BİÇER GÜNER

Attorneys-at-Law

INFORMATION NOTE ON THE CYBERSECURITY LAW

INTRODUCTION

Cybersecurity constitutes a critical area for national security, economic stability and the protection of individuals' private lives in today's world where digitalization is accelerating. In this regard, the Cybersecurity Law (“Law”), which was submitted to the Grand National Assembly of Türkiye (“GNAT”) on January 10, 2025, has been adopted by the GNAT on March 12, 2025 and has entered into force upon publication in the Official Gazette No. 32846 dated March 19, 2025, aims to strengthen Türkiye's existing cybersecurity strategies and align them with international standards.

FUNDEMENTAL ELEMENTS OF THE LAW

The Law aims to strengthen the cybersecurity of the Republic of Türkiye and aims to protect the elements that constitute the national strength against internal and external threats. In the Law;

- Provisions to increase the security of the public and private sectors against cyber-attacks and to establish cybersecurity strategies are introduced;
- Framework of the strategies for identification and protection of critical infrastructures are being established;
- The organization of cybersecurity drills and taking proactive measures against threats become mandatory;
- New provisions are introduced, including the storage of log records, audit processes, and testing and certification processes of hardware products for data security.

The Law clearly defines the responsibilities of public and private sector organizations operating in the field of cybersecurity, requiring them to take cybersecurity measures and report vulnerabilities in a timely manner. It also requires such organizations to use only cybersecurity products and services approved and certified by the Cybersecurity Directorate (“Directorate”). The Directorate plays a central role in formulating and implementing cybersecurity strategies, as well as conducting audit processes. It is envisaged that the Directorate can initiate legal processes such as search, copying and seizure to ensure compliance with cybersecurity rules.

The Law envisages that the Cybersecurity Board (“Board”), which will be established under the Presidency Office of the Republic of Türkiye, will formulate and implement nationwide cybersecurity policies, strategies and action plans. The Board aims to increase Türkiye's cybersecurity capacity by enhancing international cooperation.

CYBERSECURITY PRODUCTS AND COMPANIES

The Law stipulates that the sale of cybersecurity products, systems, software, hardware and services abroad shall be carried out in accordance with the procedures and principles to be determined by the Directorate and that the approval of the Directorate shall be sought for the sale of certain products abroad.

It is also stipulated that the merger, spin-off, share transfer or sale transactions of companies operating in the field of cybersecurity and producing cybersecurity products, systems, software, hardware and services shall be notified to the Directorate; and that transactions that provide real or legal persons individually or collectively with direct or indirect control rights or decision-making authority over the company are subject to the approval of the Directorate and transactions carried out without this approval shall be deemed invalid.

PENAL PROVISIONS AND SANCTIONS

The Law stipulates criminal sanctions for violations of the law in the field of cybersecurity, and stipulates that prison sentences and judicial fines will be imposed on persons who obstruct information and hardware requests, fail to fulfill their security obligations, or commit crimes through data leaks. In the event that cybersecurity officers violate their obligations, criminal sanctions are foreseen and it is stipulated that a portion of the administrative fines collected will be transferred to the budget of the Directorate.

Accordingly, the following penalties are stipulated in the Law:

- Imprisonment from 1 year to 3 years and a judicial fine from 500 days to 1500 days for those who do not provide or prevent the provision of the information, documents, software, data and hardware requested by the authorities authorized by the Law and audit officers within the scope of their duties and powers;
- Imprisonment from 2 years to 4 years and a judicial fine from 1000 days to 2000 days for those who operate without obtaining the approvals, authorizations or permits required by the Law;

- Imprisonment from 4 to 8 years for those who violate the confidentiality obligation;
- Imprisonment from 3 to 5 years for those who, as a result of a data leak, make available, share or offer for sale, for a fee or free of charge, personal or key public service corporate data that previously existed in cyberspace, without the permission of individuals or institutions;
- Imprisonment from 2 to 5 years for those who create or disseminate false content about data leaks related to cybersecurity in order to create anxiety, fear and panic among the public or to target institutions or individuals, despite knowing that such leaks do not exist;
- Imprisonment from 8 to 12 years for those involved in cyber-attacks;
- Imprisonment from 10 to 15 years for those who disseminate, send elsewhere or put up for sale the data obtained as a result of a cyber-attack;
- Administrative fines from TRY 1 million to TRY 10 million for private companies that do not fulfill the information requests of public institutions, and from TRY 10 million to TRY 100 million for those who violate the obligations regarding cybersecurity products and companies; and
- An administrative fine of not less than TRY 100,000 and up to 5% of the gross sales revenue in the independently audited annual financial statements for companies that fail to fulfill their obligations within the scope of the audit, and an administrative fine of TRY 100,000 to TRY 1 million for other persons.

TRANSITION PROVISIONS

The Law stipulates that the movable property, IT infrastructure, systems, vehicles, tools, equipment and materials, all kinds of records and documents, and all receivables and debts of the Directorate of Information and Communication Technologies ("ICTA") and the Digital Transformation Office, all of which are used for cybersecurity activities, shall be transferred to the Directorate within 6 months following the publication of the Law. Furthermore, it is stipulated that the personnel employed by the ICTA and the Digital Transformation Office, who provide services in the field of cybersecurity, will be assigned to the Directorate upon their request.

Within 1 year following the publication of the Law, secondary regulations regarding the implementation of the Law will be enacted by the Directorate and within 1 year following the entry into force of such secondary legislation; associations, federations of associations, foundations and trade companies in the field of cybersecurity shall be obliged to fully comply with the Law and the secondary legislation to be enacted pursuant to the Law.

COMPARATIVE ASSESSMENT

1. United Nations Convention on Cybercrime

The Convention on Cybercrime (“UN Convention”), which the United Nations will open for signature in 2025, aims to increase international cooperation and establish a standardized basis for combating cybercrime among member states. The Convention requires member states to harmonize their national legislation in areas such as cross-border information sharing, collection of digital evidence and extradition. It also envisages the contribution of technology companies to the fight against cybercrime by encouraging cooperation between the private sector and public institutions.

The Law is substantially in line with the UN Convention. However, the Law places a more limited emphasis on international cooperation by prioritizing the creation of a cybersecurity ecosystem at the national level. The cross-border information sharing and joint operation mechanisms envisaged in the UN Convention are not explicitly regulated in the Law. On the other hand, Türkiye's approach of a central authority-based oversight mechanism differs from the UN's more flexible and cooperation-oriented structure.

2. European Union Rules

The European Union's Cyber Resilience Act and the Network and Information Security Directive (NIS 2) are risk management-based regulations that aim to protect critical infrastructure and enhance the security of digital products. The EU regulations provide a guiding framework, allowing member states to develop their own risk management processes.

The Law, on the other hand, adopts a more centralized supervision and enforcement mechanism compared to the EU regulations. In contrast to the EU's flexible regulations, the Law stipulates strict legal obligations and administrative penalties. This reflects Türkiye's priority to protect its national interests and respond faster to cybersecurity risks.

3. Rules of the United States of America

The United States' National Cybersecurity Strategy aims to protect critical infrastructures and raise cybersecurity standards through sector-based regulations. The US regulations are based on cooperation between the private sector and the government and adopt a voluntary approach.

Unlike the US sectoral approach, the Law provides a comprehensive framework that covers all sectors. Moreover, unlike the voluntary methods of the US, Türkiye emphasizes mandatory compliance and centralized enforcement mechanisms. This approach shows that the Law prioritizes national security priorities and follows a centralized control-oriented strategy.

CONCLUSION AND ANALYSIS

In today's digital world, cybersecurity has a strategic importance in terms of protecting the rights of individuals, ensuring economic stability and strengthening national security. In this context, the Cybersecurity Law aims to strengthen Türkiye’s cybersecurity infrastructure and create a more effective ecosystem at the national level. The regulations stipulated by the Law include important steps, especially in terms of protecting critical infrastructures, establishing a national cybersecurity strategy and implementing a centralized audit mechanism against cybersecurity threats.

While building a national cybersecurity ecosystem, the Law adopts a more centralized and mandatory oversight approach compared to the United Nations Convention on Cybercrime, European Union regulations and the national strategies of the United States. This can be interpreted as an effort to prioritize Türkiye's national interests and develop a system that suits its internal dynamics. However, the limited regulations on international cooperation and cross-border information sharing can be considered as a deficiency in effectively addressing global threats.

Contact

Burçak Kurt Biçer
Managing Partner
burcak.bicer@bicerguner.com

Uğurkan Şeber
Managing Associate
ugurkan.seber@bicerguner.com

Doğaç Karakurt
Associate
dogac.karakurt@bicerguner.com

BİÇER GÜNER

Attorneys-at-Law