Open Dialogue Foundation
Brussels | Warsaw | Kyiv | Miami
HQ: Rond-point Schuman 6/5
1040 Brussels, Belgium

Brussels, 11 June 2025

SLAPP & Transnational Financial Repression across Belgium/EU and the United States:

The Case Against Lyudmyla Kozlovska and the Open Dialogue Foundation

In 2022, Kazakhstan's special services orchestrated a collective criminal complaint in Belgium against the Open Dialogue Foundation and its President, human rights activist Lyudmyla Kozlovska. The operatives, filing complaints on behalf of their minor children, accused the Foundation and its President in harassment, slander and cyberbullying, posed as victims, and demanded the removal of social media videos published by the Foundation that documented their involvement in political repression, torture and killings in Kazakhstan.

The Belgian court ultimately dismissed the proceedings against the Foundation and its President, ruling that Belgium lacked territorial jurisdiction over the alleged offences. Belgian court documents reveal that Kazakh authorities, using these operatives who posed as ordinary citizens while being active members of Kazakhstan's police and security services, sought extensive personal surveillance data on both the Foundation and Kozlovska across Belgium/EU and the United States, including:

1. Kozlovska's complete passport data and travel history, particularly her movements between Belgium and the U.S.
2. Details of her flights and border crossings at Belgian airports within the Schengen zone.
3. Comprehensive financial information, including:
    - Hotel bills from Miami and Washington,
    - Complete bank account transactions,
    - Funding sources for her travel and accommodation.
4. Private email correspondence between Kozlovska and the Foundation during her stays in Belgium and the USA.
5. Internal operational details of the Foundation, including how Kozlovska managed activities whilst travelling; and
6. Technical data from videos recorded by Kozlovska, including:
    - Raw media files, recordings and photographs,
    - Creation and publication dates,
    - Equipment ownership and funding details,
    - Names of technical staff. [Attachment 1]

The Belgian investigating judge explicitly stated that these requests appeared designed "to use Belgian justice to collect the maximum amount of personal and private data on Kozlovska for purposes other than simply revealing the truth in this case." [Attachment 2]

This case illustrates both two tactics of undermining rule of law and financial, cybersecurity integrity of Western countries:

1. **Strategic Lawsuit Against Public Participation (SLAPP) –** well known tactics of abusive litigation targeting journalists and rights defenders, based on Article 81(2)(f) of the Treaty on the

Functioning of the European Union and adopted so-called the anti-SLAPP directive (Directive (EU) 2024/1069).[1]

2. **Transnational Financial Repression –** new tactic, which means the deliberate misuse and manipulation of international financial regulatory frameworks by foreign governments or non-state actors, for the purposes of silencing, intimidating, surveillance or otherwise repressing individuals, organizations, or entities beyond their territorial jurisdiction. These regulatory frameworks, developed based on Financial Action Task Force (FATF) recommendations, include anti-money laundering (AML) laws, countering the financing of terrorism (CFT) regulations, cybersecurity laws, and mutual legal assistance treaties (MLATs). Forms of transnational financial repression include, but are not limited to, actions aimed at unjustified freezing or confiscation of assets, depriving access to financial services, exploitation of financial intelligence and personal data, dissemination of targeted misinformation to undermine an entity's economic reputation, and initiation of politically-motivated legal proceedings (SLAPP). This form of transnational repression violates the foundational principle of mutual trust inherent in international cooperation on AML/CFT regulations and other security treaties. It compromises fundamental human rights, national and economic security, financial integrity, and the rule of law of the EU and its allies.

Claude Monique, former intelligence officer of France and current head of the European Strategic Intelligence and Security Center (ESISC) [2] —a private intelligence and lobbying firm in Belgium—played a pivotal role in these proceedings. On 1 July 2022, Monique filed the criminal complaint against Kozlovska and the Open Dialogue Foundation, acting as legal representative for the Kazakhstani police officers and their children through a power of attorney from a Kazakhstani lawyer.

The case files show that Monique's involvement facilitated these extensive data collection requests. The legal actions coordinated by Monique were strategically designed to shield Kazakhstani security agents and law enforcement officials from international scrutiny regarding human rights abuses while simultaneously gathering intelligence on human rights defenders operating in Western democracies.

In the 13 December 2023 court decision, the Belgian investigating judge specifically noted that some investigative actions requested by the “victims” appeared intended to "instrumentalize Belgian justice" for purposes beyond establishing relevant facts. [Attachment 2]

It's worth noting that Monique's organization, ESISC, was previously investigated for alleged corruption within the Parliamentary Assembly of the Council of Europe (PACE) during 2017-2018 regarding illegal lobbying for Azerbaijan (the "caviar diplomacy" case). [3]

The case demonstrates a concerning pattern of abuse of the cybersecurity and AML/CFT framework, developed on the recommendations of the FATF, and the urgent need for reform:[4]

[1] https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-initiative-against-abusive-litigation-targeting-journalists-and-rights-defenders
[2] http://www.esisc.org/about-us/our-mission
[3] https://assembly.coe.int/Communication/IBAC/IBAC-GIAC-Report-EN.pdf
[4] https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

1. **Weaponization of Financial Transparency Requirements**: The Kazakhstan-linked parties attempted to use allegations loosely framed around suspicious financial activity to commit harassment, slander and cyberbullying as a pretext to demand extensive financial records. This represents a direct attempt to misuse the principles behind FATF Recommendations 10 (Customer Due Diligence) and 20 (Suspicious Transaction Reporting) for politically motivated surveillance rather than legitimate financial crime concerns.
2. **Abuse of Cross-Border Information Sharing Mechanisms**: The request for detailed banking records and transactional activities exploits the international cooperation mechanisms established under FATF Recommendations 37 and 40, which were designed for legitimate law enforcement purposes rather than targeting dissidents.
3. **Misappropriation of Counter-Terrorism Financing Framework**: The court documents show that standard financial control mechanisms designed to prevent terrorism financing were being repurposed to monitor human rights defenders, directly undermining the intended purpose of FATF Recommendation 6.
4. **Exploitation of Jurisdictional Gaps**: The attempt to use Belgian legal channels to access U.S. financial data reveals how authoritarian regimes exploit differences in national implementation of FATF standards to forum-shop for the most advantageous jurisdiction.
5. **Politically Exposed Person (PEP) Framework Inversion**: Rather than using enhanced due diligence to monitor corrupt officials (as intended), the case shows how the PEP framework can be inverted to allow those officials to target their critics at such jurisdictions as Belgium and U.S.

This case provides concrete evidence of how international financial and cybersecurity regulatory frameworks are being exploited. Rather than combating financial crime or cybercrime as intended, these systems are being misused to enable transnational financial repression and SLAPP tactics. This misuse undermines the very rule of law, national security, and financial integrity of Western countries these frameworks were designed to protect. It also demonstrates that once data requests enter the judicial system, privacy of Belgium/EU and the U.S. citizens, residents are already at risk.

Attachments:

1. *ORDINANCE Art. 61 quinquies C.I.Cr.* Complementary Investigative Acts - refusal by the Court of First Instance of Brussels to provide Kazakhstani secret services with requested personal, travel and financial data in Belgium and the U.S. – and its English translation.
2. Decision of the Court of First Instance of Brussels and its English translation.

For more information please contact:

Lyudmyla Kozlovska, President of the Open Dialogue Foundation
Email: lyudmylakozlovska@odfoundation.eu