implications-of-cyber-threats-for-humanitarians/

[27] OCHA (2022) Overview of Revision Process for IASC Operational Guidance on Data Responsibility. OCHA. https://www.calpnetwork.org/publication/overview-of-revision-process-for-iasc-operational-guidance-on-data-responsibility/

[28] OCHA (July 2020) Exploring the Mosaic Effect on HDX Datasets. OCHA. https://centre.humdata.org/exploring-the-mosaic-effect-on-hdx-datasets/

29 Ibid.

30 Capotosto, J. (February 2021) Mosaic Effect and Revelation Risks. Humanitarian Law & Policy Blog. ICRC. https://blogs.icrc.org/law-and-policy/2021/02/09/mosaic-effect-revelation-risks/

31 HNPW (April 2023) Data Responsibility Working Group session.

32 OCHA (2021) Data Responsibility Working Group Terms of Reference. OCHA. https://reliefweb.int/topics/data-responsibility-working-group-drwg#:~:text=The%20Data%20Responsibility%20Working%20Group,responsibility%20across%20the%20humanitarian%20system

33 Elliott, V. quoting Raymond, N. (February 2022) Humanitarian Organizations Keep Getting Hacked because They can't Spend to Secure Data. Rest of World. https://restofworld.org/2022/humanitarian-organizations-hack/

34 Taylor, L. (29 January 2020) The hack the UN tried to keep under wraps. The New Humanitarian. https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack

35 ICRC (2022) Cyberattack on ICRC: What we know. ICRC. https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know

36 NRC (July 2023) Cyberattack on Norwegian Refugee Council Online Database. NRC. https://www.nrc.no/news/2023/july/cyberattack-on-norwegian-refugee-council-online-database/

37 Harrington, J. (9 March 2022) From cyber attacks to bot farms: The top tech threats humanitarians face in Ukraine. The New Humanitarian. https://www.thenewhumanitarian.org/opinion/2022/03/09/from-cyber-attacks-to-bot-farms

38 Mwai, P. and Nkonge, A. (July 2023) Kenya cyber-attack: Why is eCitizen down? https://www.bbc.com/news/world-africa-66337573

39 Barnett, M. and Schneckener, U. (2022) The SolarWinds hack: Lessons for international humanitarian organizations. International Review of the Red Cross, 104(926), 111–130. https://www.cambridge.org/core/services/aop-cambridge-core/content/view/71F740743D309BFB3E8176F71815DC72/S1816383122000194a.pdf/the-solarwinds-hack-lessons-for-international-humanitarian-organizations.pdf

40 OCHA (2023) Guidance Note on the Implications of Cyber Threats for Humanitarians. OCHA. https://centre.humdata.org/guidance-note-on-the-implications-of-cyber-threats-for-humanitarians/

41 Global Platform (May 2018) Introduction to Secure Elements. Global Platform. https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Secure-Element-15May2018.pdf

42 Butler, K. (2017) Security and Privacy Challenges for Mobile Money Applications. Florida Institute for Cybersecurity Research. https://www.cepal.org/sites/default/files/events/files/day_2-session_5-security_privacy_concerns-kevin_butler.pdf

43 Ibid.

44 Geo Phone. About Geo Phone. Geo Phone. https://geophonebd.com/about-us/

45 Mann, C. (March 2023) Salt, Starlink Switzerland Satellite Connectivity Deal. Advanced Television. https://advanced-television.com/2023/03/02/salt-starlink-switzerland-satellite-connectivity-deal/

46 Weatherbed, J. (April 2023) AT&T-backed satellite can pick up regular phone signals from space. The Verge. https://www.theverge.com/2023/4/26/23699366/att-ast-spacemobile-satellite-cellular-connection-phone-call-space

47 TransUnion (2023). TransUnion 2023 State of Omnichannel Fraud Report: Trends and strategies for enabling trusted commerce. TransUnion. https://www.transunion.com/content/dam/workfront-assets/truportfolio/GFS-22-F125939-TruVa-2023OmnichannelFraud-RPR-US_EN-US.pdf

48 Huston, J. and Stella, L. (2023) Fraud in D.R.C. – our apology and response. GiveDirectly. https://www.givedirectly.org/drc-case-2023/

49 Mwaniki, M. (2023) MPESA SIM Swap Fraud: How to protect yourself. Rest of World. https://restofworld.org/2023/mpesa-sim-swap-fraud/

50 Kamwathi, M. (July 2022) Survey finds half of mobile users lose cash to fraudsters. Business Daily Africa. https://www.businessdailyafrica.com/bd/economy/survey-finds-half-mobile-users-lose-cash-fraudsters-3654490

51 GMSA (2021) GSMA Mobile Money Programme – Mobile Money Policy and Regulatory Handbook. GSMA. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/10/Mobile-Money-Policy-Handbook.pdf

52 GMSA (2021) The Mobile Money Regulatory Index 2021: Regional and Country Profiles. GSMA. https://www.gsma.com/mobilefordevelopment/resources/the-mobile-money-regulatory-index-2/

53 GMSA (2018) GSMA Mobile Money Certification, Defining and promoting excellence in the provision of mobile money services. GSMA. https://www.gsma.com/mobilefordevelopment/mobile-money/certification

54 Holloway, K., Al Masri, R. and Abu Yahia, A. Digital Identity, Biometrics and Inclusion in Humanitarian Responses to Refugee Crises. ODI: Humanitarian Policy Group. https://www.calpnetwork.org/wp-content/uploads/2021/10/Digital_IP_Biometrics_case_study_web.pdf

55 Ibid.

56 WFP (January 2022) Strategic Evaluation of WFP's Use of Technology in Constrained Environments. WFP. https://www.wfp.org/publications/strategic-evaluation-wfps-use-technology-constrained-environments

57 Holloway, K., Al Masri, R. and Abu Yahia, A. (2021) Digital Identity, Biometrics and Inclusion in Humanitarian Responses to Refugee Crises. HPG. https://www.calpnetwork.org/wp-content/uploads/2021/10/Digital_IP_Biometrics_case_study_web.pdf

58 GMSA (2022) State of the Industry Report on Mobile Money. GSMA. https://www.gsma.com/sotir/wp-content/uploads/2022/03/GSMA_State_of_the_Industry_2022_English.pdf

59 UNHCR (May 2023) UNHCR's Biometric Tools in 2023. UNHCR. https://www.unhcr.org/blogs/unhcrs-biometric-tools-in-2023/

60 Oxfam (2021) Oxfam Biometric & Foundational Identity Policy. Oxfam. https://oxfam.app.box.com/v/OxfamBiometricPolicy

61 ICRC (2019) Policy on the Processing of Biometric Data by the ICRC. ICRC. https://www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf

62 WFP (2022) Strategic Evaluation of WFP's Use of Technology in Constrained Environments. WFP. https://www.wfp.org/publications/strategic-evaluation-wfps-use-technology-constrained-environments

63 The Engine Room (2023) Biometrics in the Humanitarian Sector, A current look at the risks, benefits and organisational policies. The Engine Room. https://www.theengineroom.org/wp-content/uploads/2023/07/TER-Biometrics-Humanitarian-Sector.pdf

64 Ibid.

65 Human Rights Watch (March 2022) New Evidence that Biometric Data Systems Imperil Afghan. Human Rights Watch. https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans

66 Human Rights Watch (June 2021) UN Shared Rohingya Data Without Informed Consent. Human Rights Watch. https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent

67 WFP (2022) Strategic Evaluation of WFP's Use of Technology in Constrained Environments. WFP. https://www.wfp.org/publications/strategic-evaluation-wfps-use-technology-constrained-environments

68 CARE (n.d.) Blockchain and Crypto at CARE. CARE. https://www.care.org/our-work/womens-economic-justice/blockchain-and-crypto-at-care/

69 WFP (April 2020) How Blockchain is Helping WFP's Fight against Coronavirus in Bangladesh. WFP. https://medium.com/world-food-programme-insight/how-blockchain-is-helping-wfps-fight-against-covid-19-in-bangladesh-d2b466a8becf

70 UNICEF (2023) Rahat: Simplifying access to cash relief. UNICEF. https://www.unicef.org/nepal/stories/rahat-simplifying-access-cash-relief

71 Tonea, D. and Palacios, V. (2022) Registration Targeting and Deduplication Emergency Response inside Ukraine Thematic-paper. CALP. https://www.calpnetwork.org/wp-content/uploads/2022/09/Registration-Targeting-and-Deduplication-Emergency-Response-inside-Ukraine-Thematic-paper-1.pdf

72 Fang, L. (19 January 2022) Starving Afghans Use Crypto to Sidestep U.S. Sanctions, Failing Banks and the Taliban. The Intercept. https://theintercept.com/2022/01/19/crypto-afghanistan-sanctions-taliban/

73 UNHCR (8 March 2023) UNHCR Launches Pilot Cash-Based Intervention Using Blockchain Technology for Humanitarian Payments to People Displaced and Impacted by the War in Ukraine. UNHCR. https://www.unhcr.org/ua/en/52555-unhcr-launches-pilot-cash-based-intervention-using-blockchain-technology-for-humanitarian-payments-to-people-displaced-and-impacted-by-the-war-in-ukraine-unhcr-has-launched-a-first-of-its-kind-integ.html

74 Rust, B. (2019) Unblocked Cash: Piloting Accelerated Cash Transfer Delivery in Vanuatu. Oxfam. https://oxfamilibrary.openrepository.com/bitstream/handle/10546/620926/rr-unblocked-cash-delivery-vanuatu-311019-en.pdf

75 Slavin, A. (2019) Distributed Ledger Identification Systems in the Humanitarian Sector. Sovrin. https://sovrin.org/wp-content/uploads/14A-Report.pdf

76 Cheesman, M. (n.d.) Web3 and Communities at Risk: Myths and problems with current experiments. Minderoo Centre for Technology and Democracy. https://www.mctd.ac.uk/web3-and-communities-at-risk-myths-and-problems-with-current-experiments/

77 Oxfam (n.d.) UnBlocked Cash Project: Using blockchain technology to revolutionize humanitarian aid. Oxfam. https://www.oxfam.org/en/unblocked-cash-project-using-blockchain-technology-revolutionize-humanitarian-aid

78 WFP (nd) Building Blocks. WFP. https://innovation.wfp.org/project/building-blocks

79 Currion, P. (2022) SAFE PASSAGE: Options for Data Portability in the Humanitarian Sector. CCD Network. https://www.collaborativecash.org/_files/ugd/477045_8adbdc1a90144e67b86f943284d1509b.pdf

80 DG ECHO (2023) DG ECHO Policy Framework for Humanitarian Digitalisation. DG ECHO. https://civil-protection-humanitarian-aid.ec.europa.eu/system/files/2023-03/DG%20ECHO%20Policy%20Framework%20on%20Digitalisation%20-%20final_0.pdf

81 Donor Cash Forum Statement and Guiding Principles on Interoperability of Data Systems in Humanitarian Cash Programming (September 2022) https://www.calpnetwork.org/publication/donor-cash-forum-statement-and-guiding-principles-on-interoperability-of-data-systems-in-humanitarian-cash-programming/

82 Currion, P. (2022) SAFE PASSAGE: Options for Data Portability in the Humanitarian Sector. CCD Network. https://www.collaborativecash.org/_files/ugd/477045_8adbdc1a90144e67b86f943284d1509b.pdf

83 Worthington, R. and Duechting, A. (2023) Landscape Mapping Overview. IFRC/DIGID. https://static1.squarespace.com/static/639843c19e367d3f019f26f6/t/64615d026ec1c54e3020066d/1684102440772/DIGID+Interoperability+-+Landscape+Mapping+Overview.pdf

84 ACTED and OCHA (26 April 2022) Ukraine: Task Team 3 – Building Blocks Ukraine Inter-Organizational Usage. ACTED, OCHA. https://reliefweb.int/report/ukraine/ukraine-task-team-3-building-blocks-ukraine-inter-organizational-usage-26-april-2022

85 Tonea, D. and Palacios, V. (2022) Registration Targeting and Deduplication Emergency Response inside Ukraine Thematic-paper. CALP. https://www.calpnetwork.org/wp-content/uploads/2022/09/Registration-Targeting-and-Deduplication-Emergency-Response-inside-Ukraine-Thematic-paper-1.pdf

86 Worthington, R. and Duechting, A. (2023) Use Case 1 – Deduplication of people, families and households. IFRC/DIGID. https://static1.squarespace.com/static/639843c19e367d3f019f26f6/t/64615d46f46ae72ee24eff24/1684102478006/DIGID+Interoperability+-+Deduplication+of+people%2C+families+or+households.pdf

87 Ibid.

88 Tonea, D. and Palacios, V. (2022) Registration Targeting and Deduplication Emergency Response inside Ukraine Thematic-paper. CALP. https://www.calpnetwork.org/wp-content/uploads/2022/09/Registration-Targeting-and-Deduplication-Emergency-Response-inside-Ukraine-Thematic-paper-1.pdf

89 Ibid.

90 WFP (2022) Geotargeting Analysis for Seasonal Assistance: Case study. WFP. https://www.calpnetwork.org/publication/geotargeting-analysis-for-seasonal-assistance-case-study-chad/

91 Keen, L. (2023) How AI Helped 6x our Disaster Response Speed. GiveDirectly. https://www.givedirectly.org/hurricane-relief-2022/

92 Worthington, R. and Duechting, A. (2023) Landscape Mapping Overview. IFRC/DIGID. https://static1.squarespace.com/static/639843c19e367d3f019f26f6/t/64615d026ec1c54e3020066d/1684102440772/DIGID+Interoperability+-+Landscape+Mapping+Overview.pdf

93 Raftree, L. (2021) Case Study: Data Responsibility and Digital Remote Targeting During Covid-19. CALP. https://www.calpnetwork.org/wp-content/uploads/2021/03/CaLP-Case-Study-Remote-Targeting.pdf

94 Mercy Corps. Lebanon Analytics Hub: Economic Vulnerability Index. Mercy Corps. https://d4it4d.shinyapps.io/Lebanon_Analytics_Hub/_w_b63c21c7/

95 Tonea, D. and Palacios, V. (2022) Registration Targeting and Deduplication Emergency Response inside Ukraine Thematic-paper. CALP. https://www.calpnetwork.org/wp-content/uploads/2022/09/Registration-Targeting-and-Deduplication-Emergency-Response-inside-Ukraine-Thematic-paper-1.pdf

96 GMSA (2020) Connected Society: Mobile Coverage Maps – How-to Guide. GSMA. https://www.mobilecoveragemaps.com/static/files/MobileCoverageMaps_HowTo_EN.pdf?v=1658397267

97 WFP (2022) Geotargeting Analysis for Seasonal Assistance: Case study. WFP. https://www.calpnetwork.org/publication/geotargeting-analysis-for-seasonal-assistance-case-study-chad/

98 Keen, L. (2023) How AI Helped 6x our Disaster Response Speed. GiveDirectly. https://www.givedirectly.org/hurricane-relief-2022/

99 Twilio (February 2023) Providing Humanitarian Assistance Without Delay. Twilio. https://www.twilio.com/blog/providing-digital-humanitarian-assistance-quickly

100 Zing (2022) Developer Q&A: Helping the Norwegian Refugee Council (NRC) deploy information gathering chatbots in Ukraine. Zing. https://zing.dev/news-and-views/helping-the-norwegian-refugee-council-nrc-deploy-information-gathering-chatbots-in-ukraine

101 IFRC (nd) Register with the Bulgarian Red Cross for Financial Assistance. IFRC https://ukrainefinancialassistance.ifrc.org/bulgarian-red-cross

102 Burton, J. (2021) "Doing no harm" in the digital age: What the digitalization of cash means for humanitarian action. International Review of the Red Cross. https://international-review.icrc.org/articles/doing-no-harm-digitalization-of-cash-humanitarian-action-913

103 CartOng (2021) What Digital Solutions for Feedback and Complaint Mechanisms? CartOng. https://www.im-portal.org/system/files/content/resource/files/main/2021_What-digital-solutions-for-feedback-and-complaint-mechanisms_CartONG_Groupe-URD.pdf

104 Samuel, M. (2022) JDF COBAFS Model to AAP. Jireh Doo Foundation. https://jirehdoo.org/wp-content/uploads/2022/09/AAP-Innovation-1.pdf

105 Ibid.

106 WFP (2021) Internal Audit of SCOPE WFP's Digital Management of Beneficiaries. WFP. https://docs.wfp.org/api/documents/WFP-0000128891/download/#:~:text=31.,driven%20implementation%20and%20hosting%20costs

107 (June 2022) Red Rose Press Release. RedRose LinkedIn. https://www.linkedin.com/feed/update/urn:li:activity:6940527332713455616/

108 Assaf, G. and Kumar, M. (2020) Open Source Software in the Social Sector: Examining Barriers, Successes, and Opportunities. GitHub/The Case Foundation. https://socialimpact.github.com/assets/img/research/GitHub_tCF_OSSInSocialSector_FINAL_updated.pdf

109 openIMIS (n.d.) openIMIS Documentation Home. openIMIS. https://openimis.atlassian.net/wiki/spaces/OP/overview?mode=global

110 NETHOPE, TAG and techsoup (2022) Digital Infrastructure Funding: A guide for governments and development partners. Nten, NETHOPE, TAG and techsoup. https://cdn.ymaws.com/www.tagtech.org/resource/resmgr/resource_library/Digital_Infrastructure-Funde.pdf

111 Monich, A., Pablo, V. H-N., and Raju, R. (2023) 'The stagnation of innovation in humanitarian cash assistance'. Journal of International Humanitarian Action. 8, 4. https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-023-00136-3

112 CALP (February 2023) How are Humanitarians using AI Tools like Chat GPT? CALP. https://www.calpnetwork.org/blog/how-are-humanitarians-using-ai-tools-like-chat-gpt/

113 Beduschi, A. (2022) Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks. International Review of the Red Cross 919. https://international-review.icrc.org/articles/harnessing-the-potential-of-artificial-intelligence-for-humanitarian-action-919

114 Ibid.

115 Blouin, L. (2023) AI's 'black box' problem means that researchers are often unable to why an AI model gave a particular response. https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained