MARIF

Disputes **October 1, 2025**

Publication

Cybersecurity Law No. 7545

The Cybersecurity Law No. 7545 ***("Law")*** entered into force upon its publication in the Official Gazette No. 32846 on 19 March 2025 specifically governing this field for the very first time under Turkish law. The Law aims to identify threats directed at all components of Turkey's cyberspace, protect institutions, organizations, and individuals from cyberattacks, and to establish national cybersecurity strategies. The fundamental principles underlying the Law include cybersecurity as an inseparable part of national security, institutionalization, sustainability, promotion of domestic and national solutions, stakeholder responsibility, rule of law, protection of privacy, and respect for fundamental rights.

1. Who Is Covered by the Law?

The Law extends to public institutions and organizations, professional bodies with public institution status, natural and legal persons, as well as entities without legal personality that operate, provide services, or otherwise maintain a presence in cyberspace. Conversely, activities conducted under the Police Duties and Powers Law, the Coast Guard Command Law, the Gendarmerie Organization, Duties and Powers Law, the State Intelligence Services and National Intelligence Organization Law, and the Turkish Armed Forces Internal Service Law are excluded from the scope of the Law.

2. Duties and Powers of the Cybersecurity Presidency

The Law sets forth the duties and powers of the Cybersecurity Presidency ***("Presidency").***

2.1. Duties

- **Ensuring Cyber Resilience:** Protecting critical infrastructures and information systems, detecting, preventing, and mitigating cyberattacks; conducting risk analyses and threat intelligence activities.
- **Identification of Critical Infrastructures:** Preparing inventories of public institutions and critical infrastructures, determining and implementing security measures according to the level of importance of assets.

- **Cyber Security Incident Response Team (CSIRT) Management:**Establishing, supervising, and enhancing the maturity levels of CSIRTs, as well as ensuring international coordination.
- **National Solutions and Infrastructures:** Developing domestic and national security tools and establishing or ensuring the establishment of necessary security infrastructures.
- **Standards and Certification:** Preparing standards for software, hardware, products, and services; carrying out testing and certification processes; providing certification for experts and companies.
- **Supervision and Regulation:** Defining procedures and principles to be followed by actors in the field of cybersecurity; supervising public institutions and critical infrastructures.
- **International Cooperation:** Coordinating with foreign countries and international organizations, sharing information, and representing Turkey in the field of cybersecurity.

2.2. Powers

- **Taking Precautionary Measures:** Ensuring the implementation of necessary measures against cyberattacks.
- **Incident Response:** Intervening in cyber incidents on-site or remotely, documenting them, and submitting findings to judicial authorities.
- **Requests for Information and Data:** Requesting and assessing information, documents, data, and log records from relevant institutions and organizations.
- **Supervisory Authority:** Conducting cybersecurity audits and authorizing or revoking the authorization of independent auditors.

3. Duties of the Cybersecurity Board

With the enactment of the Law, the Cybersecurity Board ***("Board")*** has been established. The Board is composed of the President, the Vice President, the Head of the Cybersecurity Presidency, several ministers, and heads of public institutions. The main duties of the Board are defined as follows:

- **Policy and Strategy:** Adopting decisions on policies, strategies, action plans, and regulatory measures concerning cybersecurity; exempting certain institutions and organizations from such decisions where necessary.
- **Technology Roadmap:** Adopting decisions on the nationwide implementation of the technology roadmap prepared by the Presidency.
- **Incentives and Human Resources:** Identifying priority areas to be incentivized in the field of cybersecurity and deciding on measures to enhance human resources.
- **Critical Infrastructures:** Identifying critical infrastructure sectors nationwide.
- **Dispute Resolution:** Resolving disputes that arise between the Presidency and public institutions.

4. Duties and Responsibilities of Service Providers and Data Processors

The Law regulates the duties and responsibilities of entities that provide services, collect, or process data through information systems. These duties and responsibilities are listed as follows:

- **Provision of Information and Documents:** Submitting data, documents, hardware, and software requested by the Presidency in a timely manner.
- **Precaution and Notification:** Taking necessary measures for national security and public service, and promptly reporting identified vulnerabilities or cyber incidents.
- **Authorized Procurement:** Procuring products and services to be used in critical infrastructures only from sources authorized by the Presidency.
- **Operational Approval:** Obtaining approval from the Presidency before commencing operations for companies subject to certification.
- **Compliance with Strategy:** Implementing the measures set forth in the policies and strategies developed by the Presidency.
- **Cooperation:** Cooperating with public institutions, the private sector, and other entities in the course of operations.

In addition, the Law provides that the Presidency may supervise the activities and transactions of institutions, organizations, and individuals falling within its scope. For this purpose, it conducts on-site inspections, appoints independent auditors, and carries out off-program audits when deemed necessary.

Entities subject to audit are obliged to make their devices, systems, software, and hardware available for inspection, to keep them operational, and to provide the necessary infrastructure. Local administrative authorities such asgovernors and law enforcement units are also required to provide full support to the audit.

For reasons of national security and public order, searches, copying, and seizures may be carried out either pursuant to a court order or, in cases where delay poses a risk, upon the order of a public prosecutor. Actions taken without a court order must be submitted for judicial approval within 24 hours, and if no decision is rendered within 48 hours, the data obtained must be destroyed.

5. Offenses and Sanctions

Description of Offense	Prescribed Sanction
Persons who fail to provide, or obstruct the provision of, information, documents, software, data, or hardware requested by the authorities or inspectors authorized under the Law	Imprisonment from one to three years together with a judicial fine ranging from five hundred to one thousand five hundred days shall be imposed.
Persons who carry out any activity without obtaining the approval, authorization, or permits required under this Law	Imprisonment from two to four years together with a judicial fine ranging from one thousand to two thousand days shall be imposed.
Persons who breach the obligation of confidentiality stipulated by the Law	Imprisonment from four to eight years shall be imposed.
Persons who, as a result of a data breach in cyberspace, disclose, share, or put up for sale—whether for free or for a fee—personal data or institutional data related to critical public services without the consent of the relevant individuals or entities	Imprisonment from three to five years shall be imposed.
Persons who, despite knowing that no data breach has occurred, create or disseminate false content for the purpose of causing fear, panic, or concern among the public, or of targeting institutions or individuals	Imprisonment from two to five years shall be imposed.
Persons who launch cyberattacks against the components constituting the national cyber power of the Republic of Turkey, or who keep the data obtained through such attacks in cyberspace (provided that the act does not constitute a more severe offense)	Imprisonment from eight to twelve years shall be imposed.
Persons who disseminate, transfer, or put up for sale the data obtained as a result of such attacks	Imprisonment from ten to fifteen years shall be imposed.
Persons who abuse the duties and powers arising from this Law, or who cause data breaches by failing to take the necessary measures to protect critical infrastructures against cyberattacks	Imprisonment from one to three years shall be imposed.

6. Conclusion

The Law No. 7545 on Cybersecurity introduces a comprehensive legal framework designed to strengthen and systematize cybersecurity in Türkiye. . The Law imposes clear obligations on public institutions, the private sector, and individuals, while also introducing deterrent sanctions.

Its effectiveness, however, will depend on the timely issuance of secondary regulations, the enhancement of institutional technical capacities, and the continued safeguarding of fundamental rights. If implemented effectively, the Law will enhance the resilience of Türkiye's digital infrastructure and provide a strong shield against cyber threats.