

**Joint submission of the civil society coalition regarding
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 and terrorist financing**

Can the EU's anti-money laundering reform help dictators?

- As the European Union gets closer to adopting stronger anti-money laundering/financing of terrorism (AML/CFT) and cryptocurrency regulations, 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;
- The practice of the so-called de-risking was established to comply with strict AML/CFT laws. It leads banks to terminate contracts with individuals and organisations targeted with 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 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 European legislators draft the revised AML/CFT rulebook in order to enlarge the scope of the existing regulatory framework and to close existing loopholes, they should not harm the rights of law-abiding customers, including those fleeing from or fighting authoritarianism.

The risks of a zero-risk approach: how AML compliance hurts civil society

As banks and other financial institutions, including cryptocurrency exchanges, are required to be "*fit and proper*" when following regulations, new clients tend to be taken under a zero-risk approach. 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 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 in several languages for financial institutions to flag and refuse a customer. As an effect, 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 non-profits having 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 even more dire 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 account closure or 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 increase 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, not only corruption (as in the case of MEP Eva Kaili and Qatar) 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 assistance of leading law and advisory firms.

The phenomenon of illiberal regimes banishing opponents from the financial system currently suffers from the lack of public awareness, which further exacerbates the abuse of legal cooperation mechanisms. ODF fell victim to the misuse of AML bank compliance as a result of politically-motivated public attacks. As a result of de-risking, ODF became considered as a high-risk client by banks, and subsequently faced financial exclusion and account closures.

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 campaign, 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 a smear campaign against it 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, that 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

The issue with authoritarian governments controlling financial institutions stands apparent: assets are unsafe due to the risk of being seized at any time, which may lead to the starvation of an NGO. Additionally, it allows security and fiscal services 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 in Russia,² Turkey,³ Kazakhstan^{4, 5} and Belarus,⁶ human rights defenders, activists, and families of political prisoners can face severe consequences, including potential charges of extremism, terrorism, or money laundering, for receiving even the smallest amounts of money from abroad.

In countries such as Venezuela, Afghanistan,⁷ 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.

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.reuters.com/article/us-russia-politics-navalny/russia-freezes-bank-accounts-linked-to-opposition-politician-navalny-idUSKCN1UY1ER>

³ <https://stockholmcf.org/erdogans-long-arm-deutsche-bank-closes-accounts-of-erdogan-opponents-without-giving-any-reason/>

⁴ <https://www.hrw.org/news/2021/07/07/kazakhstan-crackdown-government-critics>

⁵ https://en.odfoundation.eu/a/32928_oppositionist-therefore-extremist/

⁶ <https://www.theguardian.com/world/2020/nov/13/belarus-tells-banks-seize-money-raised-help-protesters-lukashenko>

⁷ <https://bitcoinmagazine.com/culture/bitcoin-financial-freedom-in-afghanistan>

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.⁸⁹ Meanwhile, the Iranian Islamic Republic plans to use street cameras to track women and block their bank accounts for refusing to wear the hijab.¹⁰

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 citing internal rules that exclude transactions associated with *"armaments, military goods, and services"*.^{11,12}

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.

In January 2023, 29 members of the Parliamentary Assembly of the Council of Europe, representing 14 countries, submitted a motion for resolution concerning the misuse of legal cooperation and AML/CFT laws.¹³ 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.

Voices of civil society: testimonies from around the world

Full texts of the testimonies 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

8

<https://www.haaretz.com/2015-06-23/ty-article/former-pm-of-palestine-accused-of-money-laundering/0000017f-e3ec-d7b2-a77f-e3efbc930000>

⁹ <https://pace.coe.int/en/files/31623/html>

¹⁰ <https://www.iranintl.com/en/202212067151>

¹¹ <https://ain.ua/2022/08/09/wise-zablokuvav-rahunky-fondiv-yaki-dopomagaly-ukrayini/>

¹² <https://vctr.media/ua/ne-takyj-j-idealnyj-chomu-ukrayinczi-vzhe-skarzhatsya-na-paypal-132476/>

¹³ <https://pace.coe.int/en/files/31622/html>

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 used financial records from Lithuania and Poland as evidence. Now, regimes like Belarus use AML allegations as a pretext to collect financial information from Western democracies. 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.”

- (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 also treat them as terrorists, smugglers, and money launderers.

- (4) **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.

- (5) **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*" 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 being de-banked or de-platformed, leaving them no other option but to

turn to cryptocurrencies like Bitcoin 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.”

- (6) **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.
- (7) **Testimonial of Bota Jardemalie (Kazakhstan, political asylum in Belgium):** Bota Jardemalie, a Harvard Law graduate, is a licensed attorney in the State of New York and a human rights defender from Kazakhstan. For years, she had defended the Kazakh opposition, political activists, human rights defenders and victims of torture, advocates for human rights, democracy, and the fight against corruption. In 2013, 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. 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 misuse of AML mechanisms. Belgium refused those extradition requests.

She received a credible threat that she was in danger and was investigated for criminal conspiracy targeting her. 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 Federal prosecutor dismissed (*non-lieu*) the case (“*Il n’existe aucune charge contre Botagoz Jardemalie*”).

Kazakhstan made at least three mutual legal assistance requests to Belgium to receive all her banking information, all her electronic devices, and her professional legal files. She was falsely accused of money laundering by an agent of the Kazakhstani regime - BTA Bank. Two Belgian banks provided her banking information to the regime that persecuted her for years, without her knowledge or consent. In April 2018 the Minister of Justice of Belgium accepted one of the mutual legal assistance requests filed by Kazakhstan, without carrying out proper verification required under the law, failing to protect a refugee and to respect the rights of a lawyer and the legal profession. On 13 January 2022, the

Constitutional Court of Belgium in its judgement 1/2022¹⁴ upheld Jardemalie's position, ruling that, despite the absence of a right explicitly provided for by the law, the remedy should exist for someone in her position when the request for mutual legal assistance comes from a non-EU Member state, and it was necessary to provide her a right of appeal in Belgium in order to be able to challenge the legitimacy of the mutual assistance in criminal matters requested by Kazakhstan. (Constitutional Court, judgement 1/2022)

In parallel, for years, 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 and refused to open her a bank account. She also was blocked from making a Western Union transfers. Her case illustrates the abuse of international cooperation mechanisms and banking information by authoritarian regimes.

Recommendations

As the EU legislative process, including the 6th Anti-Money Laundering Directive,¹⁵ Regulation to fight money laundering and counter terrorist financing,¹⁶ Regulation establishing a new EU AML/CFT supervisory authority,¹⁷ is still ongoing and now entering the committee phase of the European Parliament (specifically the Economic and Monetary Affairs, Civil Liberties, Justice and Home Affairs committees), it is crucial to address the current shortcomings:

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 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.

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 re-platformed. This should be

¹⁴ <https://www.const-court.be/public/f/2022/2022-001f.pdf>

¹⁵ [https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-6th-directive-on-amlcft-\(amld6\)](https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-6th-directive-on-amlcft-(amld6))

¹⁶ <https://data.consilium.europa.eu/doc/document/ST-15517-2022-INIT/en/pdf>

¹⁷ [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733645/EPRS_BRI\(2022\)733645_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733645/EPRS_BRI(2022)733645_EN.pdf)

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.

The European Union must take into account all of these arguments when developing and passing much-needed upcoming regulation. 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 them.

We have included case studies on the misuse of AML/CFT laws and the beneficial role played by crypto assets in the appendix to this brief.