11TH JUDICIAL REFORM PACKAGE – ARTICLE 128/A OF THE CPC: SCOPE OF APPLICATION AND LEGAL IMPLICATIONS

I. Regulation Introduced by the Legislative Proposal

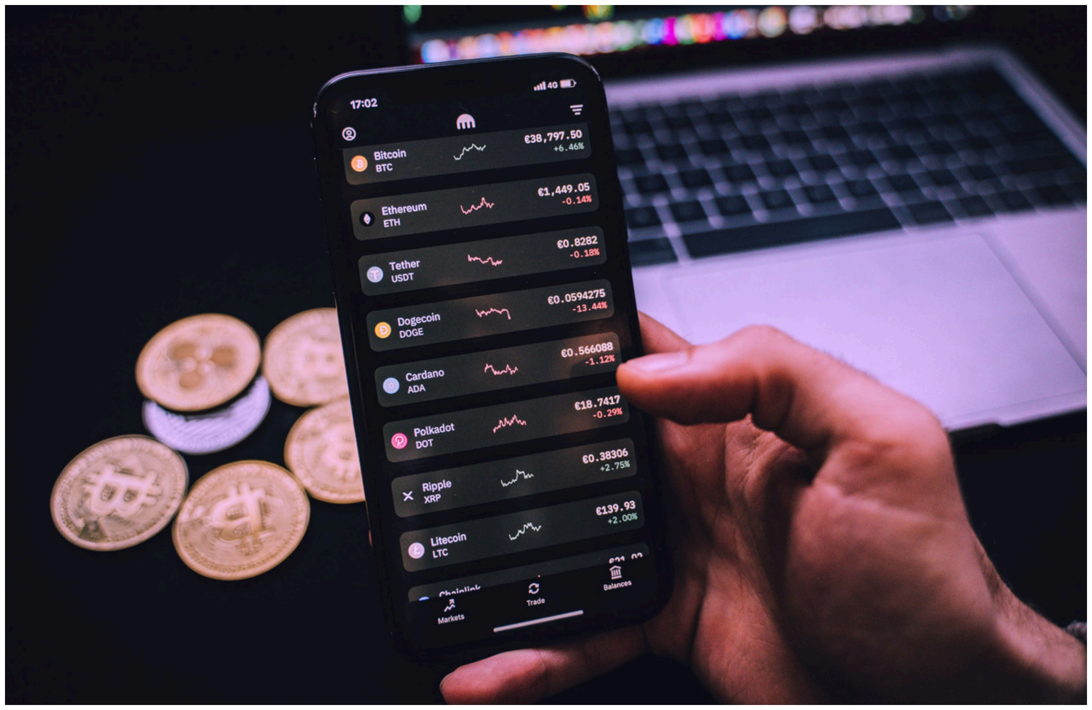
The legislative proposal submitted to the Grand National Assembly of Türkiye envisages the insertion of Article 128/A, titled "*Suspension and Seizure of Accounts to Prevent Proceeds Derived from Cybercrimes*", into the Code of Criminal Procedure No. 5271 (the "**CCP**"). Under this new provision, where there is reasonable suspicion that the offenses of aggravated theft, aggravated fraud, or the misuse of bank or credit cards, each defined under the Turkish Criminal Code No. 5237 (the "**TCC**"), have been committed, the relevant bank, payment service provider, or crypto-asset service provider may order the suspension, for up to forty-eight hours, of any account used in connection with the offense, including accounts held with or transactions conducted through such institutions, or attempted to be conducted through them. Following the suspension, the institution must immediately notify the Chief Public Prosecutor Office of the suspension measure and related account activities, together with all relevant information and documentation.

In addition, the suspension measure must also be notified to the account holder. The account holder may apply to the Chief Public Prosecutor Office for the lifting of the suspension, and the prosecutor is required to render a decision on such application within twenty-four hours. If it is determined that the proceeds of the offense were transferred to another financial institution before the suspension was executed, the legislative proposal requires that the relevant institution be notified without delay in order to implement the suspension measure.

The article further provides that, upon the written order of the public prosecutor, or upon the application of the relevant financial institution in cases where delay would be prejudicial, a seizure order may be issued with respect to the proceeds of crime contained in the suspended accounts. Any such seizure order must be submitted to the criminal judgeship of peace for approval within twenty-four hours; if the judge does not issue a decision within this period or rejects the seizure, the measure shall be deemed automatically lifted. Where it is established that the seized proceeds belong to the victim harmed by the offense, the proposal allows such proceeds to be returned directly to the victim during the investigation or prosecution phase.

II. Current Regulatory Framework

Under the current system, banks, payment institutions, and crypto-asset service providers are not granted any direct authority under the CCP to "suspend" accounts for the purpose of preventing proceeds derived from fraud or similar offenses committed through information systems.



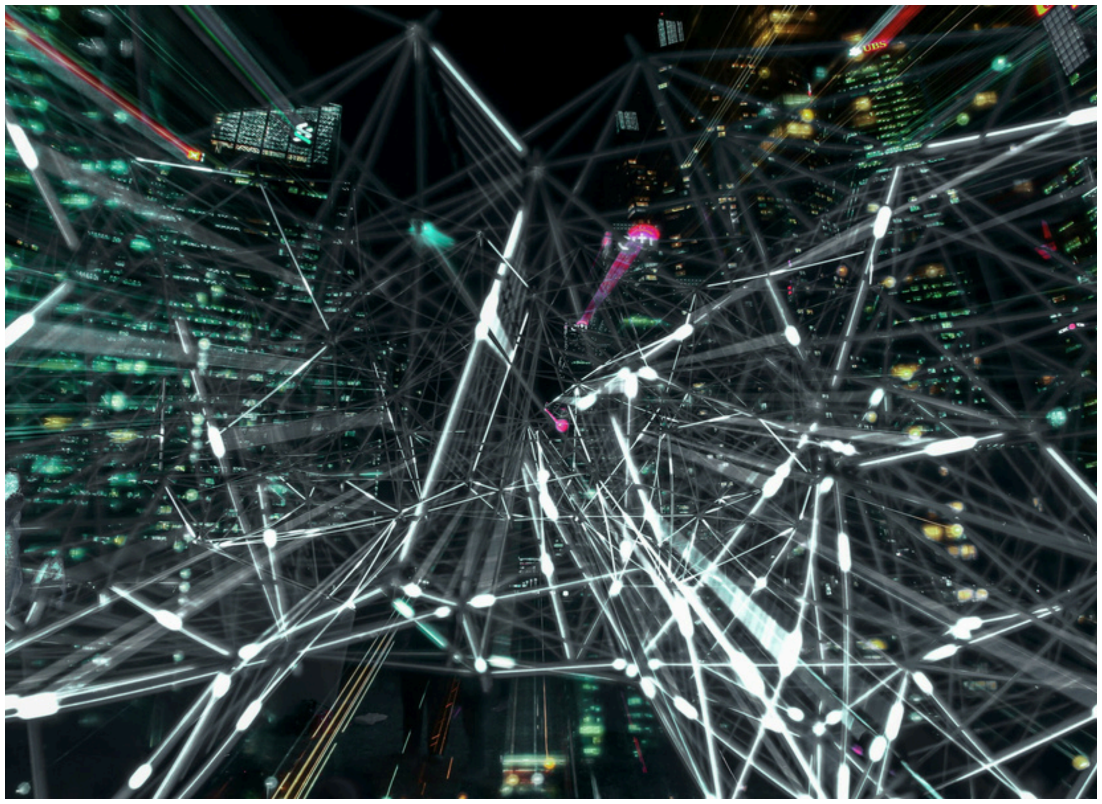
Interventions targeting funds or assets considered to constitute proceeds of crime are primarily carried out through the "seizure" measure under Article 128 of the CCP, which is imposed upon the request of the public prosecutor and by order of the criminal judgeship of peace. In this process, reviews and reports obtained from Financial Crimes Investigation Board (the "**FCIB**") and the Capital Markets Board (the "**CMB**") play a determinative role in establishing that the assets stem from criminal activity. However, in practice, the seizure mechanism often reacts too slowly in the context of digital transactions, which occur instantaneously and at high speed.

Additionally, under Article 19/A of Law No. 5549 on the Prevention of Laundering Proceeds of Crime, crypto-asset service providers, banks, and other financial institutions may file suspicious transaction reports with the FCIB. Where deemed necessary, FCIB may instruct the relevant financial institution to temporarily halt the transaction or to prevent its execution.

FCIB's transaction-suspension order is, as a rule, limited to seven business days, and may also be implemented on the basis of notifications received from foreign counterpart authorities in accordance with the principle of reciprocity. Financial institutions that act in violation of such instructions are subject to administrative fines.

III. Legal Analysis and Identified Issues

The proposed Article 128/A offers a significant advantage compared to the current framework by enabling rapid intervention within the first forty-eight hours. Nonetheless, the provision contains certain practical gaps. Unlike the FCIB-driven and administrative "transaction postponement" authority under the existing Article 19/A, the "account suspension" authority under Article 128/A would be exercised directly by banks, payment institutions, or crypto-asset service providers. However, the legislative proposal does not set out how these two mechanisms are to be coordinated. This issue must be clarified either during the legislative process or through secondary regulations; otherwise, parallel or conflicting instructions concerning the same transaction may arise.



Moreover, the proposal does not specify the objective criteria on which the "reasonable suspicion" threshold will be based. In situations where funds are rapidly transferred to another institution, the notification obligation under Article 128/A will only be effective if a real-time technical infrastructure is established between institutions. Therefore, although Article 128/A is theoretically designed to complement the existing regime, its practical effectiveness will depend on supportive secondary regulations.

In this context, crypto-asset service providers will need to update their internal policies and procedures to identify fraud patterns and reasonable-suspicion criteria specific to aggravated theft, aggravated fraud, and fraudulent use of bank or credit cards. They will also need to establish an almost 24/7 coordination line among their legal, compliance, and operations departments for notifications to prosecutors and other financial authorities, and adopt additional safeguards regarding technical infrastructure and data confidentiality.