27 November 2023, Brussels

Joint submission of the civil society coalition:

Tools to prevent abuse of FATF anti-money laundering/financing of terrorism rules and address transnational repression

- **Germany, as one of the founding members of the Financial Action Task Force (FATF), creates standards for global financial policy to comply with anti-money laundering/countering the financing of terrorism (AML/CFT) rules;**
- **FATF Recommendations lead to non-governmental organisations (NGOs) and non-profit organisations (NPOs) to be defined as high-risk organisations by financial institutions, thereby by default opening the door for abuses for the authoritarian states. Submission presents cases when fully implemented FATF recommendations has led to financial exclusion and penalization of NGO;**
- **As the European Union gets closer to adopting stronger anti-money laundering/financing of terrorism (AML/CFT) and cryptocurrency regulations, the interests of ordinary people and NGOs are hardly taken into account;**
- **Bitcoin and stablecoins have provided pro-democracy activists with an important tool to avoid two main problems: de-banking and autocratic governments' control over financial institutions as result of abuse of the FATF recommendations;**
- **The practice of so-called 'de-risking' has been adopted by financial institutions worldwide in order to comply with the strict recommendations of the FATF on AML/CFT laws. De-risking leads, among other consequences, to banks terminating business relations with individuals and organisations targeted by smear campaigns or politically motivated legal assistance requests. This has proven to be a simple yet powerful tool of transnational repression for authoritarian governments and other illiberal regimes aiming to paralyse the activities of their opponents – even in the very heart of the EU;**
- **One of the consequences of this abuse is the financial exclusion and undue deprivation of property (freezing of assets). Moreover, transnational legal assistance frameworks allow malicious governments to access sensitive information, including banking data. As FATF revises Recommendation 8 in connection with abuse of CFT laws against NGOs, and European legislators draft the revised AML/CFT rulebook in order to expand the scope of the existing regulatory framework and to close existing loopholes, it is essential that these efforts should not infringe upon the rights of law-abiding customers, including those seeking refuge from or opposing authoritarian regimes;**

- Abuse of FATF recommendations is possible due to the fast-paced and closed legislative process within the FATF, which lacks broad participation from civil society and industry representatives needed to address unintended consequences.

The risks of a zero-risk approach: how FATF's AML compliance financially excludes civil society

Banks and other financial institutions (including cryptocurrency exchanges) are required to adhere to *"fit and proper"* standards when following FATF's recommendations and adopted on their basis regulations globally, often applying a zero-risk approach to new clients. However, *"propriety"* is a loosely defined term. To assess the risk level of a customer, these institutions use automated systems that examine an individual or an organisation's online media coverage.

This process presents an opportunity for an illiberal government to completely expel a civil society organisation from the banking system, not only domestically but also at an international level. The only requirement is to generate negative coverage across different media outlets in several languages, prompting financial institutions to flag and refuse a customer. As a result, politically-exposed organisations or individuals can become victims of the so-called **false positives** in AML compliance, which disproportionately affects low-profit customers *(*Annex *2).*

Financial institutions prioritise customers based on their value, with ordinary individuals having relatively low value and nonprofits having an even lower value. When automated systems, such as Refinitiv or services offered by Dun & Bradstreet, detect negative coverage, the most likely result is the rejection of a potential customer's application or termination of the existing relationship. This decision is made irrespective of whether the negative coverage is part of an orchestrated smear campaign, as financial institutions tend to take a zero-risk approach, even at the expense of organisations that work for democracy and the benefit of people in need, such as providing humanitarian aid.

The situation can become more drastic when an autocratic government, exerting full control over its law enforcement agencies, fabricates politically motivated criminal charges against its opponents, perverting, at the end of the day, the European justice system. When a Western bank receives a formal request for information from a law enforcement or judicial body of a country in which it operates, which itself received the request from a third country, it raises a red flag automatically in relation to the person or entity in question. This situation can have significant consequences, including an account closure or the rejection of the customer's application, further harming civil society organisations and politically-exposed individuals.

Clearly, such investigations tend to create sensational news, which further increases the number of negative results indexed by search engines and business intelligence firms. Regime propaganda eagerly exploits this. The news is quickly transmitted to banks, auditors, and even real estate companies or landlords, allowing subservient propagandists and prosecutors of illiberal regimes to hurt those who are affected.

Therefore, corruption is not the only method (as in the case of MEP Eva Kaili and Qatar) that can be effectively employed in the service of malign foreign actors to expand their influence within Europe, this situation with misuse of AML/CFT regulations creates a mockery of the principle of mutual trust between states. Once again, the West is played by its enemies, often with the assistance of leading law and advisory firms.

The practice of illiberal regimes excluding their opponents from the financial system currently suffers from a lack of public awareness, which further exacerbates the abuse of legal cooperation mechanisms. ODF became a victim of the misuse of FATF recommendations, which resulted in negative consequences for ODF's AML bank compliance. This occurred due to politically motivated public attacks and abuse of mutual legal requests, including mechanisms of the Schengen Information System, by the illiberal regimes that also tried obtaining banking data of the organisation and associates. As a result of the misuse of AML compliance, ODF and associates became considered high-risk clients by banks and subsequently faced financial exclusion and account closures.

The FATF recommendations are drafted with an accusatory bias for NPOs/NGOs. However, there is no substantiated statistical data to support this practice. Moreover, this approach is consistent with the rhetoric of authoritarian and undemocratic states, which inherently categorise and treat NGOs as entities that not only create threats to national security but are also involved in money laundering and terrorist financing. This further reduces civic spaces.

ODF's experience with de-risking

For over a decade, ODF has been exposing numerous instances of EU, bilateral, and international legal cooperation mechanisms enabling transnational repression. Since 2017, ODF has been subjected to significant abuse of inter-state mechanisms. In 2017, ODF took a stand in defence of the rule of law in Poland, which was met with a legal harassment and disinformation campaigns conducted by the Law and Justice government alongside the Kazakhstani and then-Moldovan regimes that ODF had criticised. Moreover, the Law and Justice government orchestrated numerous attempts at shutting down or paralysing ODF by organising smear campaigns against the foundation in Poland and within international institutions, including the European Parliament, the Parliamentary Assembly of the Council of Europe, and the OSCE Parliamentary Assembly.

ODF has been successful in nearly all court disputes with the Polish authorities, including several libel cases. Although some proceedings launched by ODF against the authorities are still pending, all allegations against the organisation have been proven false. Despite ODF's successes in court, raising a compliance red flag is much easier than removing it. Unfortunately, a persistently damaged reputation can take years to heal, and the current legal framework does not offer any remedies to restore the bank accounts of the NGO and its associates whose accounts have been closed in Belgium.[1] Based on its own experiences, ODF understands the need to raise public awareness regarding the practice of cutting opponents of illiberal regimes from the financial system.

Crypto-assets as a bank of last resort: the role of Bitcoin and stablecoins in supporting civil society amid financial repression

In May 2023, a G7 Finance Ministers and Central Bank Governors Meeting announced in its communiqué[2] about the need for the "effective monitoring, regulation and oversight are critical to addressing financial stability and integrity risks posed by crypto-asset activities and markets, while

[1] https://www.politico.eu/newsletter/eu-confidential/politico-eu-confidential-tv-star-to-run-slovenia-banned-from-schengen-summer-time-feedback-overload/

[2] https://www.consilium.europa.eu/media/64307/g7-communique-20230513.pdf

supporting responsible innovation." The G7 manifested its commitment to implement an “effective regulatory and supervisory frameworks for crypto-asset activities and markets as well as stablecoin arrangements, which are consistent with the FSB’s recommendations and standards and guidance established by SSBs.” While the G7 presented crypto-assets as "a financial stability and integrity risk," it has yet to address the growing problem of financial exclusion and the abuse of AML/CFT laws for transnational repression against activists and opponents. They also have not acknowledged how peer-to-peer transactions and Bitcoin self-hosted wallets have become the only tool available for human rights activists in illiberal countries.

The problem of authoritarian governments exerting control over financial institutions is evident: assets are at risk of being seized at any time, jeopardising the survival of NGOs. Additionally, this situation enables security and fiscal services to exploit FATF recommendations to monitor the funding sources of watchdog organisations, providing authorities with information that can be used to intimidate and persecute these NGOs politically.

In countries such as Russia,[3] Turkey,[4] Kazakhstan,[5,6] and Belarus,[7] human rights defenders, activists, and families of political prisoners can face severe consequences for receiving even the smallest amounts of money from abroad. These include potential charges of extremism, terrorism, or money laundering,

In countries such as Venezuela, Afghanistan,[8] Russia, and Belarus, where the economy is collapsing, the opposition has found ways to help people pay for basic necessities outside of official channels through Bitcoin and stablecoins, thus avoiding government surveillance.

In Palestine, rampant corruption forces people out of official banks to protect their hard-earned savings, while banking data is used to target the opposition.[9,10] Meanwhile, the Iranian Islamic Republic plans to use street cameras to track women and block their bank accounts for refusing to wear the hijab.[11]

A significant example of de-risking relates to the situation with Ukrainian and pro-Ukrainian NGOs and volunteer initiatives that fundraise to provide humanitarian aid to soldiers and refugees. In February 2022, following the Russian attack on Ukraine, the Ukrainian society and the state encountered two critical challenges that the traditional banking system could not adequately address.

First, banks and other financial institutions were temporarily paralysed, causing payments from and to Ukraine to be delayed or get stuck *"in transit"* for several weeks. This was a critical time when life-saving equipment, drones, and other supplies were urgently needed. Second, crowdfunding platforms' accounts and bank accounts of organisations supporting Ukraine financially and through in-kind donations were massively suspended. GoFundMe, Patreon, Wise (formerly TransferWise), and regular banks closed the accounts of numerous organisations around the world, often without explanation or

[3] https://www.reuters.com/article/us-russia-politics-navalny/russia-freezes-bank-accounts-linked-to-opposition-politician-navalny-idUSKCN1UY1ER
[4] https://stockholmcf.org/erdogans-long-arm-deutsche-bank-closes-accounts-of-erdogan-opponents-without-giving-any-reason/
[5] https://www.hrw.org/news/2021/07/07/kazakhstan-crackdown-government-critics
[6] https://en.odfoundation.eu/a/32928,oppositionist-therefore-extremist/
[7] https://www.theguardian.com/world/2020/nov/13/belarus-tells-banks-seize-money-raised-help-protesters-lukashenko
[8] https://bitcoinmagazine.com/culture/bitcoin-financial-freedom-in-afghanistan
[9] https://www.haaretz.com/2015-06-23/ty-article/former-pm-of-palestine-accused-of-money-laundering/0000017f-e3ec-d7b2-a77f-e3efbc930000
[10] https://pace.coe.int/en/files/31623/html
[11] https://www.iranintl.com/en/202212067151

citing internal rules that exclude transactions associated with *"armaments, military goods, and services."*[12,13]

In each of the aforementioned situations, crypto assets have served as a bank of last resort for those who otherwise would have been unable to protect their funds or make money transfers. This has allowed many to keep their savings safe from the hands of corrupt governments, local dictators, and political police. Privacy and ease of use have been crucial in making cryptocurrencies viable tools for civil society, enabling NGOs to continue providing crucial support.

We do believe it is a crucial time to address this issue and are grateful to Members of the parliaments across the Council of Europe and the OSCE region for considering our recommendations:

- In January 2023, 29 members of the Parliamentary Assembly of the Council of Europe (PACE), representing 14 countries, submitted a motion for resolution concerning the misuse of legal cooperation and AML/CFT laws.[14] The motion called to ensure protection against both transnational crime and the protection of privacy and human rights. Notably, this was the first time that European legislators acknowledged the role of crypto assets, such as Bitcoin and stablecoins, as tools for facilitating the work of civil society initiatives and the delivery of humanitarian aid.
- During the June session in 2023, the PACE discussed and adopted a resolution, which stressed the "*misuse on politically motivated grounds of interstate legal co-operation mechanisms such as anti-money laundering and anti-terror financing measures may result in violations of the right to a fair trial (…) This may in turn lead to financial exclusion of targeted individuals and NGOs and effectively prevent them from conducting their human rights activities and participating in economic and social life."*[15]
- In July 2023, the Parliamentary Assembly of the Organisation for Security and Cooperation in Europe (OSCE PA) adopted our amendment to the so-called Vancouver Declaration, which calls its 57 member states to "*ensure that Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) mechanisms are not used as tools of transnational repression to stifle dissent or target human rights defenders, anti-corruption campaigners, exiled dissidents, and diaspora communities, taking into account the potential unintended consequences of prevention-focused AML/CFT regulations and their side effects, including the potential for increased financial exclusion and further malicious exploitation of strict AML/CFT and related provisions, and further urges them to reflect in relevant regulations the use of crypto-assets, such as bitcoin and stablecoins, to defend human rights and to provide humanitarian aid.*" Furthermore, we greatly appreciate the adoption by the Members of the OSCE PA a Resolution specifically on the role of national parliaments in enhancing the participation of civil society in parliamentary and decision-making processes.[16]
- In October 2023, members of the PACE submitted a motion for resolution acknowledging the concerns raised by the United Nations Special Rapporteur on counter-terrorism and human rights, Fionnuala Ní Aoláin. She stressed that 69 % of relevant Human Rights Committee recommendations focused on the abuse of counter-terrorism surveillance practices against civil society, as well as the need to define transnational repression and analyse/reflect in the relevant regulation what role bitcoin and stablecoins play in that case.[17]

[12] https://ain.ua/2022/08/09/wise-zablokuvav-rahunky-fondiv-yaki-dopomagaly-ukrayini/
[13] https://vctr.media/ua/ne-takyj-j-idealnyj-chomu-ukrayinczi-vzhe-skarzhatsya-na-paypal-132476/
[14] https://pace.coe.int/en/files/31622/html
[15] https://pace.coe.int/en/files/32999/html
[16] https://www.oscepa.org/en/documents/annual-sessions/2023-vancouver/declaration-29/4744-vancouver-declaration-eng/file
[17] https://pace.coe.int/en/files/33081/html

- The recent public consultation on the FATF Best Practice Paper to Combat the Abuse of NPOs faced significant challenges. Despite being conducted in a tight timeframe, it took years to start public consultation discussions about FATF's recommendations' negative consequences.[18] This situation highlights the need for NGOs to be provided with more time and resources to address regulatory issues that significantly impact their operations and existence. Moreover, the consultation should not be limited to addressing only terrorism financing (TF) abuses but should also encompass concerns related to money laundering (ML) abuse. The AML/CFT legal frameworks are usually based on the same legislative foundations, and the issues related to AML are often more prevalent than those related to TF. Therefore, the entire study and its specific recommendations should comprehensively cover both TF and ML concerns.

We hope that an open dialogue between civil society and German regulators on how FATF recommendations and transnational legal cooperation can be enhanced will ensure protection against transnational crime while safeguarding privacy and human rights. Furthermore, it should be reflected in relevant regulations how peer-to-peer transactions and Bitcoin self-hosted wallets have become the only tool available to human rights activists in illiberal countries.

Voices of civil society: testimonies from around the world

Full texts of the testimonies are available in Annex 1 to this Paper.

(1) **Testimonial of Jaroslav Likhachevsky (Belarus, currently resides in the Netherlands), co-founder of the New Belarus platform and Bysol Foundation, director of the AI company Deepdee from Belarus:** "There are two serious problems with banks in the EU Member States for the Belarusians in exile: (1) they face difficulties opening/holding accounts in the EU and CoE Member States, and (2) they cannot use the banking system to deliver financial support to activists in Belarus due to the danger and ineffectiveness of the traditional bank transfers to authoritarian regimes. Ales Bialiatski, a current political prisoner in Belarus and 2022 Nobel Prize recipient, was arrested under tax evasion charges in 2011. The Belarusian regime has abused FATF recommendations on AML/CFT preventive measures to gain access to financial records from Lithuania and Poland as evidence. Now, regimes like Belarus use FATF recommendations on AML allegations as a pretext to collect financial information from Western democracies.[19] Therefore, the team has developed a safe and secure solution to provide financial support for local activists and organisations using crypto assets, which also allows them to build their own institutions and services in parallel. The team uses Bitcoin and stablecoins to deliver humanitarian aid to Belarus and support pro-democratic and anti-Russian activists on the ground. The team's future plans include building Digital Belarus, as a prototype for the future Belarusian Democratic state, with democratic institutions, including taxation and representation, using crypto assets like Bitcoin and stablecoins to maintain privacy and security, and to ensure they are not de-platformed or de-banked due to the upcoming Anti-Money Laundering regulation. In parallel, the Ministry of Interior of Belarus announced the development of a regulation to ban cryptocurrency peer-to-peer transactions between individuals, allegedly to combat criminal transactions.[20]

On 29 August 2023, Alexander Lukashenko signed a decree on measures to counteract unauthorised payment transactions that should give law enforcement agencies of Belarus unorganised access to

[18] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/FATF-BPP-Combat-Abuse-NPOs-Public-Consultation.html
[19] https://news.zerkalo.io/economics/47760.html?c
[20] https://t.me/police_minsk/12242

the financial information of Belarusian residents. This law will become another tool for political repressions in Belarus."

(2) **Testimonial of Anna Chekhovich, financial director of Alexei Navalny's Anti-Corruption Foundation (FBK) (Russia, currently resides in Lithuania):** "The Anti-Corruption Foundation (ACF), founded by Alexei Navalny, has been collecting donations in cryptocurrency since 2016 due to the unsafe nature of collecting only fiat donations, with the Russian banking system being fully controlled by the regime. Since the ACF's recognition as an extremist organisation in 2021, the organisation was forced to leave Russia, and most have moved to EU countries, where they registered legal entities to continue their activities. However, the founders of the Future Russia Foundation, formerly the ACF, have been facing problems in opening a simple bank account due to banks' AML compliance, and their bank accounts get closed without any explanation. Western banks treat Russians in exile as potential money launderers, and their transactions are often treated as suspicious. This leads to living without bank accounts which is impossible in the modern world. At some point, humanitarian aid was only possible through cryptocurrency, but European banks refused to conduct transactions related to cryptocurrency, making it impossible to buy cryptocurrency directly from the fund's accounts. Paysera payment system closed the organisation's account after attempting to buy BTC.

Now the EU has banned all crypto transactions with Russia within the framework of new sanctions against Russia, making it absolutely impossible for the foundation to financially support activists who are fighting the regime while in Russia. These new restrictions will not play a significant role in the fight against sanctions circumvention, but will cause enormous damage to the activities of activists and human rights organisations working with Russia. It will not stop Russian corrupt officials, but it will have a significant impact on the Russian opposition movement, and the founders of the Future Russia Foundation call for a solution that will not hinder humanitarian aid and will not put recipients of funds in Russia at risk."

(3) **Testimonial of Ismail Mesut Sezgin, Turkish opposition political commentator and research assistant at Regent's Park College, and self-employed business (Turkey, currently resides/citizen of the UK):** The case of transnational repressions in Turkey shows how authoritarian regimes can abuse international institutions and regulations to destroy lives of those who speak up against them, even if they are in the EU and other democracies. Mesut Sezgin, who wrote his Ph.D. at Leed Beckett University on the Hizmet Movement, spoke publicly and published YouTube videos about the failed coup attempt in Turkey. His Twitter and YouTube accounts were blocked by Turkish authorities, and Patreon account was also blocked in Turkey. In 2021, Mesut Sezgin was enlisted as a member of *"Fethullahist Terrorist Organisation"* by the Turkish government, causing financial assets to be frozen and seized internationally without due process. The financial blacklist caused problems, destroying his financial situation and business. Even in the UK, financial institutions started treating him as if he were a terrorist.

This situation is not unique, as people in Turkey designated as *"terrorists"* and blacklisted cannot send or receive money from or to their families and friends in Turkey. Even providing financial support can be used as evidence of being a member of a terrorist organisation, and some people in Turkey have been banned from banking. This creates a dire situation for families of political prisoners and blacklisted activists, as any financial support from European countries or other democracies is impossible. The western financial institutions following broad wording of the recommendations of FATF on AML/CFT preventive measures also treat them as terrorists, smugglers, and money launderers.

(4) **Testimony of Jorge Jraissati (Venezuelan, currently residing in Spain), Director of Alumni for Liberty, an international network of young freedom activists with over 10,000 members from 139 countries:** "Authoritarian regimes and illiberal governments have been weaponizing the international banking system as a tool for domestic and transnational repression. In response to this development, our activists have turned Bitcoin into their "bank of last resort." Our organisation has used Bitcoin to finance its activities in over fifty countries, and we currently pay 29 staff members through this cryptocurrency. In autocratic countries, our activists have reported that their bank accounts were either closed or weaponized. We have also documented cases of activists in exile who have been deprived of the right to have financial services, as they are targeted with disinformation campaigns and fabricated criminal allegations, which trigger de-risking mechanisms in bank compliance. This means that requirements originally established to adhere to AML/CFT laws are harming human rights defenders even at the very heart of the European Union. Similarly, several transnational legal assistance frameworks are allowing malicious governments to access sensitive information of their opponents abroad (including their banking data), jeopardising their safety. For these reasons, regulators and civil society have to work together to build mechanisms to prevent the unintended consequences of FATF standards and instruments to protect the financial rights of all law-abiding citizens."

(5) **Testimonial of Fadi Elsalameen, a prominent critic of corruption in the Palestinian Authority's government led by Mahmoud Abbas), an adjunct senior fellow at the American Security Project and the Bitcoin Policy Institute in the US (Palestine, currently U.S. citizen):** Fadi Elsalameen, who has been exposing human rights violations and corruption in Palestine for over a decade, presents on two issues: (1) how the Palestinian Authority's complete control over the banking system has been weaponized to harass dissidents and anyone who exposes abuse of humanitarian aid or financial assistance, and (2) how Bitcoin has become a solution to protect activists against corrupt regimes and connects communities in Israel and Palestine through Bitcoin transactions. Elsalameen personally experienced the Palestinian Authority's abuse of anti-money laundering regulations and anti-terrorism laws when his accounts were frozen by Bank of Palestine in 2021, which then leaked his personal information to a newspaper owned by the terrorist organisation Hezbollah. The leak was intended to incite violent attacks against him, which later led to Palestinian security forces shooting at his house with live bullets in March 2021.

The European Parliament's latest resolution on Palestine calls for transparent elections, an end to repression of dissent, and accountability for human rights violations. Civil society in Palestine has welcomed this resolution, but is still facing the high cost of corruption under the regime of Mahmoud Abbas. The European Union and Council of Europe must take action in the following ways: (1) exclude the Palestinian Interior Ministry and security services from European Union financial assistance until effective measures are taken to stop torture, hold those responsible accountable, and release political prisoners; (2) ensure that AML/CFT regulations are not abused by the PA to harass dissidents; and (3) prevent the abuse of AML/CFT regulations through mutual legal assistance to silence opponents abroad.

(6) **Testimonial of Obi Nwosu, former CEO of a regulated Bitcoin exchange Coinfloor (UK, Portugal):** "While KYC procedures and risk-based approaches are necessary to prevent money laundering and terrorist financing, they can inadvertently lead to de-banking and de-platforming of high-risk customers. The *"travel rule"* developed by FATF recommendations requires sharing of customer information, which can be used by dictatorial regimes to target recipients of funds. The *"tipping off"* rule prevents financial institutions from disclosing the reasoning behind their risk-based approach rules to their customers, due to concerns of money laundering and terrorist financing. However, this can lead to unintended consequences for individuals who are targeted with false information or adverse media, particularly those living under dictatorships and authoritarian regimes. These

individuals may be off-boarded or de-platformed without explanation, leaving them with no recourse. The *"fitness and propriety"* standards can lead to a risk-averse culture, and discrepancies in anti-money laundering and terrorist financing rules are often not spoken about due to fear of regulators. Financial institutions are facing a complex challenge when it comes to providing services to members of civil society, activists, human rights defenders, and NGOs, as they are often considered high-risk customers. In some cases, these requirements can result in one being de-banked or de-platformed, leaving them no other option but to turn to cryptocurrencies such asBitcoin and stablecoins. Therefore, two provisions should be put in place: (1) enabling members of civil society to seek recourse if they have been de-banked or de-platformed and (2) allowing them to use services like Bitcoin and stablecoins without being de-platformed or de-banked purely because they use these services.``

(7) **Testimonial of Jesús González, a computer engineer and representative of the Venezuelan opposition (Venezuela, currently resides in Spain):** Jesús González has been opposing the dictatorship of Chavez and Maduro for over 15 years and has been a member of the Interim Government of Venezuela since 2019. The opposition aimed to use the frozen Venezuelan funds in the US to provide financial aid to activists, opposition members, and social programs in Venezuela. With the help of the US government, they successfully implemented a program called "Heroes de la Salud" in 2020 during the pandemic. The program converted designated US funds into stablecoins and transferred them to over 68,000 health workers in Venezuela through a direct and secure platform to avoid reprisals of Maduro's regime. The program was replicated with frozen funds and digital platforms for all areas of the Interim Government, allowing them to continue operating without putting their personal security at risk. The mechanism helps overcome obstacles imposed by the authoritarian state-controlled financial system. However, human rights defenders and opposition members, like Leopoldo López, well-known pro-democracy activist and Sakharov prize laureate, face bank compliance problems in the EU, with many of their colleagues unable to even open a bank account due to banks de-risking and closing their accounts or freezing their payments following broad wording of the FATF recommendations on AML/CFT preventive measures.

(8) **Testimonial of Bota Jardemalie, a licensed attorney in the State of New York and a human rights defender (Kazakhstan, political asylum in Belgium):** Bota Jardemalie was granted political asylum in Belgium due to the extraordinary risks she faced in the form of reprisals by Kazakhstan against her for her legal work against the regime. The Council of Bars and Law Societies of Europe (CCBE) recognises Jardemalie as "lawyer in danger."

Despite Jardemalie's political asylum, she remained in danger even in Belgium. At Kazakhstan's request, in 2013 INTERPOL published a Red Notice to arrest Jardemalie on fabricated charges of alleged embezzlement of BTA Bank in Kazakhstan, that was later INTERPOL cancelled this Red Notice for non-compliance with the rules against political abuses of INTERPOL. Kazakhstan's regime twice tried to extradite Jardemalie from Belgium unsuccessfully, with false AML allegations. Belgium refused those extradition requests.

After their attempts at extraditing Jardemalie and physically harassing her failed, in 2016, a proxy for the Kazakhstani regime, BTA Bank, filed a criminal complaint against Jardemalie in Belgium, accusing her of money laundering on Belgium soil. The Chamber du Conseil of the Tribunal of the First Instance of Brussels dismissed the criminal investigation against Jardemalie and ordered the complainer to pay Jardemalie €15000 in procedural compensation and €5000 more, *ex aequo et bono*, as compensation for the temerarious and vexatious procedure. This case is an example of SLAPP - Strategic Lawsuit Against Public Participation, another tool of transnational repression, with abuse of AML laws.

In parallel, Jardemalie has been a target of a very aggressive smear PR campaign in 5 languages online, sponsored by the Kazakh regime. As a result of negative PR, she started experiencing problems with banking: banks in Belgium closed her bank accounts without any explanation, considering as a high-risk client, and refused to open her a bank account. She also was blocked from making Western Union transfers. She fell victim to the misuse of AML bank compliance as a result of politically motivated public attacks, and subsequently faced financial exclusion and account closures.

(9) **Testimonial of Roya Mahboub, a serial entrepreneur and one of the first female CEOs in her home country, Afghanistan (Afghanistan, currently residing in the US)**: "Bitcoin allowed the organisation to overcome physical and social obstacles in paying Afghan women. With a simple transaction, Bitcoin could instantly appear in a woman's digital wallet, without interference from men. My team has trained over 17,000 young women in coding, digital skills, and entrepreneurship, and has built dozens of internet classrooms and mobile computer labs across Afghanistan. We tried to develop practical skills and foster self-reliance among women, breaking down traditional cultural barriers that limit them to domestic duties.
Since August 2021, bank and wire services like Western Union, MoneyGram have run out of paper currency and have cut off services, leaving one-third of Afghans struggling with food insecurity and 50-70% with unstable housing situations. Websites like GoFundMe have been blocked from fundraising efforts for "compliance" reasons. Bitcoin has provided a crucial financial lifeline for many during these difficult times, who stay in the country and continue working behind closed doors."

(10) **Testimonial of Suba Churchill, executive director of the Kenya National Civil Society Centre and chairperson of the Horn of Africa Civil Society Forum (Kenya):** "I am a member of Kenya's Universal Peer Review (UPR) process, and I can at best describe the National Risk Assessment on Money Laundering and Terrorism Financing for Kenya as a farce. First, the entire process in my view, has always been shrouded in unnecessary secrecy, and is approached by the concerned Kenyan authorities as (1) an investigation into an already established crime (2) in which the Not-for-Profit sector is presumed guilty until proven innocent despite the country's constitutional provision of presumption of innocence until one is proved guilty by a court of competent jurisdiction Second, consultation of NPOs has been done remotely, and without their knowledge of what one is being drawn into. I can testify on my own and other NGOs' experience that Kenya's state security agencies are engaged in harassment of non-governmental organisations but claim that this was consultation on FATF standards."

(11) **Testimonial of Tetiana Pechonchyk, head of the Board of the Human Rights Center ZMINA, (Ukraine):** "In Ukraine, the implementation of the FATF Recommendations negatively affects the operations of the NGOs and has led to financial exclusion of NGOs. For example, in November-December 2021, banks blocked the accounts of two reputable Ukrainian civil society organisations - the Institute of Mass Information and the Civil Network OPORA.[21] However, two months later, the full-scale invasion of Ukraine by the Russian Federation began, and the requirement to submit the ultimate beneficial owners for civil society organisations was postponed until the end of martial law in the country. In other words, the problem was postponed but not solved, as this trend will resume after the war ends. In addition, inspections can be applied during martial law to those NGOs that have managed to submit their ultimate beneficial owners data.

The regulatory measures introduced in Ukraine, ostensibly aimed at preventing money laundering and terrorist financing, have inadvertently led to unnecessary overregulation and operational impediments for NGOs. While the intention to align with international standards and protect against financial crimes is commendable, the hurried and unclear implementation of these regulations has

[21] https://zmina.info/articles/chomu-banky-blokuyut-rahunky-gromadskyh-organizaczij-i-chy-mozhna-z-czym-shhos-zrobyty/

created significant challenges. The lack of precise definitions for ultimate beneficial owner (UBOs) in NGOs and the absence of accessible guidance and practical submission options have hindered compliance efforts, rendering it virtually impossible for many entities.

The postponement of deadlines and ongoing debate over the Methodology for determining UBOs underscore the flaws in the regulatory framework. These issues, compounded by the impact of external events such as the Russian invasion, further demonstrate the need for a more balanced and effective approach to AML/CFT regulations that genuinely serves their intended purpose without causing undue burdens on civil society organisations.

Our key recommendation to FATF is to involve civil society in the regulatory process to avoid such consequences and financial exclusion. We advocate that NGOs should be removed from the list of entities obliged to report UBOs, both in the Law and in the Methodology. Should NGOs remain on the list, a proper communication mechanism must be established among the National Bank of Ukraine, banks, and NGOs to prevent blocking of banking services for NGOs."

Recommendations

In the ongoing EU legislative process, including adoption of the 6th Anti-Money Laundering Directive,[22] regulations aimed at combating money laundering and terrorist financing,[23] and the establishment of a new EU AML/CFT supervisory authority, [24] the trilogue phase is currently underway. This phase involves discussions among representatives of the European Parliament, the Council of the European Union, and the European Commission. Simultaneously, the FATF is conducting plenary and working group meetings to update the global approach to regulation, encompassing both traditional financial industries and cryptocurrencies. It is important to address the existing deficiencies during this period:

1) It is important to prioritise the interests of bank clients, including ordinary people, small and medium enterprises (SMEs), as well as individuals and NGOs that are subject to politically motivated attacks. Currently, many of them face difficulties due to increased bureaucracy in the financial services and ever-increasing diligence requirements, which can result in a prolonged process of opening a bank account and negatively affect their ongoing relations with financial institutions.

2) The currently proposed EU regulation does not adequately define the term *"false positive,"* which has become a well-known issue in AML/CFT compliance, when a financial institution's automated systems process flags a client or transaction as suspicious, shutting down the payment or locking down an account completely, incorrectly identifying as criminal or illicit. The regulation also appears to overlook the natural inclination of financial institutions to continually decrease risk by becoming increasingly selective in accepting new clients, thus exacerbating the risk of financial exclusion. Additionally, there are no provisions for remedies related to false positives.

3) While the proposed regulations based on FATF recommendations aim to combat money laundering, their focus on prevention may have unintended consequences. The new procedures and restrictions could potentially lead to increased financial exclusion, without sufficient consideration of their side-effects.

[22] https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-6th-directive-on-amlcft-(amld6)
[23] https://data.consilium.europa.eu/doc/document/ST-15517-2022-INIT/en/pdf
[24] https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733645/EPRS_BRI(2022)733645_EN.pdf

It is crucial to establish provisions that enable members of civil society to seek recourse if they have been de-banked or de-platformed, including the appointment of a third-party ombudsman to determine the reasons for the banks' actions and whether the person/NGO can be replatformed. This should be mandated by the government, as financial institutions have no financial incentive to do this on their own and every incentive - both financial and regulatory - not to.

4) While the Anti-money Laundering Authority (AMLA) is required to provide annual reports to the European Parliament, European Commission, and Council, there are no concrete mechanisms in place for holding the AMLA accountable for any potential misuse of its mandate.

5) Despite the potential impact on civil society and the FinTech and business communities, there has been limited consultation on the proposed regulations. Transparency International stands out as a notable exception. As a result, there is a lack of understanding of the potential threats of financial surveillance, privacy violations, arbitrary actions of law enforcement, and disclosure of sensitive information to authoritarian and other illiberal regimes under legal assistance mechanisms.

6) It is important to ensure that members of civil society are not unfairly targeted and excluded from financial services simply because they use tools like Bitcoin and stablecoins. These services may act as the only means of accessing financial services in situations where traditional banking options are not available, and it is crucial to prevent de-platforming or de-banking of individuals and organisations who rely on them.

7) There should be recourse options for those who have been de-banked or de-platformed to ensure accountability and prevent abuse of power by financial institutions, including due diligence companies. It is necessary to provide for such persons/organisations the possibility to bring effective legal action before the courts or other competent bodies in order to access, correct, delete or retrieve data, or to obtain, where relevant, compensation in connection with an alert relating to them.

8) There is noticeable lack of consideration of the proposed regulation’s impact on entrepreneurship and the business environment, including the FinTech sector, and the crypto industry, and, consequently, the EU's overall competitive position and influence on innovation in these areas of the market. A reliable analysis of the anticipated effects of the regulation should also focus on costs, including directly on the cost of compliance.

9) There is a pressing need to create formal and direct communication channels with FATF for NPOs. NPOs should have access to platforms and mechanisms where norms are established and assessed. They should also have the capability to report instances of significant misuse of FATF standards directly, even outside the regular country evaluation cycles. NPOs should be able to provide information about human rights abuses, as these are reliable indicators of potential misapplication of FATF standards. It is essential that NPOs gain access to FATF plenary sessions, similar to their access in other international organisations, like in the PA OSCE.

Germany and other relevant members and institutions that shape FATF policy approaches must consider all of these arguments when developing and passing much-needed upcoming regulations. It is also essential to remember that the most effective way to counter the abuses of autocratic regimes is to work together with those opposing these regimes.