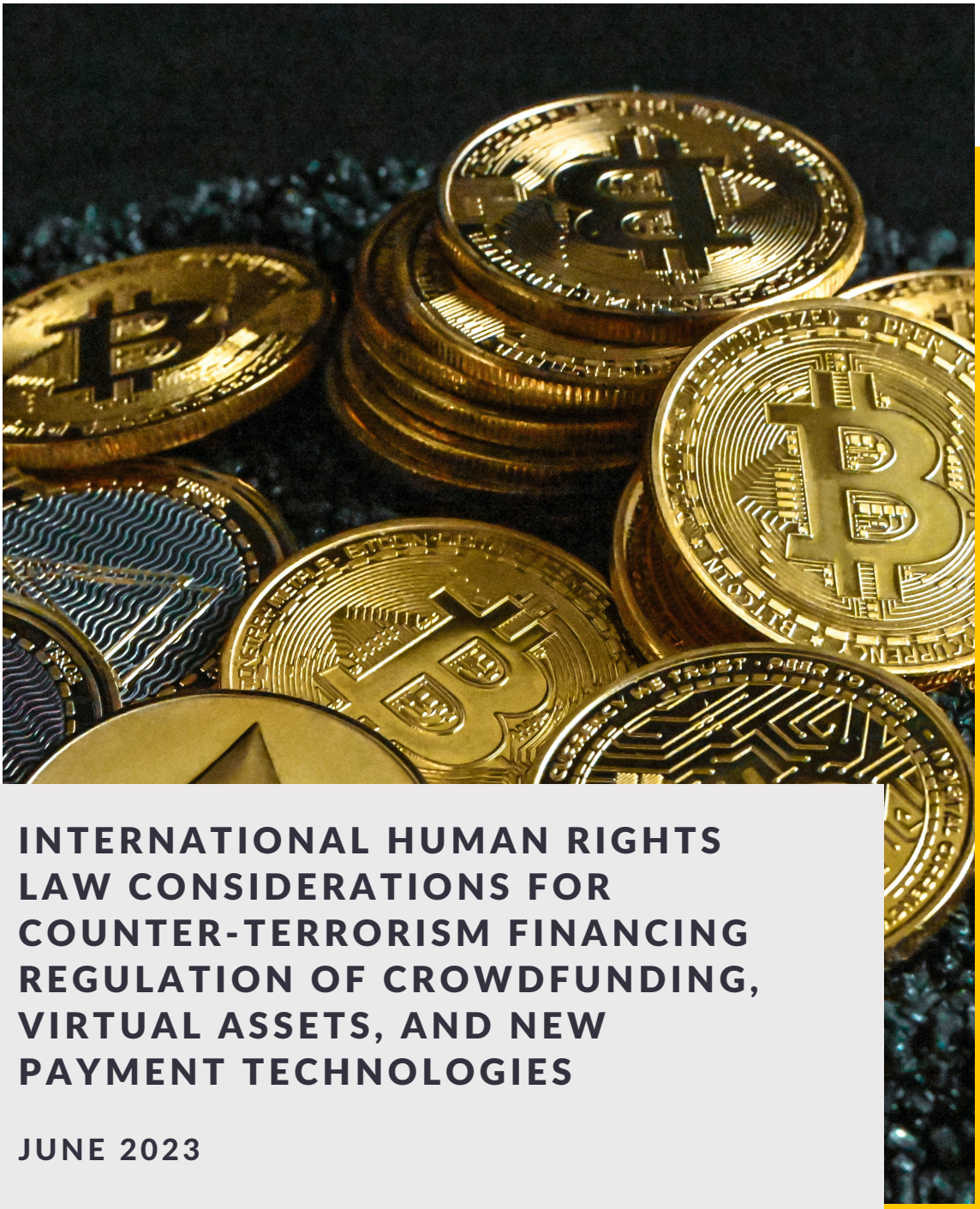
UNITED NATIONS
HUMAN RIGHTS
SPECIAL PROCEDURES
SPECIAL RAPPORTEURS, INDEPENDENT EXPERTS & WORKING GROUPS

Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism



INTERNATIONAL HUMAN RIGHTS LAW CONSIDERATIONS FOR COUNTER-TERRORISM FINANCING REGULATION OF CROWDFUNDING, VIRTUAL ASSETS, AND NEW PAYMENT TECHNOLOGIES

JUNE 2023

Acknowledgements

This position paper on International Human Rights Law Considerations for Counter-Terrorism Financing Regulation of Crowdfunding, Virtual Assets, and New Payment Technologies is presented by Professor Fionnuala Ní Aoláin, the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.

Work on this report was led by Alyssa T. Yamamoto, Legal Advisor to the Special Rapporteur. Legal Advisor Adriana Edmeades Jones provided inputs to the completion of the report. Facilitation and publication management for this work was provided by the Human Rights Center at the University of Minnesota Law School, which provides ongoing programme management support to the mandate of the Special Rapporteur. Facilitation and programme management for the work of the Special Rapporteur are led by the Office of the UN High Commissioner for Human Rights.

The Special Rapporteur extends appreciation to colleagues at the Human Security Collective and European Center for Not-for-Profit Law (both leading members of the Global NPO Coalition on FATF (Financial Action Task Force)), as well as the World Bank for their thoughtful review of and contributions to the report.

Introduction

Since its establishment, the mandate of the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (SR) has focused on the intersection of countering the financing of terrorism (CFT) measures and State obligations under international human rights law and international humanitarian law.[1] As the international community has grappled with novel CFT issues —including in recent years, the appropriate way to regulate crowdfunding, virtual assets, and new and emerging payment technologies and financial instruments—so too has the SR. Although international convenings and guidelines have sought to address how existing international CFT obligations and regulatory frameworks may extend to these digital assets and new payment technologies,[2] less attention has been paid to the potential human rights consequences of such regulatory responses, including their impacts on civil society and civic space.[3]

This position paper sets out some **preliminary human rights and rule of law considerations at this global regulatory inflection point**. Building on her Position Paper on the Human Rights and Rule of Law Implications of Countering the Financing of Terrorism Measures,[4] the Special Rapporteur cautions against the overregulation of virtual assets and new payment technologies and underscores the need for any CFT regulatory response to be proportionate to the empirically identified terrorism financing risks and vulnerabilities identified, specific to platform user. She reiterates the importance of ensuring compliance with the international law requirements of legality, proportionality, necessity, and non-discrimination, and reiterates the conceptual alignment of a human rights-based approach to CFT rooted in necessity and proportionality with the requisite Financial Action Task Force (FATF) risk-based approach.

The position paper defines "virtual assets" as a "digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes."[5] This includes both centralized and decentralized digital assets that have been tokenized, i.e., converted into security tokens representing real tradable assets. "Crowdfunding" is defined as a way for individuals or entities to raise money, through donations or investments, from multiple individuals, as facilitated by online platforms.[6] A form of crowdsourcing, crowdfunding has a long history of practice with various iterations of platforms and networks.[7] Today crowdfunding may solicit funds through both traditional and new payment methods, including virtual assets. Recognizing the diverse range of existing and developing virtual assets and cryptocurrency systems,[8] the paper addresses the payment technologies landscape broadly, including to encompass the underlying blockchain technologies[9] that enable virtual assets, cryptocurrencies and non-fungible tokens, among other financial instruments.

The position paper proceeds in three parts. **Part 1** considers the risks and benefits of virtual assets and new payment technologies and cautions against a presumption of inherent terrorist financing risk. **Part II** briefly summarizes recent trends in regulatory responses to these new technologies at the international and national levels, including calls from the UN Security Council and General Assembly to protect against their abuse for the purpose of terrorist financing. **Part III** considers the potential human rights impacts of CFT regulatory responses to new payment technologies, namely impacts on the rights to privacy, freedom of association, due process and fair trial, and non-discrimination, as well as humanitarian assistance. Part III is non-exhaustive and intended only as illustrative of potential considerations for States and private actors including in any related human rights impact assessment. The SR concludes by

reiterating the urgent need for human rights due diligence and ex ante impact assessments, meaningful civil society participation in the design, delivery, and assessment of CFT measures, independent, impartial oversight, and accountability for any human rights abuse. Moreover, she underscores the need to exercise restraint and humility to ensure responsible regulation virtual assets, crowdfunding, and new payment technologies —particularly with recognition of both the nascent documentation of the terrorist financing risks and the lack of assessment in place for downstream human rights and humanitarian consequences.

I. Risks & Benefits of Virtual Assets and New Payment Technologies

Although cryptocurrencies and virtual assets have existed for over a decade,[10] their use has only moved into the mainstream in the past few years, with mixed success and undoubted volatility.[11] The use of crowdfunding has also expanded in recent years, in part due to the Covid-19 pandemic, which limited the ability to raise funds through in-person contact.[12] Civil society organizations as well as international organizations have begun accepting and transferring cryptocurrency donations and grants in turn.[13] In addition, there has been a rise in the use of mobile money platforms and other digital financial services as a core component of financial inclusion efforts,[14] particularly in developing countries where the rural unbanked otherwise may face challenges conducting financial transactions.[15] New payment technologies and digital financial services have also proven particularly useful in humanitarian crises and conflict regions, where there are limitations to the formal banking sector.[16]

The SR underscores that new payment technologies and digital financial services play a vital role in advancing financial inclusion, ending poverty, promoting economic growth and productive employment, and attaining development goals, including in line with the Sustainable Development Goals.[17] Indeed, digital financial services are "a critical lifeline for billions of people facing emergencies (health, natural disasters, conflict) and can be designed to benefit women in particular"—reducing the gender gap in financial inclusion—and other marginalized and vulnerable communities.[18] **She acknowledges that the proliferation of virtual assets, crowdfunding, mobile money platforms, and other new payment technologies warrants thorough identification of the empirical risks of and vulnerabilities to terrorist financing abuse, but emphasizes that the proven and potential benefits of such technologies must remain at the forefront of any regulatory discussions**.

Terrorist financing risk assessments are part and parcel to the adoption of any proportionate, risk-based approach in line with the FATF Standards. To date, however, there is still only a limited body of evidence of the empirical threats posed by these new technologies. Although there have been discrete instances identified where designated terrorist groups have misused virtual assets and online exchanges and wallets,[19] the exact extent of misuse of virtual assets and new payment

technologies remains unclear.[20] Existing documentation of virtual asset misuse typically focuses on money laundering, fraud, and theft broadly speaking; where terrorist financing is referenced, it is often not disaggregated from broader money laundering and financial crime cases.[21] Despite the limited documentation of misuse, there appears to be, as some commentators have observed, "an obsession with the perceived vulnerabilities of new technologies" that has inflated the actual threat posed.[22] The SR observes in this context the inordinate focus that many States have taken on combatting purported terrorist financing risks, including as posed by non-profit organizations and civil society more broadly, despite limited empirical evidence.[23]

Notwithstanding the empirical risks of terrorist financing abuse of virtual assets, crowdfunding, and other new and emerging payment and financial technologies, the SR reiterates the potential benefits of these technological advancements, especially to fully resource a vibrant and active civil society—a key component part of any effective counter-terrorism and preventing or countering violent extremism strategy.[24] She notes in this regard that **virtual assets and crowdfunding have become an attractive alternative for civil society to secure funding, often in the face of undue de-risking, financial exclusion, and/or unreliable banking systems**. As the Special Rapporteur on the rights to freedom of peaceful assembly and association has observed, through new digital technologies including crowdfunding platforms, "civil society organizations have been able to reach new audiences, spread information, attract members and find funding in ways that were previously impossible or extremely costly."[25] New financial technologies, particularly blockchain systems, can facilitate faster and easier donations and further diversify a non-profit organization's donor base.[26] By rendering the transfer of value of information without intervention from a trusted third party, blockchain technologies and virtual assets have also been of particular use to facilitate humanitarian assistance and to support human rights defenders, political dissidents, and democracy advocates.[27] Blockchain features have similarly been used to combat human rights abuses in supply chains, secure land titles, and provide financial services to the unbanked.[28] Encryption, pseudonymity, and other security features have also facilitated the right to associate, particularly among minorities;[29] and separately or together, created a zone of privacy to protect opinion and belief,"[30] the need for which is acute in "hostile political, social, religious and legal environments." In this regard, some commentators have stipulated that virtual assets and other emerging financial technologies offer new solutions to the unintended consequences resulting from the misapplication of the FATF Standards.[31]

II. Regulatory Responses

A. International Developments

The global counter-terrorism architecture, including the United Nations Security Council, General Assembly, Counter-Terrorism Executive Directorate, Office of Counter-Terrorism, and Global Counter-Terrorism Coordination Compact, as well as Financial Action Task Force and Global Counter-Terrorism Forum, among others,[32] has sought to keep up with the expanding use of virtual

assets and new payment technologies and the potential threat of their misuse for the purpose of terrorist financing. In Resolution 2462, the Security Council called on States "to enhance the traceability and transparency of financial transactions, in compliance with international law, including international human rights law and humanitarian law." This includes:

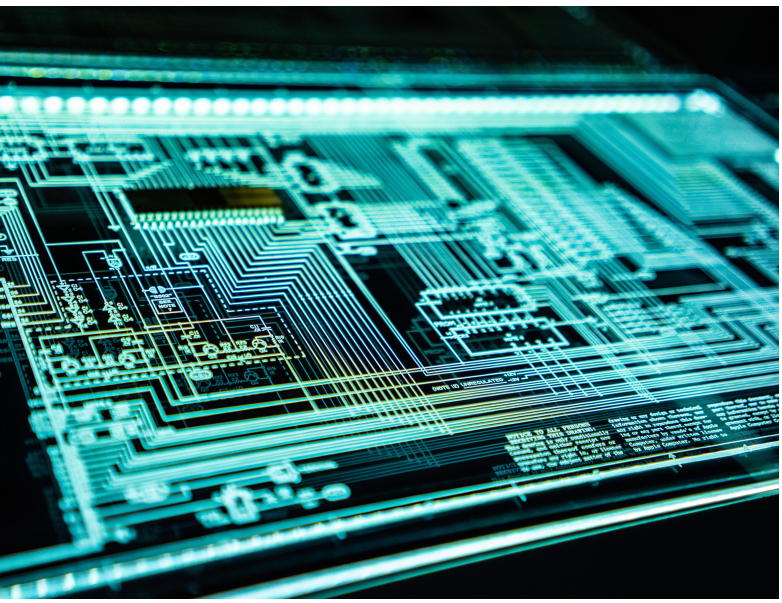
> ***assessing and addressing potential risks associated with virtual assets and as appropriate, the risks of new financial instruments, including but not limited to crowd-funding platforms, that may be abused for the purpose of terrorist financing and taking steps to ensure that providers of such assets are subject to AML/CFT obligations.***[33]

The Security Council Counter-Terrorism Committee's Delhi Declaration further recalled the need for Member States to implement CFT "regulations, monitoring, and supervision to providers of relevant services," and called on States to "enhance the specialized expertise and capacity of the authorities … to keep pace with the rapid evolution in financial tools and terrorism-financing methods" and to "establish effective partnerships with the private sector, including financial institutions, the financial technology industry and Internet and social media companies, with regard to the evolution of trends, sources, and methods of the financing of terrorism."[34] Along similar lines, in its Seventh Review of the Global Counter-Terrorism Strategy, the General Assembly called on Member States to "enhance their efforts in the fight against the financing of terrorism by … tackling the risks associated with … virtual assets and other anonymous means of monetary or financial transactions, as well as to anticipate and address, as appropriate, the risk of new financial instruments being abused for the purpose of terrorist financing."[35]

The FATF has taken the lead in clarifying how exactly States may protect against terrorist financing abuse in this new and technologically complex terrain. In October 2018, the FATF updated its Standards to clarify that they extend to financial activities involving virtual assets and virtual asset service providers. In particular, the amended FATF Recommendation 15 and its interpretative note stipulate that countries ensure that virtual asset service providers are regulated for anti-money laundering (AML) and CFT purposes, licensed or registered, and subject to effective systems for monitoring or supervision, including through licensing or registration, customer due diligence, record-keeping, suspicious transaction reporting, and international cooperation.[36] In particular, FATF's Travel Rule requires virtual asset service providers and other financial institutions to share relevant originator and beneficiary information alongside virtual asset transactions. The Security Council welcomed the extension of FATF Standards to virtual assets, and in this vein, has encouraged "Member States to apply risk-based anti-money laundering and counter-terrorist financing regulations to virtual asset service providers."[37]

The SR acknowledges FATF's normative leadership, as well as her mandate's ongoing positive constructive engagement with the FATF Secretariat and Presidency, as well as its members. She reiterates, however, her concerns previously expressed regarding the broader human rights deficits of the FATF norms and structure, as well as the legitimacy concerns stemming from the role of FATF fast-tracking "soft" standards, including through gold-plating by the UN Security Council.[38] Although she positively recognizes that FATF has clarified that its guidance on virtual assets may interface with the non-profit sector,[39] she expresses serious concern that **inadequate attention has been paid to the structural consequences of CFT regulation of virtual assets and other new payment technologies on human rights and fundamental freedoms** (as discussed further below). At most, the FATF guidance acknowledges that implementation of the FATF virtual asset standards should be "compatible with national data protection and privacy rules"—absent reference to underlying international human rights and broader public international law norms.[40]

The SR reiterates that any regulatory measures carried out in furtherance of the foregoing CFT obligations must be carried out in accordance with other international law obligations, including under international human rights law, international humanitarian law, and international refugee law.[41] Indeed, as the Security Council has expressly clarified, States enacting CFT measures, including with regard to terrorist financing risks stemming from virtual asset abuse, must act "in compliance with international law, including international human rights law and humanitarian law."[42] The SR further observes in this context that international organizations, including UN entities, providing technical assistance and capacity building to Member States in this space[43] must similarly ensure the requisite human rights-based approach to regulating virtual assets, crowdfunding, and new payment and financial technologies.



B. National Developments

The present state of national CFT and broader regulatory responses to the use of virtual assets, crowdfunding, and other technologies is quite fragmented. While some States have granted unbacked tokens legal tender status, others have adopted outright bans on the use of certain cryptocurrencies, or sought to adopt more targeted restrictions, recognizing the varying degrees of regulation, supervision, oversight, and taxation that may be appropriate depending on the use case.[44] These regulations include rules requiring mandatory data collection on users and transactions, including mandatory reporting of certain transactions reaching a certain monetary threshold, and regulations only permitting built-in anonymization in trading platforms where the full transaction history remains identifiable by authorized virtual asset service providers.[45] Other policymakers particularly within the European Union have targeted virtual assets and virtual asset providers as the riskiest of new financial technologies with regard to terrorist financing.[46] Still, the majority of countries have not yet started regulating virtual assets and virtual asset service providers,[47] and fewer still have adopted any regulations specific to countering the terrorism of financing. The SR reiterates in this regard that further, inclusive, **comprehensive empirical research is needed to analyze terrorist financing risks and vulnerabilities, specific to identified technologies, products, services, sectors, uses, and user in various contexts, also taking into account emerging sector-specific self-governance measures**. She cautions against exacerbating the existing, disproportionate emphasis and unintended consequences of CFT measures by presumptively assuming terrorist financing risks among the non-profit sector and civil society activities.[48]

Certain States have also adopted new legislation, regulatory controls, and policies for crowdfunding activities, including as related to charitable non-profit activities, at times on the basis of AML/CFT.[49] These include regulations requiring individuals and entities to formally register and/or obtain permission from governmental authorities before engaging in any crowdfunding activities, and also regulations requiring online crowdfunding platforms to report transactions in accordance with other anti-money laundering and CFT regulations.[50]

A key actor in these regulatory responses to virtual assets, crowdfunding, and new payment

and other financial technologies is the private sector, whether through formal delegation through public-private partnerships or independent responses. For instance, technology firms have:

- *proactively adopted de-risking, de-platforming and other risk avoidance measures against civil society organizations, individuals, and communities;*
- *partnered with legacy financial institutions in adopting appropriate regulatory responses;*
- *simply assumed some terrorist financing risks as part of the overall risk of doing business;*[51] *and/or*
- *joined forces including in private-private partnerships like the global FinTech Financial Crime Exchange, which encourages cross-jurisdictional information and best practice sharing.*[52]

III. International Human Rights Law Considerations

The SR reiterates the importance of States ensuring that any CFT measure adopted—whether to regulate or supervise financial activities using traditional assets or virtual assets and new payment and other financial technologies—comport with their concurrent obligations under international law, including international human rights law, international humanitarian law, and international refugee law. She reaffirms here the clear interface of CFT obligations stemming from the Terrorist International Convention for the Suppression of the Financing of Terrorism, Security Council and General Assembly resolutions, and the FATF Standards, with existing international law obligations, as set out in her broader position paper on CFT.[53] She underscores that financial technology firms and other private actors operating in the virtual assets, crowdfunding, and new technologies space have independent human rights obligations, as set out in the UN Guiding Principles on Business and Human Rights.[54]

Regrettably, the SR observes that many States continue to fail to mainstream human rights into CFT laws, regulations, and policies, including when implementing CFT measures relating to the non-profit sector and civil society more generally.[55] She is seriously concerned that early CFT regulation and policymaking in the virtual assets and new financial technologies space—such as restrictions on virtual currency and mobile money donations, registration and reporting requirements for crowdfunding activities, and information-sharing partnerships across jurisdictions—may not have adequately considered their direct and indirect human rights impacts. She is also concerned about the vulnerabilities of small, newer financial technology firms and private entities to human rights abuse, absent further resourcing and knowledge building on international human rights law, international humanitarian law, civic space, and financial inclusion. The SR **cautions States, private actors, and other stakeholders against preemptive and over-regulatory CFT responses untethered to empirically identified risks and vulnerabilities of specific sub-sector users** to terrorist financing. She underscores the importance of ensuring non-discrimination in the implementation of any new CFT measures, acknowledging the well-documented, disproportionate harms to women, LGBT and gender diverse persons, and ethnic and religious minorities, as well as intersecting forms of discrimination in practice to date.[56]

The following section sets out a non-exhaustive list of human rights and fundamental freedoms that may be implicated by CFT measures regulating or restricting the use of virtual assets, crowdfunding, and other new and emerging payment technologies and financial instruments.

A. Right to Privacy

Imprecise or overbroad CFT laws, regulations and policies on virtual assets, cryptocurrencies, crowdfunding, and mobile money platforms may risk unlawful infringement on the right to privacy, which is enshrined under international human rights law[57] and a gateway right to other rights and fundamental freedoms. In particular, regulations that limit the degree of anonymity on the blockchain and/or require expansive monitoring, collection, storage, and transfer of sensitive data, including biometrics and other analytics, by virtual asset service providers, crowdfunding and digital platforms, and/or government agencies—including through cross-jurisdictional information-sharing activities—may endanger the right to privacy. Such measures also risk impinging on other applicable data privacy and protection regulations, such as the right to be forgotten.[58]

In this context, the SR echoes the finding of the former Special Rapporteur on the right to privacy that any States enacting measures that may interfere with the right to privacy must ensure the measure is:

> ***authorized by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse.***[59]

She observes in this context that by their very nature, because blockchains permanently record transactions, any policy to collect transactional crypto data may risk

encompassing a march larger swathe of personal data and sensitive information than what the regulation purports to cover. Any privacy policies including on how Central Bank digital currencies, financial technology platforms, and other intermediaries process personal data must therefore be made transparent and readily available to consent by users. Moreover, in this context the SR underscores the **importance of techniques that are being developed to reinforce confidentiality and anonymity and to give users more control over their data**,[60] as well as ongoing efforts to limit the storage and transfer of such data with third parties.[61]

B. Rights to Freedom of Association and Expression

CFT restrictions on the use of virtual assets and new payment technologies may also impose undue restrictions on the rights to freedom of association, peaceful assembly, opinion, and expression.[62] The SR observes in this context that the network of users that cooperate on blockchains is in itself an association in the broadest sense.[63] As the Independent Expert on debt, other international financial obligations and human rights has underscored, the "backbone of the digital economy is hyper connectivity which means interconnectedness

of people, organisations, machines that results from the Internet, mobile technology and the internet of things."[64] CFT regulatory measures requiring governmental vetting of fundraising activities or other approvals and reporting requirements for the use of new financial technologies are highly vulnerable to disproportionate, undue implementation in potential contravention of these rights. For instance, restrictive CFT measures requiring registration with authorities prior to undertaking any crowdfunding campaign or other mobile money transfers and enhanced customer due diligence protocols on the part of service providers may result in the de-platforming or de-risking of individuals or entities, on the basis of their well-protected political speech, human rights advocacy, and/or humanitarian activities.

As with CFT measures regulating traditional assets, a proportionate and human rights compliant approach must be taken with regard to virtual assets and related financial activities, without making blanket assumptions about the level of risk by virtue of its technological features alone. In this regard, the SR echoes the call by the Special Rapporteur on freedom of peaceful assembly and of association in his report on access to resources for States to:

> ***ensure that associations – registered and unregistered – can fully enjoy their right to seek, receive and use funding and other resources from natural and legal persons, whether domestic, foreign or international, without prior authorization or other undue impediments – including from individuals, associations, foundations and other civil society organizations, foreign Governments and aid agencies, the private sector, the United Nations and other entities.***[65]

She observes how overbroad non-profit registration and reporting requirements adopted in the name of CFT—including the dissolution of unregistered organizations, restrictions on permissible funding sources, and de-risking limiting access to funding and bank accounts—have already had significant impacts on the ability of civil society organizations to operate.[66] CFT regulatory responses to new financial technologies may merely exacerbate these challenges, particularly for individuals or organizations that have turned to virtual assets, mobile money platforms, and other new and emerging technologies as a direct result of undue CFT restrictions on traditional assets. The impacts not just on the right to freedom of association and peaceful assembly, but also on financial inclusion and broader developmental rights—including as stipulated in the Sustainable Development Goals—may be particularly dire in this respect.

On the regulation of crowdfunding platforms, the SR emphasizes that crowdfunding platforms can serve important public benefit and protected charitable purposes. She cautions against including crowdfunding platforms under the definition of "obliged entities"[67] and reiterates the importance of ensuring any regulatory requirements imposed are directly tailored to empirically identified terrorist financing risks and vulnerabilities specific to the platform and uses at hand. Presumptively including these platforms could have chilling effects on the rights of individuals to form, lead, participate in, fundraise for, or otherwise support civil society groups and communities.

The SR underscores that restrictive measures affecting the freedom of peaceful assembly and association must meet the proportionality, necessity, legality, and non-discrimination test, and must be "limited to the associations falling within the clearly identified aspects characterizing terrorism only. They must not target all civil society associations."[68] Indeed, as the FATF has clarified, it is important that "measures taken to protect them do not disrupt or discourage legitimate charitable activities, and should not unduly or inadvertently restrict NPO's ability to access resources, including financial resources, to carry out their legitimate activities."[69] This is particularly important to ensure a risk-based approach pursuant to the FATF Standards including with regard to any

CFT regulatory approach to associations or non-profit organizations and their funding—as well as broader civil society entities, individuals, families, and communities—including virtual assets, pursuant to FATF Recommendations 8 and 15.

C. Right to Humanitarian Assistance

As mentioned above, virtual assets and new payment technologies have proven particularly vital in humanitarian crises, where often the formal banking sector is either inoperable or seriously hindered.[70] In line with international humanitarian law, it is important that CFT and broader counter-terrorism measures **not target and impede the digital payments and funds transfers of humanitarian actors intended for the delivery of neutral, independent, and impartial humanitarian assistance**, including medical assistance, food, shelter, and other essential services for the civilian population to survive.[71] Indeed the SR has previously cautioned against the use of CFT measures that criminalize or otherwise have chilling effects on protected humanitarian and human rights activities in conflict settings.[72]

D. Due Process Rights

The SR recalls the observation by the FATF that several categories of CFT measures may have due process and procedural rights impacts, including "issues relevant to investigation and prosecution of TF and ML offences, such as the presumption of innocence and a person's right to effective protection by the courts" and "incorrect implementation of UNSCRs and FATF Standards on due process and procedural issues for asset freezing, including rights to review, to challenge designations, and to basic expenses."[73] These challenges apply equally to CFT measures regulating virtual assets, crowdfunding, and other new payment technology activities, including where States may stipulate platform registration procedures, surveillance and screening powers, and de-platforming and disciplinary sanctions to public entities and/or designated service providers. They are further complicated by the transnational and cross-jurisdictional nature of transactions on public blockchains and other new payment platforms, as well as the alternative dispute resolution provisions typically offered there.[74]

As with CFT measures regulating traditional assets, due process safeguards and procedural guarantees must be provided in line with international human rights law.[75] For instance, where associations are required to apply for authorization to use crowdfunding and other platforms, they should have prior notice and an opportunity to appeal a rejection before an independent, impartial body. Where surveillance and other discretionary powers are invoked by public entities, operations should be approved "only in accordance with international human rights law and when authorized by a competent, independent and impartial judicial body, with all appropriate limitations on time, manner, place and scope of the surveillance."[76] Moreover, where the right to privacy is implicated—as is frequently the case (see Part III.A)—**robust, independent oversight systems are particularly vital, both through the involvement of an independent and impartial judiciary and the availability of effective remedies in cases**[77] **of abuse**. The SR also stipulates that due process and procedural rights should be considered in FATF mutual evaluations and other assessments of CFT compliance.

These requisite due process safeguards apply equally to States and private entities, such as virtual asset service providers, financial intermediaries, crowdfunding platforms, and other financial technology firms due to the independent human rights obligations of businesses. For instance, in instances of de-platforming, de-risking, and other administrative measures, there should be a right to review and appeal decisions. Moreover, in criminal and civil proceedings involving virtual assets, as with such proceedings involving terrorist financing claims involving traditional assets, there must be a presumption of innocence, the principle of equality of arms, and the right to review and appeal designations. The SR echoes the call by the UN Office on Drugs and Crime that investigative practices applied to virtual assets be "based on the respect for fundamental rights and guarantees of parties to the criminal proceedings."[78]

E. Non-Discrimination

As with other CFT measures, the SR underscores the importance of protecting the principles of equality and non-discrimination when implementing CFT regulatory measures in the virtual assets, crowdfunding, and new financial technologies space.[79] No CFT measure should be used to unduly restrict the legitimate activities of non-profit organizations, including organizations committed to minority rights, religious freedom, gender identity and sexual orientation, and other marginalized issues, or the legitimate activities of these communities served. Non-discrimination must be guaranteed in any decision-making procedures by platform operators and State actors determining eligibility and managing data and contents. This **extends to any online-automated procedures and artificial intelligence algorithms that may have been built in to operate, process, analyze and detect transactional and other sensitive data, as such technologies are vulnerable to discriminatory biases**.[80] The need for robust non-discrimination safeguards also applies to any CFT risk assessment processes relying on social media intelligence and automated detection models. With these challenges in mind, the SR underscores the importance of developing and embedding—in partnership with affected communities and civil society—any terrorist financing risk assessment and CFT review processes with human feedback loops on top of artificial intelligences.[81]

Conclusion

The SR **incorporates by reference here the recommendations set out in her CFT position paper** as equally applicable to CFT measures adopted in the virtual assets, crowdfunding, and new and emerging financial technologies space.[82] As with traditional assets, any CFT laws, regulations, policies, and measures on virtual assets, crowdfunding, and new payment technologies at the national, regional, or international level must protect against human rights abuses, including unlawful infringement on the rights to privacy, freedom of association, due process, non-discrimination, and other fundamental rights and freedoms.

Safeguarding against CFT regulatory abuse or overreach in the virtual assets, crowdfunding, and new payment technologies space requires, among others:

- **meaningful participation** by civil society and affected communities in the design, delivery, and oversight of CFT regulatory responses at the national, regional, and international levels;
- **consistent coordination with human rights and development entities**, including at the international level in coordination with the Office of the UN High Commissioner for Human Rights, UN Development Programme, World Bank, and other entities tasked with advancing financial inclusion and the Sustainable Development Goals;
- **transparent, accessible, and readily comprehensible risk assessments** of the risks and vulnerabilities of virtual assets, crowdfunding, and other new financial technologies to terrorist financing, specific to identified technologies, products, services, sectors, uses, and users in various contexts and taking into account existing self-governance and internal controls;
- **further, concerted empirical research** on the scale and scope of the use of virtual assets and new payment technologies, and its impact on financial inclusion and other fundamental rights and freedoms—as well as the impacts of disproportionate regulation on financial exclusion;
- **human rights and gender ex ante impact assessments, due diligence, and benchmarking** in the rollout of any CFT regulatory measure, particularly in safeguarding the rights to privacy, freedom of assembly and association, freedom of opinion and expression, and other fundamental rights and freedoms;
- **unambiguous exemptions** for humanitarian and human rights organizations and protected activities therein;
- **independent, impartial oversight and review processes** for financial technology registration procedures, de-risking, de-platforming, and other discretionary measures;
- **independent and adequately resourced oversight of UN and other international and regional organization entities** providing technical assistance to States on CFT and new payment technologies; and
- **consideration in any assessment of CFT compliance** of human rights impacts, including on financial inclusion and related rights, and overregulation.

Lastly, the Special Rapporteur emphasizes that new payment and financial technologies are still in their early stages of development, with varying models and use cases and only nascent documentation of empirical risks posed. **A one-size-fits-all regulatory approach is therefore neither appropriate, nor in line with the human rights requirements of necessity and proportionality and the risk-based approach stipulated in the FATF Standards**. Targeted restrictions could apply but must be tailored to the specific risk of the specific virtual asset, crowdfunding, or other technology implicated, as well as the specific consumer or user at hand.

Endnotes

[1] See, e.g., A/73/361; A/74/335.
[2] See, e.g., FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Oct. 2021); CTED, Tech Sessions: Highlights on 'Threats and Opportunities related to New Payment Technologies and Fundraising Methods,' https://www.un.org/securitycouncil/ctc/news/cted%E2%80%99s-tech-sessions-highlights-%E2%80%9Cthreats-and-opportunities-related-new-payment-technologies-0.
[3] But see, e.g., ECNL, The Potential and Risks of Using Digital Technologies in Fundraising: A Comparative Research (Mar. 2021) [hereinafter ECNL, Potential and Risks].
[4] SRCT&HR, The Human Rights and Rule of Law Implications of Countering the Financing of Terrorism Measures (June 2022) [hereinafter "CFT Position Paper"].
[5] The FATF definition of VA explicitly excludes digital representation of fiat currencies, securities and other assets that are covered elsewhere in the FATF standards.
[6] CTED Fact Sheet, Counter-Terrorism in Cyberspace, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_cted_factsheet_ct_in_cyberspace_oct_2021.pdf.
[7] See, e.g., Ying Zhao et al., Crowdfunding Industry—History, Development, Policies, and Potential Issues, Journal of Public Affairs (2019), p. 2.
[8] IMF, Elements of Effective Policies for Crypto Assets, Policy Paper No. 2023/004 (Feb. 2023), p. 6 ("There are yet no globally consistent definitions and classification or taxonomy of crypto assets.").
[9] Blockchain is a secure public ledger system of financial transactions maintained by certain types of decentralised virtual currencies that are open-source and peer-to-peer. See UNODC, Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies (2014).
[10] See IMF, Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations, FinTech Notes No. 2021/002 (Oct. 2021), p. 1 [hereinafter IMF, Virtual Assets] (noting that since Bitcoin was launched in 2009, thousands of cryptocurrencies have been issued).
[11] See, e.g., Aditya Narain & Marina Moretti, Regulating Crypto, Finance & Development (Sept. 2022), p. 18; see also IMF, Elements of Effective Policies for Crypto Assets, Policy Paper No. 2023/004 (Feb. 2023), pp. 11-17 (recognizing the concerns digital assets raise with respect to consumer and investor protection and market integrity, in addition to money laundering and terrorist financing).
[12] ECNL, Potential and Risks, p. 4.
[13] Id. (citing as examples WWF and UNICEF).
[14] See UNSGSA et al., Igniting SDG Progress through Digital Financial Inclusion (Feb. 2023).
[15] See Global Center on Cooperative Security, Understanding Bank De-Risking and Its Effects on Financial Inclusion (Nov. 2015).
[16] See, e.g., WFP, GSMA and UN World Food Programme Accelerate the Use of Mobile Financial Services for Humanitarian Assistance (Aug. 7, 2020).
[17] See generally UNSGSA et al., Igniting SDG Progress through Digital Financial Inclusion (Feb. 2023).
[18] Id., p. 7.
[19] See, e.g., Chainalysis in Action: Department of Justice Announces Takedown of Two Terrorism Financing Campaigns with Help from Blockchain Analysis, Chainalysis (Aug. 13, 2020) (identifying two crypto schemes used by al-Qaeda and Hamas); see also CTED, Thematic Summary Assessment of Gaps in Implementing Key Countering the Financing of Terrorism Provisions of Security Council Resolutions (Dec. 2022), p. 16 ("Terrorists are also known to have abused mobile payment systems, virtual assets (including bitcoins, lesser-known cryptocurrencies, and privacy coins), and online exchanges and wallets.").
[20] See, e.g., IMF, Virtual Assets, p. 3 (finding that the "exact extent of misuse of [virtual assets] around the globe is unclear" and "so far appears to be smaller in volume and frequency than misuse of traditional financial service"); RUSI & Project Craaft, Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks (Apr. 2022) ("[N]ew financial technologies have indeed been used in the procurement and financing of attacks, but only with certainty in a small proportion of cases.").
[21] See, e.g., IMF, Virtual Assets, p. 3 n. 15; but see U.S. Department of Treasury, 2022 National Terrorist Financing Risk Assessment (Feb. 2022).
[22] See RUSI & Project Craaft, Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks (Apr. 2022), pp. 1-2.
[23] CFT Position Paper, p. 19.
[24] See A/HRC/40/52 (2019).
[25] A/HRC/41/41, para. 25.
[26] ECNL, Potential and Risks, p. 13 (explaining how "blockchain not only provides the prospect of more donations and greater speed but also the advantage of safe and censorship-resistant donations").
[27] See, e.g., Council of Europe, The Impact of Blockchains for Human Rights, Democracy, and the Rule of Law (2002), p. 6; Joel Khalili, In Ukraine, Crypto Finds a Purpose, Wired (Mar. 15, 2023); Ana Nicenko, Millions in crypto donations pour for Turkey and Syria earthquake relief, Finbold (Feb. 23, 2023); Roger Huang, Dissidents are Turning to Cryptocurrency as Protests Mount around the World, Forbes, (Oct. 19, 2020); International Crisis Group, Crowdfunding a War: The Money behind Myanmar's Resistance (2022).

[28] Council of Europe, The Impact of Blockchains for Human Rights, Democracy, and the Rule of Law (2002), p. 17. Blockchain technology has also been proposed to facilitate secured voting platforms and other democratic functions. Id
[29] A/HRC/41/41, para. 24.
[30] A/HRC/29/32, para. 12.
[31] See Global Center on Cooperative Security, Understanding Bank De-Risking and Its Effects on Financial Inclusion (Nov. 2015).
[32] See A/74/335.
[33] S/RES/2462 (2019), para. 19(d).
[34] Delhi Declaration (Oct. 2022), paras. 21-25.
[35] Seventh GCTS Review, A/75/L.105 (2021), OP57.
[36] FATF Recommendation 15, interpretative note. See FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (2022), p. 5. FATF guidance further calls on States to require virtual asset service providers to conduct customer due diligence for transactions over USD/EUR 1,000 and to obtain, hold and transmit certain originator and beneficiary information regarding virtual asset transfers—otherwise known as the "Travel Rule." Id.
[37] S/RES/2462 (2019), para. 21.
[38] See CFT Position Paper, p. 9.
[39] See FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Providers (2021), p. 42, para. 118.
[40] Id., p. 5.
[41] CFT Position Paper, p. 10.
[42] S/RES/2462 (2019), para. 6; see also Delhi Declaration (Oct. 2022), para. 14; CFT Position Paper, pp. 3-9.
[43] Among others, the UN Office of Counter-Terrorism has offered programming on crypto and terrorism financing risks in Bosnia and Herzegovina, Morocco, and Russia and UN Office of Drugs and Crime has organized trainings on money laundering and terrorist financing risks of virtual asset in Fiji, Thailand, and Egypt. See UNOCT, May 2022 workshop in Bosnia and Herzegovina, December 2021 Conference in Morocco, and September 2021 Regional Conference on Financial Investigations related to Crypto-Crimes in Russia; UNODC, July 2022 training in Fiji, 2017 training in Thailand, and 2017 training in Egypt.
[44] IMF, Elements of Effective Policies for Crypto Assets, Policy Paper No. 2023/004 (Feb. 2023), p. 5; see also FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Providers (2021), pp. 89-102.
[45] See, e.g. Gary Weinstein, Blockchain Privacy Is at Risk in the EU, CoinDesk (Feb. 9, 2023); Marta Belcher & Aaron Mackey, The U.S. Government Is Targeting Cryptocurrency to Expand the Reach of Its Financial Surveillance, Electronic Frontier Foundation (Dec. 21, 2020).
[46] RUSI & Project Craaft, Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks (Apr. 2022), p. 26.
[47] FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (2022).
[48] ECNL, Potential and Risks, p. 26.
[49] See Hong Kong Public Consultation on Regulation of Crowdfunding Activities, para. 1.14 (citing the United Kingdom, United States, Australia, and Singapore as States that have created a regulatory body for registering crowdfunding activities); ECNL, Potential and Risks, p. 24 (also citing France, Finland, Spain, and Morocco); see also RUSI & Project Craaft, Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks (Apr. 2022), pp. 28-29.
[50]See, e.g., Amnesty International, Turkey: Terrorism Financing Law has Immediate 'Chilling Effect' on Civil Society (2021); Myrna El Fakhry Tuttle & Linda McKay-Panos, Canada's Extraordinary Use of the Emergencies Act Poses Human Rights Concerns (Apr. 2022).
[51] See RUSI & Project Craaft, Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks (Apr. 2022), pp. 30-32.
[52] See Fintrail, https://fintrail.com/ffe.
[53] CFT Position Paper, pp. 3-9.
[54] OHCHR, Guiding Principles on Business and Human Rights, HR/PUB/11/04 (2011).
[55] See CFT Position Paper, p. 16, Snapshot of UN Special Procedures Communications on National Legislation or Regulations; see also CTED, Thematic Summary Assessment of Gaps in Implementing Key Countering the Financing of Terrorism Provisions of Security Council Resolutions (Dec. 2021), p. 22 ("Many States also continue to face challenges with respect to the integration of human rights obligations into CFT measures and cooperation with civil society actors in developing policies to ensure risk-based supervision of the non-profit sector.").
[56] See, e.g., CFT Position Paper, pp. 18-19, 26.
[57] UDHR, art. 12; ICCPR, art. 17; see Special Rapporteur on the right to privacy, International Standards, https://www.ohchr.org/en/special-procedures/sr-privacy/international-standards.
[58] See, e.g., EU General Data Protection Regulation; see also, e.g., OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data; Asia-Pacific Economic Cooperation Privacy Framework; Organization of American States Principles on Privacy and Personal Data Protection.
[59] A/HRC/27/37, para. 28; see also CFT Position Paper, pp. 24-25 (noting how the use and disclosure of personal data must be narrowly tailored and subject to procedural safeguards).
[60] Council of Europe, The Impact of Blockchains for Human Rights, Democracy, and the Rule of Law (2002), p. 33.
[61] ECNL, Good Practices in Digital Fundraising (2021).
[62] UDHR, arts. 19, 21, 22; ICCPR, arts. 19, 20.
[63] Council of Europe, The Impact of Blockchains for Human Rights, Democracy, and the Rule of Law (2002), Appendix, p. 43.

[64] International Financial Obligations, Digital Systems and Human Rights, Call for Inputs to the report of the Independent Expert to the Human Rights Council, 52nd session.
[65] A/HRC/50/23.
[66] See FATF, High-Level Synopsis of the Stocktake of the Unintended Consequences (Oct. 2021); see also CFT Position Paper, p. 16, Snapshot of UN Special Procedures Communications on National Legislation or Regulations.
[67] See, e.g., European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Apr. 2023).
[68] A/HRC/23/39, para. 23.
[69] FATF, Best Practices on Combating the Abuse of Non-Profit Organizations (Recommendation 8), p. 15.
[70] See, e.g., WFP, GSMA and UN World Food Programme Accelerate the Use of Mobile Financial Services for Humanitarian Assistance (Aug. 7, 2020).
[71] See CFT Position Paper, pp. 13-14.
[72] See, e.g., id., pp. 18-19.
[73] FATF, High-Level Synopsis of the Stocktake of the Unintended Consequences (Oct. 2021), p. 6.
[74] Council of Europe, The Impact of Blockchains for Human Rights, Democracy, and the Rule of Law (2002), Appendix, p. 42.
[75] UDHR, art. 10; ICCPR, art. 14.
[76] A/HRC/41/35, para. 50(c).
[77] CCPR/C/IT/CO/6, para. 36; see also ICCPR, art. 14.
[78] UNODC, Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies (June 2014), p. 97.
[79] UDHR, art. 7; ICCPR, arts. 26, 27; see also CERD.
[80] See ECNL, Potential and Risks, p. 16.
[81] Id., p. 26.
[82] See CFT Position Paper, pp. 37-39.