ELİG
GÜRKAYNAK
Attorneys at Law

Overview of the Intersection Between Digital Regulations and White Collar Crimes

Authors: Dr. Gönenç Gürkaynak, Ceren Yıldız and Gamze Yalçın of ELIG Gürkaynak Attorneys-at-Law

Upon assessing the extent to which its laws, regulations and other legislation implement Financial Action Task Force's ("FATF") 40 Recommendations and 9 Special Recommendations ("**Recommendations**"), on July 20, 2023, FATF has published its second Follow-up Report and Technical Compliance Re-Rating for Turkiye ("**2023 FUR**") [1]. Since the publication of Mutual Evaluation Report ("**2019 MER**") on December 16, 2019 and the later publication of the first Follow-up Report on November 21, 2021 ("**2021 FUR**"), one particular area that Turkiye has been identified has been Recommendation 15, which is entitled the "*New Technologies*" section and effectively calls upon countries to identify risks associated with the development of new products and new business practices and the use of new or developing technologies for both new and pre-existing products. [2]

In the same vein, but on a different scale, attention of public has also been particularly drawn to the manner "new technologies" may be used to commit crimes and/or to conceal crimes that have already been committed, or to execute the commission of crimes with the appearance of legality.

This article provides an overview of where Turkiye stands in terms of the intersection between digital regulations and white collar crimes. The particular provisions of regulations on new technologies which have been included in the scope of this article are the laws and regulations related to electronic commerce, electronic payments and virtual assets sector. Particular provisions have been selected to the extent that such provisions' legislative intent may be considered as prevention of commission, concealing, and/or legitimizing white-collar crimes.

---

[1] For 2023 FUR, *see* https://www.fatf-gafi.org/en/countries/detail/Turkey.html (Last accessed on December 17, 2023). For amended FATF Recommendations, *also* https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf (Last accessed on December 17, 2023)

[2] For 2019 MER, *see https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual-Evaluation-Report-Turkey-2019.pdf.coredownload.inline.pdf* (Last accessed on December 17, 2023); for 2021 FUR, *see* https://www.fatf-gafi.org/content/dam/fatf-gafi/fur/Follow-Up-Report-Turkey-2021.pdf.coredownload.pdf (Last accessed on December 17, 2023)

- **What are the Regulated Cyber-Crimes? (Article 243 - 246 of the Turkish Criminal Code)**

Crimes committed through information technologies (hereinafter "Cyber-Crimes") are regulated under Section 10, between Article 243 – 246 of the Turkish Criminal Code with No. 5237 ("TCC"). In addition, certain provisions under TCC also refer to the "use of information technologies" in order to distinguish the manner of commission of certain crimes. As per TCC "Cyber-Crimes" are (i) accessing an information system; (ii) obstructing, disrupting, destroying or altering data; (iii) abusing bank or credit cards; (iv) prohibited devices and programmes.

- **Other crimes in the TCC that include references to "use of information technologies"**

TCC also refers to the "use of information technologies" as an aggravating and/or distinguishing factor for several other crimes. Namely, such crimes are (i) stalking (or "persistent tracking") ("Article 123/A"); (ii) aggravated theft (Article 142 (2) (e)); (iii) aggravated fraud (Article 158 (1) (f); (iv) providing a place and possibility for gambling (Article 228 (3)).

In Turkiye, traditional white-collar crimes, namely, bribery, bid-rigging, embezzlement, malversation, obtaining benefit for unauthorized business, abuse of duty, providing commercial benefits for public officials, and improper transactions on assets are regulated under disparate provisions of the TCC.

Therefore, a conclusion can be drawn that the TCC does not include any provisions that account for cyber-commission of white-collar crimes. Cyber-crimes and white-collar crimes are regulated separately under the TCC. Moreover, none of the white-collar crimes that are particularly regulated under TCC include any references to "*use of information technologies*."

- **Digital Regulations that Intersect with Commission of White-Collar Crimes**

Even though TCC has not integrated the use of cyber-technologies to the commission of white-collar crimes, Turkiye has made notable progress on its electronic commerce, electronic payments and virtual assets sector legislation to prevent laundering of proceeds of white-collar crimes.

To elaborate, Turkiye has amended several of its laws and secondary legislation to include provisions that introduce (i) persistent record-keeping and reporting obligations to obligated parties, (ii) advanced due diligence requirements for customers (i.e. additional "know-your-customer" checks), (iii) lowering thresholds for suspicious transactions reporting and including previously excluded sectors as obligated parties. The relevant provisions of these laws are briefly described below.

- **Law No. 6563 on Regulation of Electronic Commerce**

On July 7, 2022, Law No. 7416 on Amendment of the Law on Regulation of Electronic Commerce has introduced notable amendments to the Law No. 6563 on Regulation of Electronic Commerce ("**E-Commerce Law**") with respect to reporting obligations of e-commerce service providers and e-commerce intermediary service providers above certain thresholds of net transaction volumes. Besides, the amended E-Commerce Law has also introduced a new concept of "*economic integrity*", which introduces "arm's length" requirements for certain electronic commerce transactions.

For instance, e-commerce intermediary service providers whose net transaction volume in a calendar year exceed ten billion Turkish liras are required to submit continuous reports to Capital Markets Board with regards to its activities, management and organizational structure, as well as any discrepancies it detects to be in violation of laws, in accordance with the regulatory framework determined by the Ministry of Commerce. (Additional Article 2 (2) (e) of Law No. 6563).

E-commerce service providers and e-commerce intermediary service providers that act in violation of the reporting obligation to Ministry of Commerce per Additional Article (2) (2) (e) of Law No. 6563 will be subject to an administrative monetary fine of 1 Million Turkish Liras (for the year 2023). (Article 12 (p) of Law No. 6563).

Similarly, e-commerce intermediary service providers whose net transaction volume in a calendar year exceed thirty billion may not restrict the electronic commerce service provider's commercial relations, its provision of goods or services through alternative channels for the same or different prices or its advertising. Additionally, the said parties are also prohibited from forcing the electronic commerce service provider to procure goods or service from a specific person. (Additional Article 2 (3) (c) of Law No. 6563.)

E-commerce intermediary service providers that act in violation of the prohibition on enforcing the electronic commerce service provider to procure goods or service from a specific person will be subject to an administrative monetary fine of 250,000 Turkish Liras (for the year 2023). (Article 12 (s) of Law No. 6563.)

Additionally, e-commerce intermediary service providers whose net transaction volume in a calendar year exceed sixty billion are prohibited from conducting banking activities in their e-commerce marketplace except for certain payment services, and may not accept the electronic money that they issue and except for their own sales undertaken as e-commerce service provider, sales made on their marketplaces, sales out of the scope of e-commerce, e-commerce intermediary service providers may not engage in cargo, distribution operations, transportation organizing and post service provision. (Additional Article 4 (a) (1) of Law No. 6563.)

E-commerce intermediary service providers who engage in accepting electronic money payments and banking activities will be fined of 10 Million Turkish Liras, and be provided with a sixty-day period to remove the violation. If the violation is not removed within the given time period, higher administrative monetary fines, up to 40 Million Turkish Liras (for the year 2023) may be imposed. (Additional Article 12 (3).

- **Law No. 6493 on Payment and Security Systems, Payment Services and Electronic Money Institutions ("Law No. 6493")**

The Law No. 6493 mainly regulates scope of service, licensing regime and obligations of two basic service providers: payment institutions and electronic money institutions. Electronic money institutions act as intermediaries and they provide users services to create an e-money account wherein the amount of the e-money is equivalent to the fund paid in return and to use the account for purchasing goods and/or services from providers that accept the issued e-money. Whereas, payment institutons are described as legal persons authorized for providing "payment services", within the meaning of the Law No. 6493 (payment services are listed under Article 12 of the Law, in a *numerus clausus* manner).

Amendments to Law No. 6493 in 2019 has introduced reporting, record-keeping, and collaboration obligations to payment institutions and electronic money institutions.

In this scope, Central Bank of the Turkish Republic ("CBTR") is authorized to request records, information and documents from payment and electronic money institutions regarding any transactions that are conducted by institutions under its supervision where it deems necessary. (Article 21 of Law No. 6493). Moreover, principles and procedures that determine the rights and obligations of parties are determined by the CBTR, upon receiving the opinion of Financial Crimes Investigation Board ("**MASAK**") (Article 12 (3) and Article 14 (6) of Law No. 6493).

System operators, payment institutions, and electronic money institutions are required to keep records on their transactions for at least ten (10) years. The payment institution and electronic money institution may use such records to prevent payment irregularities by taking necessary precautions on personal data. (Article 23 of Law No. 6493.)

Individuals who hinder the audit and investigation duties of CBTR will be subject to imprisonment from one year up to three years. (Article 29 of Law No. 6493.) Individuals who refrain from providing information and documents requested by CBTR are subject to imprisonment from three months up to one year and up to one-thousand-and-five-hundred (1500) days of judicial monetary fines (therefore a minimum of 30, 000 Turkish Liras and a maximum of 150,000 Turkish Liras).

Investigation of this crime is subject to CBTR's application to the public prosecutor's office with a complaint. (Article 37 (1) of Law No. 6493.)

Other crimes that are also regulated under Law No. 6493 are providing in false statements (Article 30 of Law No. 6493), acting in violation of the obligation to preserve records and information security (Article 31 of Law No. 6493), divulging secrets (Article 32 of Law No. 6493), keeping off-the-record transactions and inaccurate accounting (Article 35 of Law No. 6493), embezzlement (Article 36 of Law No. 6493.) Investigation of commission of these crimes by personnel of the payment institution or electronic money institution is subject to CBTR's application to the public prosecutor's office with a complaint. (Article 37 (3) of Law No. 6493.)

Institutions that act in violation of the Law No. 6493 will imposed an administrative monetary fine from 491,720 Turkish Liras (for the year 2023) up to 11,063,700 Turkish Liras (for the year 2023). However, if an interest has been realized or a loss has been incurred, then the administrative monetary fine may be increased. (Article 27 of Law No. 6493.) Separately judicial monetary fines and imprisonment penalties are also foreseen for crimes such as embezzlement, providing false secrets, and divulging of secrets.

- **The Regulation Prohibiting the Use of Crypto Assets for Payments ("Crypto Regulation")**

According to several news sources, Turkish Grand National Assembly is expected to adopt a new regulation for crypto assets and crypto asset service providers. [3]

Currently, there is no comprehensive regulation for crypto-asset-service-providers ("CASP") except for obligations which have been stipulated under various different laws.

Primarily, CBRT has issued a Regulation which prohibits the use of crypto assets as payments for transactions, effective as of April 30, 2021. According to the Regulation, crypto asset is defined as "*all intangible assets that are digitally created with distributed ledger or similar technology and distributed over digital networks; but, are neither characterised as fiduciary (fiat) money, bank money, or electronic currency, nor as a payment, security, or other capital market instrument*." (Article 3 of the Regulation.)

The Regulation prohibits the direct and indirect use of crypto assets in (i) payments transactions, and (ii) the provision of payment services and electronic currency exports. The Regulation draws a broad

[3] See https://www.ntv.com.tr/turkiye/kripto-para-duzenlemesi-ne-zaman-cikacak-tbmm-gundemine-gelecek,8CEsg-Y9h0C5yV3z92RoqA (Last accessed on December 17, 2023)

context for payment transactions by also including those entities that provide payment services and export electronic currency. The Regulation prohibits these entities from providing or developing any service that pertains to such a business model. (Article 4 of the Regulation.) This definition distinguishes crypto assets from capital markets instruments, making them subject to a different legal regime.

In addition to the Regulation, the Presidential Decree No. 3941, as published in the Official Gazette of May 1st, 2021 has introduced CASPs as an obligated within the scope of Law No. 5549 on the Prevention of Laundering of the Proceeds of Crimes ("**Law No. 5549**). In this scope, by including CASPS under Law No. 5549, MASAK has been authorized to initiate *ex officio* investigations regarding CASPs to monitor their compliance with anti-money-laundering and terrorist financing requirements and may impose monetary sanctions on CASPs when it is detected that they fail to comply with such requirements.

In the context of CASPs becoming an "obligated party", the Financial Crimes Investigation Board has published the Guide on Main Principles Regarding the Prevention of Money Laundering and Financing of Terrorism for CASPs wherein due diligence on customers (i.e. "know-your-customer"), reporting suspicious transactions, and providing information and documents requirements have been emphasized.[4] The Guide requires CASPs to report suspicious transactions to the Financial Crimes Investigation Board within ten days of becoming aware of such at the latest, or immediately in the event of a non-delayable case.

Article Contact: Dr. Gönenç Gürkaynak E-mail: gonenc.gurkaynak@elig.com
(First published by Mondaq on December 22, 2023)

[4] See https://ms.hmb.gov.tr/uploads/sites/12/2022/04/KVHS-Rehberi-16.04.2022.pdf (Last accessed on December 17, 2023).