YAZICIOGLU LEGAL

Türkiye's New Legal Regime in Cybersecurity: The Cybersecurity Law

28 March 2025

Enacted nearly two months after its submission to the Parliament, the Cybersecurity Law (the "**Law**") was published in the Official Gazette on 19 March 2025, and has become effective upon publication. So, to whom does the Law apply? How does the Law affect the cyber ecosystem and what changes does it introduce to the existing framework? What are the provisions in the Law that particularly concern the private sector? We have summarized these, and other important issues regulated in the Law.

1. Wasn't There a Turkish Cybersecurity Law Before?

Cybersecurity has been an important part of Türkiye's policy landscape for many years. The Law is not the first nor the only legal regulation on cybersecurity in Türkiye.

For example, Presidential Decree No. 2019/12 dated 6 July 2019, along with the Information and Communication Security Guidelines, have mandated various cybersecurity measures. However, these regulations only apply to public institutions and organizations and businesses providing critical infrastructure services.

Although the Personal Data Protection Law ("**the DP Law**") has a broader scope and imposes an obligation on data controllers and data processors to ensure data security, the DP Law only establishes the legal framework for "personal data".

In addition, various sectoral regulations contain cybersecurity-related provisions, such as the By-Law on Banks' Information Systems and Electronic Banking Services. The Law provides the legal basis for a more general and comprehensive legal framework -described in its explanatory memorandum as an "umbrella legislation"- in this fragmented field.

It is worth noting that until the secondary regulations on the implementation of the Law are enacted, the existing regulations will remain in force to the extent that they align with the Law.

2. Who Is within the Scope of the Law?

It would not be an exaggeration to say that every individual or entity engaging in any digital network activity falls within the scope of the Law. Specifically, the Law applies to: "public institutions and organizations, professional organizations with public institution status, natural and legal persons, and organizations without legal personality **that exist, operate and provide services in cyberspace**".

The term "cyberspace" in this definition also is broadly defined as "the environment consisting of **all** information systems **directly or indirectly** connected to the internet, electronic communications or computer networks and the networks interconnecting them".

Only the activities covered by various national security laws are excluded from the scope of this Law (These laws being the Police Duties and Authorities Law, the Coast Guard Command Law, the Gendarmerie Organization Law, the National Intelligence Law, and the Turkish Armed Forces Internal Service Law).

3. The New Regime: Cybersecurity Directorate and Cybersecurity Board

Two days before the Law's proposal was submitted to the Parliament, the Presidential Decree on the Cybersecurity Directorate ("**Decree**") was published in the Official Gazette, establishing the Cybersecurity Directorate ("**Directorate**"). The Decree transferred the duties of the Digital Transformation Office, which was an organization under the Presidency and has been abolished as of today, to the newly established Directorate. It also defined some of the duties and powers of the Directorate. These powers and duties consisted of determining cybersecurity strategies and conducting various activities, such as raising awareness.

The Law goes further by transferring the powers of the Information and Communication Technologies Authority (**"ICTA**") regarding the detection and prevention of cyber-attacks and the regulatory powers of the Ministry of Transport and Infrastructure regarding cybersecurity to the Directorate, thus making the Directorate the main institution authorized in the field of cybersecurity.

A Cybersecurity Board ("**Board**") is established as well, which will be chaired by the President. The Board's role is more strategic, focusing on setting road maps, policies, action plans and making decisions on regulatory matters.

The Law not only consolidates the cybersecurity-related duties and authorities of existing institutions under the Directorate, but also assigns the Directorate with a wide mission, including the protection of critical systems, detection, prevention and response to cyber-attacks, and development and implementation of domestic and national cybersecurity solutions.

It also assigns the Directorate certain powers and duties regarding response activities during and after cyber incidents. Thus, it is expected to take an active role in combating cyber-attacks and increasing cyber resilience.

The most important power granted to the Directorate by the Law is "to conduct cybersecurity audits and impose sanctions according to the results" and its details are explained below.

4. The Auditing Power of the Directorate

The Law grants the Directorate a very extensive power to audit. Accordingly, the Directorate has the authority to audit all activities that fall within the scope of the Law. As noted above, since the Law covers almost every organization operating in cyberspace, it will not be false to say that the Directorate can audit almost any activity of any person and institution related to information networks.

As part of the audit process, the Directorate is empowered to conduct on-site inspections. The auditors are authorized to examine electronic data, documents, electronic infrastructure, devices, systems, software and hardware; obtain copies, digital copies or samples; request written or oral explanations on the subject; issue the necessary records of the audit; and examine the facilities and their operation. In this regard, this auditing power compares to that of the Turkish Competition Authority.

The Directorate is also authorized to search and seize the residences, workplaces, and indoor spaces that are not open to the public and make copies (of documents) in this context. However, these powers may only be exercised for "national security, public order, prevention of crime or cyber-attacks" purposes, and a judge's decision or, in urgent cases, a written order from a public prosecutor must be obtained beforehand.

5. Obligations and Sanctions

In line with the powers of the Directorate, the Law provides various obligations for persons and institutions using information systems. They are as follows:

- **Data Submission**: All data, documents, hardware, software, or any contributions requested by the Directorate in scope of its duties and operations must be submitted thereto. Non-compliance or prevention of compliance with this obligation can result in **1 to 3 years of imprisonment and a judicial fine between TRY 50,000 and TRY 750,000.**

- **Cooperation During Audits**: Organizations must make their systems and equipment available, provide the necessary infrastructure, and ensure its proper functioning for the audits. Failure to comply is subject to an **administrative fine between TRY 100,000 and TRY 1,000,000**. For commercial companies, this can reach **up to 5% of the gross sales revenue reported in the annual financial statements audited**, which may not be less than 100,000 TRY.

- **Compliance with Cybersecurity Measures**: Non-compliance with the provisions that require implementing cybersecurity measures is subject to an administrative fine between **TRY 1,000,000 and TRY 10,000,000**.

- **Incident Reporting**: Any detected vulnerabilities or cyber incidents must be reported to the Directorate without delay. Failure may result in an administrative fine between **TRY 1,000,000 to 10,000,000**.

- **Procurement Restrictions**: Cybersecurity products, systems, and services used in public institutions and critical infrastructures must be procured from experts, producers, or companies certified by the Directorate. Non-compliance with this obligation is also subject to an administrative fine of **TRY 1,000,000 and TRY 10,000,000**.

An additional obligation is to comply with regulatory actions issued by the Directorate to enhance cybersecurity maturity; however, the Law does not include specific sanctions for those who fail to fulfill this obligation.

Finally, it should be noted that the Law also includes specific obligations and sanctions for cybersecurity companies and the personnel of the Directorate.

6. And Other Criminal Provisions...

In addition to the sanctions mentioned above, the Law introduces several new cybercrimes. They include the following:

- Launching cyberattacks targeting the elements constituting the national power of Türkiye in cyberspace or storing any data in cyberspace obtained as a result of such attacks **(imprisonment from eight to twelve years**, unless the act constitutes another crime with a heavier penalty)

- Dissemination, sharing or putting up for sale of the data obtained as a result of a cyber-attack against the elements constituting the national power of Türkiye in cyberspace (**imprisonment from ten to fifteen years**)

- Unauthorized access, sharing, or sale of leaked personal data or institutional data belonging to critical public services (**imprisonment from three to five years**)

- Creating or disseminating **false** content about a data breach related to cybersecurity **in order to cause anxiety, fear and panic among the public or with the purpose of targeting institutions or individuals**, even though there is no actual data breach **(imprisonment from two to five years**)

The last-mentioned offense caused many debates in the public and media during the discussion of the Law's proposal, since it was defined very broadly in the initial version thereof. However, during the relevant committee's discussions, the scope was limited to content creation and dissemination activities and with the specific intent of "causing anxiety, fear and panic among the public or targeting institutions or individuals". The provision was accepted in the Parliament's General Assembly as such.

7. Conclusion

Cybersecurity is not a new concept in Turkish law. However, there was no general cybersecurity legislation due to the fragmented nature of the existing regulations on the subject and the presence of multiple regulatory authorities. Previous action plans and various strategy documents stated introduction of "a framework legislation" as a policy aim; yet, so far, the biggest step in this direction seems to be the establishment of the Directorate and the introduction of the Law.

In our opinion, in order to achieve the goals in the field of cybersecurity, legislative arrangements will not suffice; rather, their implementation will be decisive.

Although the Law is centered on national security and therefore seems to mostly affect public institutions and organizations; given the obligations and sanctions stipulated in the Law and the powers of the Directorate, the private sector may reasonably expect to be significantly affected as well.

For now, a transition period seems to be in place; since the Directorate has not become operational and no secondary regulation has been introduced yet. The scope and impact of the new cybersecurity law -who it will affect and how- will depend heavily on the details outlined in the upcoming secondary regulations and, more importantly, on the Directorate's approach. We will continue to keep you informed on these developments.

Bora Yazıcıoğlu
bora@yazicioglulegal.com

Aslı Rabia Savaş
asli@yazicioglulegal.com

Ferat Gümüş
ferat@yazicioglulegal.com