



# Economic Espionage Laws

Afghanistan • Armenia • Azerbaijan • Georgia • India  
Israel • Kazakhstan • Kyrgyz Republic • Mongolia  
Peru • South Korea • Tajikistan • Turkey  
Turkmenistan • United Arab Emirates  
Uzbekistan

July 2022

LL File No. 2022-021351  
LRA-D-PUB-002587

This report is provided for reference purposes only.  
It does not constitute legal advice and does not represent the official  
opinion of the United States Government. The information provided  
reflects research undertaken as of the date of writing.  
It has not been updated.

# Contents

- Comparative Summary ..... 1
- Afghanistan..... 4
- Armenia ..... 8
- Azerbaijan ..... 13
- Georgia ..... 19
- India ..... 25
- Israel..... 30
- Kazakhstan..... 38
- Kyrgyz Republic..... 42
- Mongolia ..... 48
- Peru ..... 53
- South Korea..... 55
- Tajikistan ..... 62
- Turkey..... 65
- Turkmenistan..... 75
- United Arab Emirates..... 79
- Uzbekistan..... 83

# Comparative Summary

*Ruth Levush*  
*Senior Foreign Law Specialist*

This report addresses economic espionage laws and the regulation of fraudulent filing of corporate, import-export, and banking documentation. In addition to describing relevant legislation, the report provides examples of convictions and law enforcement activities regarding economic espionage and the violation of export control requirements from the past five years.

The report was prepared by staff of the Global Legal Research Directorate of the Law Library of Congress. In addition to this summary, the report consists of individual country surveys for the following countries: **Afghanistan, Armenia, Azerbaijan, Georgia, India, Israel, Kazakhstan, Kyrgyz Republic, Mongolia, Peru, South Korea, Tajikistan, Turkey, Turkmenistan, United Arab Emirates (UAE), and Uzbekistan.**

## I. Legislation

The countries surveyed do not have stand-alone comprehensive legislation on economic espionage. Instead, they subject certain related unauthorized activities to criminal or civil penalties, or both.

Among offenses that may be relevant to commercial espionage are espionage and offenses against state secrets, filing fraudulent corporate registration information, filing fraudulent import/export documentation, filing false customer information with banking entities, violating trade secrets and technology protections, and unfair competition. A number of the countries surveyed specifically regulate the use and export of defense technology and impose penalties on violators.

## II. Penalties

Harsh penalties consisting of long periods of imprisonment usually apply to espionage offenses in all the countries surveyed. **UAE** law allows for the death penalty for providing any type of information to an enemy.

Fraudulent filings of corporate registration documents, import and export documentation, and customer information to banking entities typically constitute criminal offenses in the countries surveyed. Offenders are subject to imprisonment, fines, or both.

Increased penalties are imposed for violating export controls involving defense equipment under **Israeli** law, or designated chemicals, organisms, materials, equipment, and technologies under **Indian** law. **South Korean** law similarly provides for longer periods of imprisonment and higher fines for the intentional use or enabling the use of defense technology in a foreign country, in addition to other penalties for violating the country's Defense Technology Security Act, and other legislation regulating unfair competition.

### III. Standard of Proof

With regard to standard of proof of economic espionage-related offenses under the Penal Code of **Afghanistan**, it appears that a lower threshold applies as compared with the standard of proof required for crimes such as adultery that are considered hudud crimes under Islamic law.

Criminal conviction in economic espionage-related offenses in **Georgia, India, Israel, South Korea, and Turkey** requires the prosecution to prove the allegations against a defendant beyond a reasonable doubt. Under **Israeli** law, authorized officials alternatively may, at their discretion and on the basis of what appears to be a lower evidentiary threshold, issue civil fines for some import-export violations.

### IV. Arrests and Convictions

A survey of convictions for economic espionage and violations of export controls has identified several **Israeli** court cases adjudicating the submission of fraudulent or erroneous import-export documents; unauthorized export of defense equipment; and sale of materials, know-how, and equipment to an enemy state. The country survey for Israel also contains information on a case where the Israeli Supreme Court approved the extradition to the United States of a person charged with illegally exporting, through others, US military spare parts from the US to Israel and US military spare parts from Israel to a third country.

In the **UAE**, a British academic was convicted in 2018 of collecting confidential information about government companies and the royal family; spying for MI6, the United Kingdom intelligence service; and jeopardizing the economic security of the UAE. He was later pardoned and allowed to leave the country.

Although **South Korean** examples from the past five years of convictions on violations of export controls or for economic espionage were not located, the National Intelligence Service in that country has detected 99 cases of attempted industrial espionage from January 2017 to February 2022.

Information on court adjudication of economic espionage-related cases in **Kazakhstan**, like in several other Central Asian countries surveyed, is usually classified. According to media reports, however, in July 2019, a government advisor was accused of sharing classified information with China's intelligence service. In April 2022, a group of persons, including a foreign citizen, reportedly were arrested in Kazakhstan on suspicion of gathering and divulging information containing state secrets.

A **Mongolian** activist was reported arrested in February 2022 for allegedly breaching national security, but it is unclear what specific charges the Mongolian General Intelligence Agency brought against him.

Very little information was located on convictions in **India** for economic espionage of foreign-controlled technology and export-control violations. However, several instances where missile-related regulated substances and equipment were being transported between two foreign

countries, with India being used as a transit point, have been reported in recent years by Indian authorities.

The individual country surveys that follow this summary provide specific information on legislation on economic espionage and related matters.

# Afghanistan

*Tariq Ahmad*  
*Foreign Law Specialist*

**SUMMARY** There are a number of provisions in the Afghan Penal Code that might apply to economic espionage, including disclosure of job-related secrets, commercial secrets, and industrial secrets. Under the Law of Limited Liability Companies, registering fraudulent documents in the Central Business Registry is an offense to which the Penal Code applies. There does not appear to be any specific provisions on providing false export/import documentation or false customer information to banks but provisions on fraud and forgery in the Penal Code may apply in such situations.

## I. Economic Espionage Legislation

Afghanistan's main codified body of criminal law, the Penal Code of Afghanistan, 2017,<sup>1</sup> contains a number of offenses concerning espionage (involving military, defensive, or security secrets),<sup>2</sup> treason,<sup>3</sup> disclosure of nuclear secrets,<sup>4</sup> disclosure of secrets related to a job or occupation,<sup>5</sup> and disclosure of commercial and industrial secrets.<sup>6</sup>

Article 627 is on the disclosure of secrets

### Disclosure of Secrets

Article 627: A person who, by virtue of his job, occupation, profession, business, trade, or the nature of his work, obtains secrets and reveals them other than in circumstances stipulated by law, or uses them for his own or another person's benefit, is deemed to have committed the crime of disclosing secrets and is to be sentenced to short imprisonment or a fine of thirty thousand to sixty thousand afghanis [about US\$330 to US\$660].<sup>7</sup>

Article 758 also imposes a short term of imprisonment for using or disclosing commercial and industrial secrets without an owner's consent.<sup>8</sup>

---

<sup>1</sup> Penal Code of the Islamic Republic of Afghanistan (Penal Code), Official Gazette No. 1260, May 15, 2017, <https://perma.cc/TSD9-P9MR> (in Dari and Pashto).

<sup>2</sup> Id. art. 240.

<sup>3</sup> Id. art. 238.

<sup>4</sup> Id. art. 330.

<sup>5</sup> Id. art. 627.

<sup>6</sup> Id. art. 758.

<sup>7</sup> Id. art. 627 (unofficial translation by author).

<sup>8</sup> Id. art. 758.

The Ministry of Industry & Trade website does include a number of other laws on the protection of trade and industrial secrets,<sup>9</sup> including the Domestic Industrial Protection Law,<sup>10</sup> Law on Protection of Trade and Industrial Secrets,<sup>11</sup> and the Industrial Design Protection Law.<sup>12</sup>

It should be noted that, with the takeover of Afghanistan by the Taliban, there is uncertainty over whether these laws are still in force.

## II. Evidentiary Legal Threshold and Penalty

Under Islamic law, there are three types of crimes: hudud, qisas, and ta'azir crimes.<sup>13</sup> The first two categories are applied in Afghanistan through Hanafi jurisprudence,<sup>14</sup> with hudud having a standard of proof that is "quite demanding," involving corroboration of a certain number of witnesses and/or a confession.<sup>15</sup> Crimes within the Penal Code are a category of crimes under Islamic law that are considered ta'azir crimes, as article 2(1) stipulates, "this law regulates Ta'aziri crimes and punishments."<sup>16</sup> It is unclear what evidence standard is used in Afghanistan for ta'azir crimes and crimes in other enacted laws, but the standard of proof and evidence appear not to be as high as for hudud crimes.

Chapter 7 of the Penal Code has a number of provisions related to forgery. Chapter 4 has provisions concerning fraud (including using forged documents) that are of general application.

### A. Filing Fraudulent Corporate Registration Information

The Law on Limited Liability Companies was enacted to regulate the affairs related to the establishment of limited liability companies.<sup>17</sup> It entered into force on March 3, 2019. Article 103 makes registering fraudulent documents in the Central Business Registry a punishable offense.<sup>18</sup>

---

<sup>9</sup> Laws, Ministry Industry & Com., <https://perma.cc/66LB-M7YV>.

<sup>10</sup> Domestic Industrial Protection Law, <https://perma.cc/J2LM-WX5T>.

<sup>11</sup> Law on Protection of Trade and Industrial Secrets, Official Gazette No. 1233, Oct. 22, 2016, <https://perma.cc/367E-CLRZ> (in Dari and Pashto).

<sup>12</sup> Industrial Design Protection Law, Official Gazette No. 1221, Sept. 6, 2016, <https://perma.cc/4TQL-STRC> (in Dari and Pashto).

<sup>13</sup> Eur. Asylum Support Off., *Afghanistan: Criminal Law, Customary Justice and Informal Dispute Resolution 12* (2020), <https://perma.cc/S54B-ZMRT>.

<sup>14</sup> Penal Code art. 2(2).

<sup>15</sup> Eur. Asylum Support Off., *supra* note 13, at 62; see also Afghanistan Legal Educ. Project, *An Introduction to the Criminal Law of Afghanistan* 87-88 (2015), <https://perma.cc/8HB8-Q92S>. "Despite mandatory penalties, the standard of proof in hudud cases is quite demanding. For most crimes, including adultery, witnesses must corroborate any claim before guilt can be established. Witness veracity is evaluated in terms of gender, community standing, the content of the statement, and the number of witnesses present."

<sup>16</sup> Penal Code art. 2(1).

<sup>17</sup> Law on Limited Liability Companies, Official Gazette No. 1292, Mar. 3, 2019, <https://perma.cc/Z8C5-DWVD>.

<sup>18</sup> *Id.* art. 103.

An English translation of what appears to be an earlier draft of the law states, “A person who intentionally signs a fraudulent document and forwards it for registration to the CBR [Central Business Registry] shall be punished according to the provisions of the Penal Code.”<sup>19</sup>

Article 97 of the law also allows a commercial court to dissolve a limited liability company (LLC) in a proceeding on certain grounds if the Ministry of Commerce and Industry establishes that the LLC obtained its license through fraud.<sup>20</sup>

## **B. Filing Fraudulent Import/Export Documentation**

Foreign trade, including export restrictions, is subject to the Customs Law,<sup>21</sup> Law on Foreign Trade,<sup>22</sup> Afghan Trade Policy,<sup>23</sup> and other laws and regulations.

The representative of Afghanistan said that export of goods was currently subject to the procedures stipulated in the Business Licence Regulation of 2004. The representative of Afghanistan said that according to Article 53 of the Customs Law, the Head of Customs Department had the authority to adopt prohibitions or restrictions for reasons of: public morality; public security; protection of the environment; protection of the health and life of humans, animals or plants; the protection of national treasures possessing artistic, historic or archaeological value; *or the protection of industrial and commercial property* [emphasis added] and other state policies. He noted that antiquities were currently prohibited from export in accordance with the Law on Preservation of Historic and Cultural Heritage of Afghanistan of 2004.<sup>24</sup>

The Business License Regulation states, “It shall be unlawful to provide false or misleading information in the business license application. The penalty for providing false or misleading information shall be the immediate revocation of the business license.”<sup>25</sup>

There also appear to be regulations on import and export licensing, but we were unable to locate a provision on false export documentation.<sup>26</sup>

---

<sup>19</sup> Limited Liability Companies Law art. 104, <https://perma.cc/2F6W-VLCK> (unofficial translation of draft law by DLA Piper).

<sup>20</sup> Law on Limited Liability Companies art. 97.

<sup>21</sup> *Afghanistan Customs Law*, UAIPIT (Mar. 20, 2005), <https://perma.cc/DP8K-98BY> (unofficial English translation).

<sup>22</sup> Law on Foreign Trade (1395), <https://perma.cc/MFT2-CADG>.

<sup>23</sup> Ministry Industry & Com., *Afghanistan National Trade Policy, 2019-2023* (2019), <https://perma.cc/55DW-F73Q>.

<sup>24</sup> World Trade Organization, *Accession of Afghanistan: Elements of a Draft Working Party Report*, WT/ACC/SPEC/AFG/3 (Nov. 9, 2012), <https://perma.cc/9BDP-FWUG>.

<sup>25</sup> Business License Regulation (2004) art. 13, <https://perma.cc/8Z3Z-ZV5U>.

<sup>26</sup> Afghanistan Gov't, *Draft Regulations on Import and Export Licensing of 2013 (1391)* (Jan. 10, 2013), <https://perma.cc/83WK-L2DX>.

The Penal Code lists offenses involving exporting strategic materials (capable of dual-use) without a license or legal permit.<sup>27</sup> It also prohibits the smuggling of goods including contraband.<sup>28</sup> It is unclear whether a specific provision on filing fraudulent import/export documentation is in the Penal Code but general provisions on forgery and fraud may apply.

### **C. Filing False Customer Information with Banking Entities**

The Banking Law of Afghanistan regulates the “banking affairs in the country.”<sup>29</sup> It penalizes certain practices that may endanger banks.<sup>30</sup> No provision was found on filing false customer information with a bank. The general provisions of the Penal Code may apply to this situation.

## **III. Past Convictions for Economic Espionage or Export-Control Violations**

No information could be found on past convictions for economic espionage or export-control violations.

---

<sup>27</sup> Penal Code of the Islamic Republic of Afghanistan arts. 326-327.

<sup>28</sup> Id. arts. 778-786.

<sup>29</sup> Banking Law of Afghanistan art. 1(1), <https://perma.cc/2CMJ-QSLR>.

<sup>30</sup> Id. art. 173.

# Armenia

Iana Fremer  
Legal Research Analyst

**SUMMARY** There does not appear to be any comprehensive law in the Republic of Armenia criminalizing economic espionage. The Criminal Code of the Republic of Armenia provides specific provisions on the crime of espionage, but does not distinguish economic espionage. There are a number of the state laws, including the Law of the Republic of Armenia on Protection of the Economic Competition and the Law on State and Official Secrets, criminalizing the passing to foreign countries of economic information that damages the state's economic interests and the unauthorized disclosure of trade secrets.

Fraudulent activities by banks and private corporations are prosecuted administratively and are generally punishable by fines unless substantial damage has been inflicted by these actions.

In Armenia, information on specific crimes committed in the area of economic espionage is usually classified and not available from public sources.

## I. Economic Espionage Legislation

There is no specific economic espionage legislation in Armenia. The Criminal Code of the Republic of Armenia defines espionage as transferring information that contains state secrets to a foreign state or foreign organization as well as gathering, stealing, and storing such information with the purpose of transferring it later to foreigners. The code prescribes imprisonment for a period of 12 to 20 years as a punishment for committing this crime.<sup>1</sup>

Information that can be classified as a state secret is defined in the Law on State and Official Secrets.<sup>2</sup> It may include any information related to the military, economy, foreign relations, science and technology, intelligence, counterintelligence, and operational intelligence activities, if dissemination of this information has been restricted by the state and may cause grave consequences for the security of the country.<sup>3</sup>

---

<sup>1</sup> Criminal Code of the Republic of Armenia, adopted on Apr. 18, 2003, last amended 2018, art. 302, <https://perma.cc/FJ7X-4DLZ> (unofficial English translation); Artak Khulian, *Armenia Toughens Penalties for High Treason, Espionage*, (Mar. 25, 2021), Radio Azatutyun, <https://perma.cc/FZ8T-T7NW>.

<sup>2</sup> Law on State and Official Secrets of the Republic of Armenia, No. HO-94, adopted on Dec. 3, 1996, last amended Jan.16, 2018, <https://perma.cc/57FJ-W6PK> (unofficial English translation).

<sup>3</sup> Id. art. 2.

According to this law, the requirements within the act shall not apply to trade and economic information unless it is related to foreign relations policy, and foreign economic activities (which may include trade, loans and currency) of the Republic of Armenia.<sup>4</sup>

Individuals who perform any type of unlawful activity with the use of information constituting state and official secrets shall bear criminal, administrative, or disciplinary liability.<sup>5</sup>

The Criminal Code states that the intentional publication of information containing a state secret by a person who had access to the state secret or became aware of it in the course of his or her service, shall be punished by imprisonment for a period of up to four years, with deprivation of the right to hold certain positions or to engage in certain activities for a period of three years.<sup>6</sup>

Imprisonment for two years, with deprivation of the right to hold certain positions or to engage in certain activities for a period of three years, must be imposed for publication of information containing a state secret by negligence.<sup>7</sup>

Under the Armenian Criminal Code, siding with the enemy, espionage, revealing a state secret to a foreign state or foreign organization or its representatives, or assisting otherwise in carrying out hostile activities, committed by a citizen of the Republic of Armenia to the detriment of the sovereignty, territorial inviolability, or external security of the Republic of Armenia is considered high treason.<sup>8</sup> In 2021, Armenia toughened penalties for high treason, making this crime punishable by a life sentence or 15 to 20 years of imprisonment, with or without confiscation of property.<sup>9</sup>

There is no specific trade secret law in Armenia, but the protection of trade secrets is covered by Armenia's Civil Code and the Law of the Republic of Armenia on Protection of Economic Competition, which prohibit illegal receipt, distribution, or usage of information containing commercial secrets.<sup>10</sup>

The Civil Code defines trade and banking secrets as information having an actual or potential commercial value by virtue of the following:

---

<sup>4</sup> Id. arts. 7, 14.

<sup>5</sup> Id. art. 27.

<sup>6</sup> Criminal Code art. 306.

<sup>7</sup> Id. art. 306, para. 2.

<sup>8</sup> Id. art. 299.

<sup>9</sup> Khulian, *supra* note 1.

<sup>10</sup> Civil Code of the Republic of Armenia, No. ZR-239, adopted May 5, 1998, last amended Mar. 28, 2022, <https://perma.cc/WMK5-ZU8M> (unofficial English translation); Law of the Republic of Armenia on Protection of the Economic Competition, No. ZR-112, of Dec. 5, 2000, last amended Mar. 11, 2022, <https://perma.cc/CEP8-EPWP> (unofficial English translation).

- it is unknown to third persons,
- there is no free access to it on a legal basis, and
- the holder of the information takes measures to protect its confidentiality.<sup>11</sup>

Also, if the individuals have illegally received information which constitutes a commercial or banking secret, they are obligated to compensate for losses caused. The same obligation is imposed on contract partners who have divulged a commercial or banking secret in violation of a civil law contract or a labor contract.<sup>12</sup>

A business entity is not required to provide information containing commercial secrets to government institutions and officials in the course of business registration or government oversight. The government is also prohibited from divulging commercial secrets that become known to the authorities.<sup>13</sup>

According to the Law on Protection of the Economic Competition, any entrepreneurial activity or conduct which may lead to acquisition, use and disclosure of undisclosed information without the consent of its lawful owner or in violation of traditions of business circulation shall be deemed as an act of unfair competition.<sup>14</sup>

The methods of acquisition, use and disclosure of undisclosed information shall be deemed as violation of business circulation traditions qualifying as an act of industrial or economic espionage.<sup>15</sup>

In addition, technical information and organizational or commercial data, including production secrets (know-how), shall be deemed as undisclosed if this data, as a whole or in parts, is completely unknown or not easily accessible to persons dealing with such information; has certain actual or possible commercial value due to being unknown to third parties; and when a legitimate owner, whether a natural person or a legal entity, has undertaken reasonable steps to maintain the confidentiality of information under existing circumstances.<sup>16</sup>

This crime is punished by a fine, restrictions on the perpetrator's freedom, correctional labor, or imprisonment for up to one year.<sup>17</sup>

Furthermore, illegal publicizing or use of commercial or banking secrets without the consent of the owner by one who knows these secrets due to professional or official activity, done for mercenary or other personal motives which cause significant damage to the commercial

---

<sup>11</sup> Civil Code art. 141, para. 1.

<sup>12</sup> Id. art. 141, para. 4.

<sup>13</sup> Law of the Republic of Armenia on Protection of the Economic Competition art. 33.

<sup>14</sup> Id. arts. 11-16.

<sup>15</sup> Id. art. 16.

<sup>16</sup> Id.

<sup>17</sup> Criminal Code, arts. 158, 159, 254.

organization or individual entrepreneur, shall be punished with a fine, with or without deprivation of the right to hold certain positions or practice certain activities for up to three years, or with imprisonment for a period of up to three years.<sup>18</sup>

Also, in accordance with article 199 of the Criminal Code, individuals can be sentenced to up to three years of imprisonment for the illegal collection or divulging of commercial or banking secrets by stealing documents, bribing, or threatening the persons who know commercial or banking secrets, or their relatives, or through intercepting communications by illegal penetration into a computer network or software system.<sup>19</sup>

## II. Prosecution of Fraudulent Activities of Private Corporations

Corporate registration is mandatory in the Republic of Armenia, and is regulated by the Law on State Registration of Legal Entities.<sup>20</sup> Violating the registration rules or conducting business without registering or obtaining proper licenses is considered illegal entrepreneurship.<sup>21</sup> It is classified as a crime and prosecuted under article 188 of the Criminal Code, which provides for punishment in the form of a fine or arrest for a period of two to three months.<sup>22</sup> The amount of the fine depends on the amount of inflicted damage or the amount of illegally received profits.<sup>23</sup> In a case where these amounts are especially large, increased fines and imprisonment will result. The same acts, if committed by a group of people or by a person previously convicted for the same violations, are punishable by imprisonment for a period of up to five years.<sup>24</sup>

Similar regulations apply to illegal banking activities.<sup>25</sup>

The Customs Code provides for a set of rules related to the import and export of goods in the Republic of Armenia. Armenia does not tax exports and does not have any licensing requirements for exporting. There are neither export duties nor VAT payment obligations or limitations.<sup>26</sup> There are regulations that impose penalties for violation of export rules.<sup>27</sup> In addition to imposing fines, the law prescribes the confiscation of illegally exported goods.<sup>28</sup>

---

<sup>18</sup> Id. art. 199, para. 2.

<sup>19</sup> Id. art. 199, para. 1.

<sup>20</sup> Law on State Registration of the Legal Entities, AL-169, adopted Apr. 3, 2001, last amended Jun. 3, 2021, art. 5, paras. 1, 3, <https://perma.cc/5XKC-7VTH> (unofficial English translation).

<sup>21</sup> Id. art. 5, para. 3; Criminal Code arts. 188, 187.

<sup>22</sup> Criminal Code art. 188, paras. 1-4.

<sup>23</sup> Id.

<sup>24</sup> Id.

<sup>25</sup> Code of Administrative Offenses, adopted Jun. 1, 1986, last amended Nov. 17, 2017, arts. 582, 584, 586, <https://perma.cc/JG32-HU8W> (in Russian); Criminal Code arts. 187-189.

<sup>26</sup> Customs Code of the Republic of Armenia, adopted on Jan. 1, 2001, amended on Jul. 1, 2003, arts. 43, 51, 90-92, <https://perma.cc/6JSF-GCQB> (unofficial English translation).

<sup>27</sup> Id. arts. 108, 113, 139.

<sup>28</sup> Id. art. 216.

Chapter 3 of the Law on Control of Export and Interstate Transit of Dual-Use Goods and Technologies through the Territory of the Republic of Armenia provides for exportation restrictions on goods, and various requirements and procedures for the control of exported goods.<sup>29</sup>

### III. Examples of Convictions on Violations of Espionage Laws

Espionage and other cases that might affect national security are investigated by the Armenian National Security Service (NSS).<sup>30</sup>

In the Republic of Armenia, information on espionage cases is usually classified. Details of these cases are not publicized, and court trials are not open to the public. The only source of information on this type of court decision appears to be media reports, which are limited due to the lack of information disclosed by authorities.

In February 2022, Radio Liberty reported that the NSS had detained 19 people suspected of being members of an “espionage network.”<sup>31</sup>

According to the article, the NSS said it gathered “undeniable evidence” that “foreign intelligence agencies created a network of spies in the territory of Armenia and involved different service members of the military.” The recruitment took place via an online dating service through which Armenian servicemen, who possessed classified data and documents, would eventually join the spy ring.<sup>32</sup>

The investigation was carried out as part of a criminal case opened on espionage and state treason.<sup>33</sup>

---

<sup>29</sup> Law of the Republic of Armenia on the Control of Export and Interstate Transit of Dual-Use Goods and Technologies through the Territory of the Republic of Armenia of Sept. 24, 2003, <https://perma.cc/6YLY-PEHV> (unofficial English translation); Customs Code, arts. 18, 19.

<sup>30</sup> Law on National Security Bodies of the Republic of Armenia, No. HO-294, adopted Dec. 28, 2001, last amended Mar. 23, 2018, arts. 9-11, 15, <https://perma.cc/HUC3-ZPDZ>.

<sup>31</sup> RFE/RL's Armenian Service, *Armenia Detains 19 People Suspected of Being in Spy Ring That Used a Dating Service* (Feb. 10, 2022), Radio Free Europe/Radio Liberty, <https://perma.cc/DZ6Y-AN2E>.

<sup>32</sup> *Id.*

<sup>33</sup> *19 Arrested as Armenian Counterintelligence Neutralizes “Network of Spies” Activated by Foreign Agencies* (Feb. 10, 2022), ARMENPRESS Armenian News Agency, <https://perma.cc/J8XT-4AGT>.

# Azerbaijan

*Kayahan Cantekin*  
*Foreign Law Specialist*

**SUMMARY** The Criminal Code of the Republic of Azerbaijan includes several offenses that would apply to the unauthorized procurement or disclosure of state secrets, which can include some classes of economic and industrial information in accordance with the Law on State Secrets, secondary legislation, and administrative decisions based on that law. The Criminal Code also criminalizes violations of the export control regime, and violations of commercial and bank secrets. This report also provides information on sanctions imposed for the filing of fraudulent corporate registration information and fraudulent import and export documentation.

## I. Overview

In Azerbaijani law, the unauthorized procurement, disclosure, or dissemination of confidential economic information is criminalized through several different offenses provided in the Criminal Code of the Republic of Azerbaijan (CCRA).<sup>1</sup> The most relevant offenses in the CCRA are those criminalizing espionage, the unauthorized acquisition of information considered to be state secrets, and violations of export controls. The espionage offenses and offenses against state secrets appear to require the information in question to be defined as a “state secret” under the applicable legal framework that will be explained below. This framework allows designated state authorities to classify certain classes of economic and industrial information as state secrets. The CCRA also includes offenses that criminalize the violation of trade and banking secrets which may cover certain acts typical of economic espionage. Certain relevant offenses in the CCRA are supplemented by delicts provided in the Code of Administrative Delicts (CAD), which cover less serious variants of some of the offenses provided in the CCRA.<sup>2</sup> This report also presents information on sanctions provided in the CCRA and CAD for the filing of fraudulent corporate registration information and fraudulent import and export documentation.

## II. Espionage Offenses, Offenses Against State Secrets, and Other Offenses Related Confidential Economic Information

### A. Espionage Offenses

Article 276 of the CCRA makes it a crime for foreigners and stateless persons to communicate, steal, or collect state secrets, or to store state secrets for the purposes of communicating them to foreign states or organizations or their representatives. Likewise, it is also a crime to communicate other information on the direction of the special services of a foreign state for the behalf of that

---

<sup>1</sup> Azərbaycan Respublikasının Cinayət Məcəlləsi (CCRA), adopted by Law No. 787-IQ, Dec. 30, 1999, <https://perma.cc/G5WC-7EFF>.

<sup>2</sup> Azərbaycan Respublikasının İnzibati Xətlər Məcəlləsi (CAD), adopted by Law No. 96-VQ, Dec. 29, 2015, <https://perma.cc/9NHJ-9QHC>.

state and to the detriment of the security of the Republic of Azerbaijan. These offenses are punishable by 10 to 15 years in prison. If committed by a citizen of Azerbaijan to the detriment of the sovereignty, territorial integrity, state security, or defensive capability of the Republic of Azerbaijan, acts of espionage, as defined in article 276, are criminalized under article 274 as treason and are punishable by 12 to 20 years in prison, or by life imprisonment.

## B. Offenses Against State Secrets

The CCRA includes three offenses that cover the unauthorized handling of state secrets. Article 284 criminalizes the unauthorized dissemination of state secrets without treasonous intent by a person who is entrusted with the secret or has come to know of the secret by virtue of his official position or work, punishable by three to six years in prison and by four to eight years in prison if the actions lead to serious consequences. Article 284-1 criminalizes the acquisition of information and documents or objects that contain state secrets by the use or threat of force or other coercive means or by deception, or by the use of special technical means, without the intent to commit treason or engage in espionage. This offense is punishable by imprisonment for a term of two to five years. Article 285 makes it a crime for a person entrusted with state secrets to cause the loss of documents or objects containing the state secrets by negligent conduct and the violation of rules determined by law governing the handling of state secrets, provided that the loss of secrets results in serious consequences. This offense is punishable by the restriction of liberty for a term of two to five years.<sup>3</sup>

## C. Definition of “State Secret”

While the definition of “state secret” – which the application of both espionage offenses and offenses against state secrets turn on – is not provided in the CCRA, the rules and principles governing the formal classification of information as “state secrets” is provided in the Law on State Secrets (LSS), where “state secret” is generally defined as “information safeguarded by the state that is related to the military, foreign policy, *economic*, intelligence, counter-intelligence and surveillance operations of the state, and the dissemination of which may harm the security of the Republic of Azerbaijan” (emphasis added).<sup>4</sup> It appears that to be protected under the CCRA offenses, the information in question must be classified as a state secret in accordance with the principles provided in the LSS.<sup>5</sup>

---

<sup>3</sup> The “restriction of liberty” sanction involves the confinement of the convict in his residence with an electronic tracking device, with the possibility of a limited liberty of movement outside the residence being granted by the court or the sentence execution officer in cases of necessity or as an incentive for good behavior. Azərbaycan Respublikasının Cəzaların İcrası Məcəlləsi (Code of Execution of Sentences), adopted by Law No. 908-IQ, July 14, 2000, as amended, arts. 51-1 to 51-7, <https://perma.cc/V4N3-4YNM>.

<sup>4</sup> Dövlət Sirri Haqqında Azərbaycan Respublikasının Qanunu (LSS), Law No. 733-IIQ, Sept. 7, 2004, art. 1.0.1, <https://perma.cc/9CAZ-L25R>.

<sup>5</sup> While research did not find authoritative guidance on this point, the structure of Azerbaijani information law supports this conclusion. The concept of “state secret” is used consistently in the Law on Access to Information (the Azerbaijani equivalent of FOIA), and the Law on Information, Informatics Applications, and Protection of Information (regulating the formation of information resources with relation to the collection, processing, storage, retrieval, and dissemination of information, the use of information systems and technologies and the creation and use of support and maintenance systems, the protection of information, and the rights of subjects involved in information processing). Both laws require state secrets to be determined by law, and do not

Article 6 of the LSS provides the main principles governing the procedure to formally classify information as a state secret and article 5 provides for a closed list of classes of information that can be formally classified as state secrets by state authorities based on subject-matter. According to Article 5.2, information on the following subject-matters related to the economy and industry may be classified as state secrets:

5.2.1. The content of preparation plans for possible military operations of the Republic of Azerbaijan and its separate regions; the mobilization capacity of industry for production and repair of weapons and military equipment; the volume of shipments of strategic raw materials used in for military purposes, reserves, as well as the placement of state and mobilization reserves, and actual volume and their use;

5.2.2. The use of the infrastructure of the Republic of Azerbaijan for the purposes of ensuring its defense capability and security;

5.2.3. The civil defense forces and equipment; the disposition, destination, and degree of protection of objects of administrative management; the degree of security of the population; and transport and communication activities intended for ensuring state security;

5.2.4. Volumes of state defense orders [i.e. requisitions] and their plans (orders); volumes in monetary value or in kind of the issuance and shipment of weapons, military equipment and other military products; enterprises that produce such weapons, military equipment and other military products and their relations and cooperation with each other with relation to the total available capacity and the increase of this capacity;

5.2.5. Scientific and technical achievements, scientific research, experimental designs, project works, and technologies, that have important defense implications or economic significance affecting the security of the state;

5.2.6. The volume of reserves, production, import and export, sale, and state reserves, of strategic minerals determined as such by legislation; the production of banknotes, securities, and protections against counterfeiting, as well as other special measures of state financial activity.<sup>6</sup>

In addition to the subject-matters listed in article 5.2 of the law, article 5.3 also allows information on the foreign trade activities of the Republic of Azerbaijan to be classified as a state secret “if the untimely disclosure of such information would harm the security of the state.”<sup>7</sup>

---

appear to presume a category of per se state secrets. See *İnformasiya Əldə Etmək Haqqında Azərbaycan Respublikasının Qanunu* (Law on Access to Information), Law No. 1024-IIQ, Sept. 30, 2005, art. 34 (distinguishing “state secrets” from “confidential” information, the latter including *inter alia* commercial, professional, and judicial secrets), <https://perma.cc/7YCW-KM8Q>; *İnformasiya, İnformasiyalaşdırma və İnformasiyanın Mühafizəsi Haqqında Azərbaycan Respublikasının Qanunu* (Law on Information, Informatics Applications, and Protection of Information), Law No. 460, Apr. 3, 1998, arts. 6, 8, 10 (referring to the Law on State Secrets as the legal basis of the determination and protection of state secrets, and distinguishing state secrets from “confidential” information, the latter including *inter alia* commercial, professional, and judicial secrets), <https://perma.cc/DUQ9-THUW>. Cf. Council of Europe, *Analysis of Azerbaijani Legislation on Access to Information*, 14-15 (Nov. 2017), <https://perma.cc/3Z35-L599>.

<sup>6</sup> LSS art. 5.2.

<sup>7</sup> Id. art. 5.3.

The actual subject matter headings that are protected as state secrets within the framework of the Law on State Secrets are provided in Presidential Decree no. 248 of June 3, 2005.<sup>8</sup> The Presidential Decree designates 19 headings as state secrets in the economic sphere and identifies the governmental agencies responsible of classifying information under the designated headings.

#### **D. Export Control**

The Law on Export Control provides the main principles of Azerbaijan's export control regime.<sup>9</sup> The list of goods and services that are subject to export controls and the details of the clearance procedures are provided by the Council of Ministers Decision No. 230 of December 15, 2005.<sup>10</sup> The CCRA provides for two offenses related to the enforcement of the export control regime. Article 202-1 of the CCRA criminalizes the unauthorized disclosure or transfer to a third party of documents or information that are related to export control. The offense is punishable by a fine of 1,500 to 2,500 Azerbaijani manats (approx. US\$883-\$1,471), or up to a year of corrective labor, or up to a year of restriction of liberty. The penalty is enhanced to double the fine, or up to two years of corrective labor or imprisonment, if the act causes significant harm.<sup>11</sup>

The second offense enforcing the export control regime is provided in article 224.2 of the CCRA, which criminalizes the export of goods and services subject to the export control to countries or end users that are restricted or prohibited by the export control regime. This offense is punishable by one to two years of correctional labor, or two to five years of restriction of liberty, or two to five years of imprisonment.<sup>12</sup>

#### **E. Violation of Trade and Banking Secrets**

Article 202 of the CCRA criminalizes the collection of information constituting commercial secrets and bank secrets by stealing, purchasing, or through threats or other illegal means, for the purposes of disseminating the information or using it illegally.<sup>13</sup> The offense is punishable by a

---

<sup>8</sup> "Dövlət Sırrına Aid Edilən Məlumatların Siyahısı"nın Təsdiq Edilməsi Haqqında Azərbaycan Respublikası Prezidentinin Fərmanı, Decree No. 248, June 3, 2005, ch. IV, <https://perma.cc/YLT2-FN9J>.

<sup>9</sup> İxrac Nəzarəti Haqqında Azərbaycan Respublikasının Qanunu (Law on Export Control), Law No. 772-IIQ, Oct. 26, 2004, <https://perma.cc/R5UP-GV6N>.

<sup>10</sup> "İxrac Nəzarəti Haqqında" Azərbaycan Respublikası Qanununun Tətbiqi ilə Bağlı Bəzi Normativ Aktların Təsdiq Edilməsi Barədə Azərbaycan Respublikası Nazirlər Kabinetinin Qərarı, Decision No. 230, Dec. 15, 2005, <https://perma.cc/TTJ5-H365>.

<sup>11</sup> CCRA art. 202-1.2.

<sup>12</sup> Id. art. 224.2.

<sup>13</sup> "Commercial secret" is defined as "information related to the production, technological, management, financial and other activities of legal and natural persons which may harm the legitimate interests of their owners if disclosed without their consent". Kommersiya Sirri Haqqında Azərbaycan Respublikasının Qanunu (Law on Commercial Secrets), Law No. 224-IIQ, Dec. 4, 2001, art. 2.0.1, <https://perma.cc/XWE8-A3MZ>. The Law on Banks requires banks to guarantee "in accordance with the Civil Code, the confidentiality of the bank account, account transactions and balances, as well as information about the customer, including the name, address and managers of the customer [and] the confidentiality of information about the availability of customers' property in the bank, the owners, nature and value of such property." Banklar Haqqında

fine of 500 to 2,500 manats (approx. US\$294-\$1,471) or corrective labor up to one year, or up to two years of imprisonment. Furthermore, the use or dissemination of information that constitutes a commercial or bank secret for personal financial gain or other personal benefit, without the consent of the owner, and provided that the act causes significant harm, is punishable by a fine in the amount of two times the value of the harm caused as a result of the offense, or up to two years of correctional labor, or up to six months in prison.<sup>14</sup>

### III. Penalties and Standards of Prosecution for Certain Specified Offenses

#### A. Filing Fraudulent Corporate Registration Information

Entities that wish to acquire legal personality in Azerbaijan, and foreign legal persons that wish to establish branches or appoint representatives in Azerbaijan must complete an official registration and be entered into the State Registry.<sup>15</sup> Providing false information to state authorities when registering a legal entity, its branches or representatives, or in the amendment of documents of incorporation or other facts entered in the Register is proscribed as a delict in Article 403 of the CAD. Natural person delinquents are subject to a fine of 700 manats (approx. US\$412), and delinquent legal entities are fined 4,000 manats (approx. US\$2,354) for this delict.<sup>16</sup> Furthermore, failure to register incorporating documents, branches, or representatives as required by law is penalized by a fine of 1,000 to 2,000 manats (approx. US\$588-\$1,176) for officials of the legal entity and 2,500 to 3,000 manats (approx. US\$1,471-\$1,764) for the legal entity itself.<sup>17</sup>

Article 193 of the CCRA provides for a specific offense that criminalizes the creation of a legal entity, including a business association, without the intention of pursuing legitimate entrepreneurial activity, for the purposes of obtaining tax or property related advantages, obtaining credit, or *concealing prohibited activity*, provided that the act causes significant harm or generates significant gains (emphasis added). The offense is punishable by a fine of two to three times the damage caused or gain obtained, or by the restriction of liberty for a period of up to six months, or imprisonment for a period of up to six months. If the same act causes large-scale damage, generates a large amount of gains, or is committed by conspiracy, the offense is punishable by a fine of three times the damage or gain generated, or by the restriction of liberty for a period of up to three years, or one to five years of imprisonment.<sup>18</sup>

---

Azərbaycan Respublikasının Qanunu (Law on Banks), Law No. 590-IIQ, Jan. 16, 2004, art. 41.1, <https://perma.cc/D2LX-4E6F>.

<sup>14</sup> CCRA art. 202.2. The same act is constituted as a delict under article 431 of the CAD if the harm (or gain) is less than 200,000 manats (approx. US\$117,717). The delict is penalized with a fine in the amount of two to four times the harm or gain resulting from the act.

<sup>15</sup> Hüquqi Şəxslərin Dövlət Qeydiyyatı və Dövlət Reyestri Haqqında Azərbaycan Respublikasının Qanunu (Law on the State Registration of Legal Persons and the State Registry), Law No. 560-IIQ, Dec. 12, 2003, arts. 5, 6, <https://perma.cc/88FU-TUJB>.

<sup>16</sup> CAD art. 403.

<sup>17</sup> Id. art. 405.

<sup>18</sup> CCRA, art. 193.2.3. The same act criminalized in art. 193 of the CCRA will be penalized under art. 402 of the CAD if the act does not cause significant harm or gain. The penalty under art. 402 is a fine in the amount of two

## **B. Filing Fraudulent Export/Import Documentation**

The smuggling offense provided in article 206 of the CCRA criminalizes the fraudulent use of any documentation or customs identification means in connection with the transport of “large amounts” of goods and other articles in and out of the customs borders of the Republic of Azerbaijan.<sup>19</sup> The offense is punishable by a fine in the amount of forty to sixty percent of the value of the goods, which can be supplemented with the restriction of liberty or imprisonment for a term up to three years.<sup>20</sup> If the value of the smuggled goods is above 200,000 but not exceeding 500,000 manats (approx. US\$ 117,717-\$294,294) the penalty is enhanced to a 50 to 70 percent fine which can be supplemented with the restriction of liberty for a period of two to five years or two to four years of imprisonment; if the value exceeds 500,000 manats, the penalty is enhanced to a 60 to 80 percent fine with a possible supplement of three to five years of imprisonment.<sup>21</sup>

## **IV. Examples from the Past Five Years of Convictions Based on Violations of Export Controls or for Economic Espionage**

Research did not find relevant incidents of conviction based on violations of export controls or economic espionage from the past five years reported in public sources.

---

to four times the harm caused or gain made by the act. The delinquent will not be held liable if the harmed parties are fully reimbursed and/or the gains are paid to the state treasury.

<sup>19</sup> “Large amounts” is defined as more than 50,000 but less than 200,000 Azerbaijani manats in value (approx. US\$29,429-\$117,717). If the value of goods in question is less than this amount, article 481 of the CAD, which penalizes the same act, will be applicable. See note 1 to CCRA art. 193. The penalty under CAD article 481 is the confiscation of the goods and means of transport, or an administrative fine in the amount of 40 to 60 percent of the value of the goods and the means of transport.

<sup>20</sup> CCRA, art. 206.1.

<sup>21</sup> Id. art. 206.1-1 & 1-2. Art. 206.2 provides a heightened penalty of three to seven years of imprisonment if the goods in question belongs to one of the following classes: “drugs, psychotropic substances or their precursors, highly active substances, toxic, poisonous, radioactive, explosive substances and devices, military weapons and equipment, firearms or ammunition (excluding unrifled hunting weapons and ammunition for these), nuclear, chemical, biological and other weapons of mass destruction, materials and equipment that can be used in the manufacture of weapons of mass destruction and are subject to special rules for the transport through the customs borders of the Republic of Azerbaijan, and strategically important raw materials, cultural, historical or archeological wealth whose transport through the customs borders of the Republic of Azerbaijan is subject to regulations. . . .”

# Georgia

*Iana Fremer  
Legal Analyst*

**SUMMARY** There does not appear to be any comprehensive law in Georgia specifically criminalizing economic espionage. The Criminal Code of Georgia provides specific provisions on the crime of espionage but does not distinguish economic espionage.

There are a number of state laws, including the Law on Competition and the Law on State Secrets that criminalize the unauthorized disclosure of trade secrets and the passing of economic information to foreign countries that damages the state's economic interests.

Georgian legislation distinguishes state secrets from commercial secrets. While state secrets are regulated specifically by the Law on State Secrets, commercial secrets are addressed in the General Administrative Code of Georgia. A number of laws define the concepts of professional secrets, banking secrets, and insider information.

Fraudulent activities by banks and private corporations are prosecuted administratively and are generally punishable by fines unless substantial damage has been inflicted by these activities.

There are no publicly available reports of specific cases of economic espionage. However, a watchdog organization has raised questions recently about a lack of transparency regarding the real owners of major business enterprises in Georgia.

## I. Economic Espionage Legislation

There is no specific economic espionage legislation in Georgia. The Criminal Code of Georgia defines espionage as

the collection, storage, transfer, or extortion or stealing of items, documents, information or other data containing state secrets of Georgia for the purpose of handing them to a foreign country, foreign organization or its representatives, or collection or transfer of other information to the detriment of Georgia upon instructions of a foreign intelligence service or of a foreign organisation.<sup>1</sup>

---

<sup>1</sup> Criminal Code of Georgia, adopted Sept. 8, 1999, last amended Jan. 13, 2022, consolidated versions (July 15, 2021 - Nov. 2, 2021), art. 314, <https://perma.cc/7NRX-4PX4>.

The code prescribes imprisonment for a period of eight to 12 years as a punishment for committing this crime.<sup>2</sup> Imprisonment for 12 to 20 years must be imposed for espionage committed during war or armed conflict or that has seriously affected the interests of Georgia.<sup>3</sup>

The content of information that can be classified as a state secret is defined by the Law on State Secrets.<sup>4</sup> It may include any

information available in the areas of defence, economy, foreign relations, intelligence, national security and law enforcement, the disclosure or loss of which can prejudice the sovereignty, constitutional order, political and economic interests of Georgia or of any party to the treaties and international agreements of Georgia and which, according to this law and/or treaties and international agreements of Georgia, is predetermined as classified or deemed to be a state secret and subject to state protection.<sup>5</sup>

Article 2 of the law specifically states, “[t]he legislation of Georgia on State Secrets does not apply to the protection of commercial or bank secrets, of financial, scientific-technological, or invention-related secrets or other secret information unless such information is classified as a state secret.”<sup>6</sup>

Under the Criminal Code, persons who learn of a state secret because of their office or in confidence under specific circumstances must not divulge the secret to unauthorized persons to the state’s detriment. Violators will be punished by imprisonment for eight to 15 years, with deprivation of the right to hold an office or to carry out certain activities for up to three years.<sup>7</sup>

The General Administrative Code of Georgia defines what constitutes a commercial secret.<sup>8</sup> According to the code, a commercial secret is considered any “information on a plan, formula, process, or means having a commercial value or any other information used for the manufacturing, preparing, processing of goods” or the rendering of services, or which is a novelty or a significant result of technical activity, and other information that may hurt competitiveness if disclosed.<sup>9</sup>

Article 27 also prescribes specific actions for determining whether information can be considered a commercial secret. The content and volume of information containing commercial secrets and the rules for its protection must be established by the entrepreneur. If a public institution does not consider information to be a commercial secret when it is submitted to it, the institution must

---

<sup>2</sup> Id.

<sup>3</sup> Id.

<sup>4</sup> Law of Georgia on State Secrets, No. 3099-IIS, adopted Feb. 15, 2015, last amended July 15, 2020, consolidated versions (July 8, 2015 – June 27, 2018), <https://perma.cc/7RG9-F36R>.

<sup>5</sup> Id. art. 1, para. 1.

<sup>6</sup> Id. art. 2.

<sup>7</sup> Criminal Code art. 313.

<sup>8</sup> General Administrative Code of Georgia, N 2181-IIS, June 25, 1999, updated in 2004, <https://perma.cc/9QKQ-WMJ2>.

<sup>9</sup> Id. art. 27(2), para. 1.

make the information open and immediately notify the person who submitted it.<sup>10</sup> Any individual may appeal a decision to consider information to be a commercial secret to a superior administrative body and to a court as determined by the procedural law of Georgia.<sup>11</sup>

Article 273 of the code defines a professional secret. Information about personal data or a commercial secret of others that has become known to a person while performing professional duties is considered a professional secret.<sup>12</sup>

There is no special trade secret law in Georgia, but the protection of trade secrets is covered by the Law of Georgia on Competition and by the Civil Code.

The Law on Competition prohibits illegal receipt, distribution, or usage of information containing commercial secrets.<sup>13</sup> Any entrepreneurial activity or conduct that may lead to acquisition, use, and disclosure of undisclosed information without the consent of its lawful owner is an act of unfair competition.<sup>14</sup>

The Civil Code states an entrepreneur who possesses a trade secret (know-how) consisting of “technological, organizational, or commercial information of extraordinary importance, as evidenced by the necessary and adequate measures taken for keeping it secret,” has an exclusive right to the information. “An exclusive right to know-how is protected under the Civil Code and other legislative acts on industrial property.”<sup>15</sup>

The code prohibits persons who become aware of a trade secret within the scope of their work and in confidence from disclosing it unless the disclosure is required by law or permitted by the possessor of the secret. The duty of nondisclosure survives the end of contractual relations.<sup>16</sup>

The Civil Code obligates confidentiality in the banking sector.<sup>17</sup> Article 863 of the code provides that a credit institution must keep the facts “relating to an account and other facts known to it during business relations with the account holder” confidential except as provided by law or “when the matter concerns ordinary banking information that is not prejudicial to the account holder’s interests.”<sup>18</sup>

---

<sup>10</sup> Id. para. 3.

<sup>11</sup> Id. para. 4.

<sup>12</sup> Id. art. 273.

<sup>13</sup> Law of Georgia on Competition, No. 2159 of Mar. 21, 2014, last amended Mar. 29, 2022, consolidated versions (Sept. 16, 2020 – Sept. 18, 2020), art. 11(3), paras. 1, 2[2], <https://perma.cc/4NDK-EYRC>.

<sup>14</sup> Id. arts. 11(3), 18.

<sup>15</sup> Civil Code of Georgia, adopted Feb. 19, 1999, last amended Mar. 29, 2022, consolidated versions (Aug. 2, 2021 – Dec. 28, 2021), art. 1105, paras. 1, 2, <https://perma.cc/7LP3-PC94>.

<sup>16</sup> Id. art. 714, paras. 1, 2.

<sup>17</sup> Id. art. 863, paras. 1, 2.

<sup>18</sup> Id.

The Law of Georgia on the Securities Market defines “insider information” as “non-public, material information” related to one or more enterprises or their publicly held securities.<sup>19</sup>

## II. Prosecution of Fraudulent Activities of Private Corporations

Corporate registration is mandatory in Georgia and is regulated by the Law on Entrepreneurs.<sup>20</sup> Violating the registration rules or conducting business without registering or obtaining proper licenses is considered illegal entrepreneurship.<sup>21</sup> A business entity must be registered with the National Agency of Public Registry, while a legal entity must be registered with the Ministry of Justice.<sup>22</sup>

Under Georgia’s Criminal Code, conducting an illegal entrepreneurial activity without registration, a permit or license, or in violation of the permit or license terms, which results in substantial damage or “receipt of large income,” is punishable by a fine or house arrest for a period of six months to two years or by imprisonment for one to three years. Imprisonment for three to five years will be imposed if the same act is committed jointly by more than one person or by a person previously convicted for this type of offense.<sup>23</sup> The code requires criminal convictions to be based on proof of guilt beyond a reasonable doubt.<sup>24</sup>

### A. Banking Secrets

The Law of Georgia on Commercial Bank Activities differentiates banking secrets as a special type of commercial secret.<sup>25</sup> Article 17 of the law defines information on transactions and accounts of legal entities and individuals as banking secrets.<sup>26</sup>

Under the law, no one has the right to allow anyone to access, disclose, and disseminate such information or use it for personal gain.<sup>27</sup>

---

<sup>19</sup> Law of Georgia on Securities Market, adopted May 13, 1999, last amended Dec. 30, 2021, consolidated versions (July 14, 2020 – July 15, 2020), art. 45, para. 1, <https://perma.cc/UDU8-3MMA>.

<sup>20</sup> Law of Georgia on Entrepreneurs of Oct. 28, 1994, last amended May 29, 2017, art. 2, <https://perma.cc/JMD8-U8QH>.

<sup>21</sup> Id. arts. 2(2), 14(2).

<sup>22</sup> Id. and Civil Code arts. 31-33.

<sup>23</sup> Criminal Code art. 192.

<sup>24</sup> Id. art. 13.

<sup>25</sup> Law of Georgia on Commercial Bank Activities, adopted Mar. 21, 1996, last amended Dec. 30, 2021, consolidated versions (Dec. 20, 2019 – Sept. 19, 2020), <https://perma.cc/3XHC-K6YZ>.

<sup>26</sup> Id. art. 17.

<sup>27</sup> Id.

The same obligation is provided in article 863 of the Civil Code.<sup>28</sup> However, there are exceptions. The law allows for the disclosure of information containing commercial secrets to law enforcement agencies but only by a court decision.<sup>29</sup>

## **B. Commercial Secrets**

The Criminal Code of Georgia prescribes punishment for the illegal collection, transfer, disclosure, or use of inside information or information containing commercial or bank secrets.<sup>30</sup> This crime is punishable by imprisonment for a period of two to four years, with or without a ban on holding certain positions or engaging in certain activities for up to three years, fines or corrective labor.

The same act, if committed for mercenary purposes or with other personal motives, “by a group of persons with preliminary agreement,” or by abusing one’s official position, “which has resulted in considerable damage,” is punishable by a fine or imprisonment for four to seven years, with or without a ban on holding certain positions or engaging in certain activities for up to five years.<sup>31</sup>

## **C. Customs Violations**

The Customs Code of Georgia details sanctions for customs fraud.<sup>32</sup>

Article 167 of the code deals with attempts to reduce the amount of import duty by submitting falsified or intentionally incorrect data.<sup>33</sup> In such cases, the penalties range from 40% to 200% of the amount of the attempted reduction in import duty.

Article 168 of the code deals with illegal export or import of goods.<sup>34</sup> These violations are punishable by fines, confiscation of the goods, confiscation of the means of transport, or a combination of these penalties.

## **III. Examples of Convictions for Violations of Export Controls or Economic Espionage**

There are no publicly available reports of specific cases related to export control violations or economic espionage. However, a watchdog organization has raised concerns recently about the rules allowing anonymous company ownership. In 2021, Transparency International Georgia published a special report underlining an issue related to anonymous ownership of major

---

<sup>28</sup> Id.; Civil Code art. 863.

<sup>29</sup> Law of Georgia on Commercial Bank Activities, arts. 17, para. 2, 17(1).

<sup>30</sup> Criminal Code art. 202, para. 1.

<sup>31</sup> Id. para. 2.

<sup>32</sup> Customs Code of Georgia, adopted July 14, 2020, last amended Dec. 29, 2021, consolidated versions (July 15, 2020 – Sept. 30, 2020), <https://perma.cc/3MLV-822W>.

<sup>33</sup> Id. art. 167.

<sup>34</sup> Id. art. 168.

enterprises in Georgia.<sup>35</sup> The report stresses the need to shed light on the beneficial owners of shell companies, who procure and manage major Georgian assets through these offshore companies. This type of company is allegedly used for political ends. The report raises questions about the potential use of anonymous companies for corrupt or malicious purposes.<sup>36</sup>

---

<sup>35</sup> Transparency Int'l Georgia, *The Problem of Anonymous Company Ownership – Why Georgia Needs a Register of Beneficial Owners* (Dec. 8, 2021), <https://perma.cc/2ESE-KGMH>.

<sup>36</sup> *Id.*

# India

Tariq Ahmad  
Foreign Law Specialist

**SUMMARY** India does not have a stand-alone law that deals with economic espionage, nor does it have specific criminal offenses dedicated to economic espionage against foreign-government-controlled technology or foreign companies. India does have specific statutes regulating corporations, banks, and its import-export system that include offenses related to fraudulent incorporation and documentation.

## I. Economic Espionage Legislation

There is no dedicated economic espionage or trade secrets law in India. Trade secrets are mostly dealt with civilly through contract law.<sup>1</sup> Nor are there specific criminal offense laws dedicated to economic espionage against foreign-government-controlled technology or foreign companies. Rather, India's main anti-espionage law is a domestic official secrets act.<sup>2</sup> It is worth noting that, apart from the specific fraud provisions in the specialized laws discussed below, India's Penal Code contains a number of fraud-related offenses, including chapter XVIII, "Of Offences Relating to Documents and to Property Marks," which includes offenses such as forgery (section 463) and making a false document (section 464), and sections 415–420, which address various crimes involving "cheating,"<sup>3</sup> among other crimes.

## II. Evidentiary Legal Threshold and Penalty

In general, in criminal proceedings, the standard of proof required for prosecution is proof beyond a reasonable doubt.<sup>4</sup>

### A. Filing Fraudulent Corporate Registration Information

India's main companies law is the Companies Act, 2013.<sup>5</sup> The law has a number of provisions on committing fraud, making fraudulent statements, and submitting fraudulent evidence. Section 7 of the Act deals with the incorporation of companies, and section 7(5)–(6) deals with fraud related to incorporation:

---

<sup>1</sup> Dhruvi Lunker & S.D. Isiri, *Protecting Trade Secrets: Need for Law Amidst Growing e-Espionage*, NLIU IPR Law Journal's Blog on Intellectual Property and Technology Law (Sept. 22, 2020), <https://perma.cc/55EF-7XAJ>; Ravindra Chhaba & Shyam Sunder Chhaba, *Inadequacy of the Trade Secret's Protection Laws in India and Legal Regime Existing in U.S.* (Manupatra, undated), <https://perma.cc/49U6-MQQB>.

<sup>2</sup> Official Secrets Act, 1923, <https://perma.cc/97XC-PGJL>.

<sup>3</sup> Indian Penal Code, Act No. 45 of 1860, <https://perma.cc/6LND-HQLK>.

<sup>4</sup> Maharashtra State Board of Secondary and Higher Secondary Education v. K.S. Gandhi and Ors. (1991) 2 SCC 716, ¶ 26, SCC Online Database (by subscription).

<sup>5</sup> Companies Act, 2013, <https://perma.cc/3GJ5-85L6>.

(5) If any person furnishes any false or incorrect particulars of any information or suppresses any material information, of which he is aware in any of the documents filed with the Registrar in relation to the registration of a company, he shall be liable for action under section 447.

(6) Without prejudice to the provisions of sub-section (5) where, at any time after the incorporation of a company, it is proved that the company has been got [sic] incorporated by furnishing any false or incorrect information or representation or by suppressing any material fact or information in any of the documents or declaration filed or made for incorporating such company, or by any fraudulent action, the promoters, the persons named as the first directors of the company and the persons making declaration under clause (b) of sub-section(1) shall each be liable for action under section 447.<sup>6</sup>

Section 447 deals with the punishment of fraud:

447. Punishment for fraud. – Without prejudice to any liability including repayment of any debt under this Act or any other law for the time being in force, any person who is found to be guilty of fraud, [involving an amount of at least ten lakh rupees or one per cent. of the turnover of the company, whichever is lower] shall be punishable with imprisonment for a term which shall not be less than six months but which may extend to ten years and shall also be liable to fine which shall not be less than the amount involved in the fraud, but which may extend to three times the amount involved in the fraud:

Provided that where the fraud in question involves public interest, the term of imprisonment shall not be less than three years.

[Provided further that where the fraud involves an amount less than ten lakh rupees or one per cent. of the turnover of the company, whichever is lower, and does not involve public interest, any person guilty of such fraud shall be punishable with imprisonment for a term which may extend to five years or with fine which may extend to [fifty lakh rupees] or with both.]

Explanation. – For the purposes of this section –

- (i) “fraud”, in relation to affairs of a company or any body corporate, includes any act, omission, concealment of any fact or abuse of position committed by any person or any other person with the connivance in any manner, with intent to deceive, to gain undue advantage from, or to injure the interests of, the company or its shareholders or its creditors or any other person, whether or not there is any wrongful gain or wrongful loss;
- (ii) “wrongful gain” means the gain by unlawful means of property to which the person gaining is not legally entitled;
- (iii) “wrongful loss” means the loss by unlawful means of property to which the person losing is legally entitled.<sup>7</sup>

The same punishment is also provided for giving a false statement:

---

<sup>6</sup> Id. § 7(5)-(6).

<sup>7</sup> Id. § 447 (citations omitted).

448. Punishment for false statement. – Save as otherwise provided in this Act, if in any return, report, certificate, financial statement, prospectus, statement or other document required by, or for, the purposes of any of the provisions of this Act or the rules made thereunder, any person makes a statement, –

- (a) which is false in any material particulars, knowing it to be false; or
- (b) which omits any material fact, knowing it to be material,

he shall be liable under section 447.<sup>8</sup>

## B. Filing Fraudulent Import-Export Documentation

India's import and export system is governed by the Foreign Trade (Development & Regulation) Act, 1992,<sup>9</sup> the Foreign Trade Policy,<sup>10</sup> and the Import, Export and SCOMET Policy.<sup>11</sup> Section 11(3) of the 1992 Act stipulates as follows:

(3) Where any person signs or uses, or causes to be made, signed or used, any declaration, statement or document submitted to the Director General or any officer authorised by him under this Act, knowing or having reason to believe that such declaration, statement or document is forged or tampered with or false in any material particular, he shall be liable to a penalty of not less than ten thousand rupees or more than five times the value of the goods or services or technology in respect of which such declaration, statement or document had been submitted, whichever is more.<sup>12</sup>

India maintains a list of items controlled for export<sup>13</sup> under its SCOMET Policy,<sup>14</sup> called the Special Chemicals, Organism, Material, Equipment and Technologies (SCOMET) list.<sup>15</sup> This list is found in Appendix 3 (SCOMET Items) to Schedule- 2 of the ITC (HS) Classification of Export and Import Items, 2018.<sup>16</sup> The ITC-HS Codes, or Indian Trade Clarification, which is based on the Harmonized System of Coding, "was adopted in India for import-export operations."<sup>17</sup> The SCOMET list "covers items which have dual-uses"<sup>18</sup> to "ensure that sensitive items do not fall

---

<sup>8</sup> Id. § 448.

<sup>9</sup> Foreign Trade (Development and Regulation) Act, 1992, <https://perma.cc/NJN2-M5PM>.

<sup>10</sup> *Foreign Trade Policy*, Directorate General of Foreign Trade (DGFT), Ministry of Commerce and Industry, <https://perma.cc/N2YF-L6XD>.

<sup>11</sup> *Import, Export and SCOMET Policy*, DGFT, Ministry of Commerce and Industry, <https://perma.cc/TC22-B7YG>.

<sup>12</sup> Foreign Trade (Development and Regulation) Act, 1992, § 11(3).

<sup>13</sup> DGFT, *India's Export Control System: SCOMET Guidelines and Procedures* (undated), <https://perma.cc/9KP5-EGMQ>.

<sup>14</sup> Suresh Varanasi & Sagnik Chatterjee, *India's Export Control – The SCOMET List*, AZB & Partners (Oct. 3, 2019), <https://perma.cc/5JHX-AXDX>.

<sup>15</sup> Janarth Visvanathan, *Export Control in India: The 'SCOMET' List*, IKIGAI Law (Mar. 26, 2021), <https://perma.cc/NF42-XSYK>.

<sup>16</sup> Appendix 3 [List of SCOMET Items] to Schedule- 2 of ITC (HS) Classification of Export and Import Items, 2018, <https://perma.cc/ZT2S-QSMC>.

<sup>17</sup> *ITC HS Code List or India Harmonised Code System Code*, DGFT, <https://perma.cc/63U2-6N72>.

<sup>18</sup> Visvanathan, *supra* note 15.

into the hands of non-state actors.”<sup>19</sup> Export of SCOMET items are either prohibited or permitted subject to authorization. The list was first notified in 1992 and “has been amended multiple times to align it with the global practices. The SCOMET list classifies items into 9 distinct categories.”<sup>20</sup>

Penalties for exporting SCOMET items without authorization are provided for in chapter IV A of the 1992 Act, which includes provisions on the suspension and cancelation of licenses and other offenses and penalties.<sup>21</sup> Section 14E directly refers to and applies the offenses and penalties of the Weapons of Mass Destruction and Their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005.<sup>22</sup> Section 18 of the 2005 Act provides a penalty for using false or making forged documents:

18. Penalty for using false or making forged documents, etc. – Where any person signs or uses, or causes to be signed or used, any declaration, statement or document submitted to the competent authority knowing or having reason to believe that such declaration, statement or document is forged or tampered with or is false in any material particular, and relates to items notified under this Act or any other relevant Act, including those related to relevant activity, he shall be punishable with fine which shall not be less than five lakh rupees or five times the value of the materials, equipment, technology or services, whichever is more.<sup>23</sup>

India’s Customs Act, 1962 also has a provision on submitting false customs declarations or documents:

132. False declaration, false documents, etc. – Whoever makes, signs or uses, or causes to be made, signed or used, any declaration, statement or document in the transaction of any business relating to the customs, knowing or having reason to believe that such declaration, statement or document is false in any material particular, shall be punishable with imprisonment for a term which may extend to [two years], or with fine, or with both.<sup>24</sup>

### C. Filing False Customer Information with Banking Entities

The Banking Regulation Act, 1949 is the main law that regulates all banking firms in India.<sup>25</sup> Section 46 provides for penalties, with section 46(1) stating as follows:

46. Penalties. – (1) Whoever in any return, balance-sheet or other document [or in any information required or furnished] by or under or for the purposes of any provision of this Act, wilfully makes a statement which is false in any material particular, knowing it to be

---

<sup>19</sup> Upendra Nath Sharma & Kartik Jain, *Financial Crime in India: Overview*, Practical Law Company (Dec. 1, 2020), <https://perma.cc/3VCN-AGVS>.

<sup>20</sup> Visvanathan, *supra* note 15.

<sup>21</sup> Foreign Trade (Development and Regulation) Act, 1992, §§ 14D & 14E.

<sup>22</sup> Weapons of Mass Destruction and Their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, <https://perma.cc/23EP-AQT9>.

<sup>23</sup> *Id.* § 46(1) (citation omitted).

<sup>24</sup> Customs Act, 1962, § 132 (citation omitted), <https://perma.cc/W3M5-YHZW>.

<sup>25</sup> Banking Regulation Act, 1949, <https://perma.cc/6GWP-WW2V>.

false, or wilfully omits to make a material statement, shall be punishable with imprisonment for a term which may extend to three years and [or with fine, which may extend to one crore rupees or with both].<sup>26</sup>

### III. Past Convictions for Economic Espionage or Export-Control Violations

Very little information was located on convictions for economic espionage of foreign-controlled technology and export-control violations. Reports mainly cover growing concern over domestic corporate espionage between competing firms or companies in recent years<sup>27</sup> or the targeting of government ministries.<sup>28</sup>

A Directorate of Revenue Intelligence report highlights instances of “enforcement of strategic trade controls in 2019–20,” where missile-related “substances and equipment controlled under the SCOMET List were being transported between two foreign countries, with India being used as a transit point.”<sup>29</sup> Another seizure was highlighted in the 2020–21 report of a case involving titanium forgings “which could be used in the manufacture of inter-continental ballistic missiles” and were transiting through India. The consignment was “intercepted, identified, and seized as per the law.”<sup>30</sup>

---

<sup>26</sup> Id. § 46(1) (citations omitted).

<sup>27</sup> Megha Bahree, *Companies of Several Indian Billionaires Embroiled in a Case of Corporate Espionage*, Forbes (Feb. 23, 2015), <https://perma.cc/549B-DZQN>.

<sup>28</sup> Dev Chatterjee & Ishita Ayan Dutt, *Corporate Espionage Is Not New to India Inc, Say CEOs*, Business Standard (last updated Feb. 21, 2015), <https://perma.cc/FPP6-NUDX>.

<sup>29</sup> Directorate of Revenue Intelligence (DRI), *Smuggling in India Report 2019–2020*, 24–25 (2020), <https://perma.cc/AL7A-RSFN>.

<sup>30</sup> Directorate of Revenue Intelligence (DRI), *Smuggling in India Report 2020–2021*, 41 (2021), <https://www.dri.nic.in/writereaddata/smugglinginindiareportfor2021/files/basic-html/page1.html>.

# Israel

*Ruth Levush*  
*Senior Foreign Law Specialist*

**SUMMARY** In the absence of special legislation on economic espionage, unauthorized disclosure and transfer of trade secrets is regulated under a number of laws that subject offenders to criminal penalties.

Fraudulent filings of corporate registration documents, import and export documentation, and customer information to banking entities constitute criminal offenses subjecting offenders to imprisonment and/or fines depending on the circumstances, with increased penalties for violation of defense export controls.

Violation of export controls may result in either criminal penalties or civil fines. As a rule, criminal conviction under Israeli law requires the prosecution to prove the allegations against a defendant beyond a reasonable doubt. Civil fines may be issued by authorized officials based on their discretion and appear to require a lower evidentiary threshold.

Israeli courts have adjudicated and convicted a number of defendants in offenses related to economic espionage and fraudulent filing of export and import documentation.

## I. Economic Espionage Legislation

Israeli law does not have special legislation on economic espionage. Current legislation addresses offenses of business espionage, as well as offenses of espionage involving disclosure of information to enemy states or disclosure with intent to harm the state. Special provisions apply to export controls.

### A. Industrial Espionage

Industrial espionage relates to “the covert, and sometimes illegal, practice of investigating competitors to gain a business advantage. The target of an investigation might be a trade secret, such as a proprietary product specification or formula, or information about business plans.”<sup>1</sup>

Under Israel’s Trade Wrongs Law, 5759-1999, victims of theft of trade secrets may be granted compensation.<sup>2</sup> A person who “receives anything fraudulently” may be held liable and be

---

<sup>1</sup> *Definition: Industrial Espionage*, TechTarget, <https://perma.cc/X8Q2-C5BW>.

<sup>2</sup> Trade Wrongs Law, 5759-1999, § 415, SH 5759 No. 1709 p. 146, available via Takdin Legal Database, <https://perma.cc/H3RD-MJ69> (in Hebrew, by subscription).

sentenced to imprisonment for three to five years, depending on the existence of aggravated circumstances.<sup>3</sup>

Additionally, the Penal Law provides that the disclosure of confidential information to a person in the course of exercising that person's profession or a craft is punishable by imprisonment for a period of six months.<sup>4</sup>

This provision, however, does not appear to address all the ways in which industrial espionage can be carried out. In the virtual world, industrial espionage may be performed by other actors through unauthorized intrusions into a company's computer from a remote computer, the use of Trojan horses, key-loggers (software or physical components that record the user's keyboard typing), screenshots (screen-capturing), and other types of malware. Nor does the provision apply to all potential participants in economic espionage such as spyware developers, espionage operators, or persons who order the espionage.<sup>5</sup>

Criminal prosecution involving online industrial espionage may therefore be based on the violation of relevant provisions in existing legislation on computer offenses, wiretapping, privacy protection, fraud, and receipt of property obtained by committing a crime under the Penal Law.<sup>6</sup>

## **B. Economic Espionage**

US law defines economic espionage as the commission of various activities such as stealing, unauthorized taking, copying, and photographing trade secrets with the intent to benefit a foreign government, foreign instrumentality, or foreign agent.<sup>7</sup> Similar activities may constitute offenses regarding state security, foreign relations, and official secrets under chapter F of Israel's Penal Law.<sup>8</sup>

According to the Penal Law, the collection, preparation, or provision of information with the intent to harm the security of the state is punishable by imprisonment for varying terms extending from five years to life depending on the type of activity involved.<sup>9</sup>

---

<sup>3</sup> Penal Law 5737-1977, SH 5737 No. 864 p. 322, as amended, §§ 112, 113, Takdin, <https://perma.cc/RWA6-B7YZ> (in Hebrew, by subscription).

<sup>4</sup> Id. § 496.

<sup>5</sup> Haim Vismanski, *Missing: Penal Prohibition for Business Espionage*, law.co.il (Aug. 4, 2006), <https://perma.cc/L3HP-REAQ> (in Hebrew).

<sup>6</sup> Id.

<sup>7</sup> For the definition of economic espionage under US law, see the Economic Espionage Act of 1996, § 1831, <https://perma.cc/XSF7-FUF7>.

<sup>8</sup> Penal Law Ch. 7.

<sup>9</sup> Penal Law §§ 112, 113.

## II. Evidentiary Legal Threshold and Penalty

### A. Filing Fraudulent Corporate Registration Information

The filing of corporate registration is regulated by the Companies Law, 5759-1999.<sup>10</sup>

In accordance with section 423 of the Penal Law, a founder, director, member, or employee of a corporation, who registers, or causes to be registered, a false detail in the corporation's documents, with intent to defraud, or who has refrained from listing an item that must be registered, with intent to defraud, is liable to five years imprisonment.<sup>11</sup>

Imprisonment for three years and a fine may be imposed for failure to disclose information by a senior official in a corporation in which the public has an interest, as defined by the Penal Law.<sup>12</sup>

As a rule, Israeli law requires proof beyond a reasonable doubt to convict someone of an offense.<sup>13</sup>

### B. Filing Fraudulent Import/Export Documentation

#### 1. *Fraudulent Import/Export Documentation to Custom Authorities*

##### a. Criminal Penalty

Two-year imprisonment or a fine may be imposed on a person who submits an import or export declaration or a document containing a statement that is false or incorrect in a particular detail. The evidentiary threshold for a criminal conviction appears to be proof beyond reasonable doubt.<sup>14</sup>

##### b. Civil Fines

An authorized official of the Ministry of the Treasury (MOT) may issue an administrative penalty of NIS 2,500 (about US\$734.50) to a person who submits a declaration containing incorrect details.<sup>15</sup>

The submission of a declaration containing incorrect details by an importer or exporter, as defined by the Customs Ordinance, may be subject to a fine at a rate of 10% of the difference in import taxes generated, or NIS 5,000 (about US\$1469.00) – whichever is higher – unless the official is convinced that the importer or exporter has given the customs agent all the documents and details

---

<sup>10</sup> Companies Law, 5759-1999, SH 5759 No. 1711 p. 189.

<sup>11</sup> Penal Law § 423.

<sup>12</sup> Id. § 424A.

<sup>13</sup> Id. § 34 V.

<sup>14</sup> The Customs Ordinance (New Version) § 212(a), 3 Dine Medinat Israel (New Version) 39, as amended, available via Nevo Legal Database, <https://perma.cc/G42R-QM2P> (in Hebrew, by subscription).

<sup>15</sup> Id. § 223B(a).

that are required for the purpose of submitting a declaration on their behalf.<sup>16</sup> Submission of a declaration containing incorrect items by a customs agent may be punishable by a fine at a rate of 1% of the difference in import taxes generated, but not more than NIS 5,000 (about US\$ 1469.00), and not less than NIS 500 (about US\$146.90) unless the official is convinced that the wrong details have been provided to the customs agent by the importer or the exporter.<sup>17</sup> A fine of NIS 150 (about US\$44.07) may be imposed on a customs agent if the difference in import taxes generated for a single export declaration does not exceed NIS 500 (about US\$146.90) under conditions enumerated by the Customs Ordinance.<sup>18</sup>

The decision to impose a civil fine is based on the MOT official's "reasonable basis to assume" that a person has violated the filing requirements. The official must inform the person of the intention to impose a fine. The offender is entitled to submit an objection against the determination of liability and the amount of the fine in writing within 30 days of the date of delivery of the notice, which may be extended by an additional period not exceeding 30 days.<sup>19</sup>

## 2. *Fraudulent Documentation of Export of Defense Equipment*

### a. Documentation Requirements

The export of defense equipment, transfer of know-how, and provision of defense services (regulated activities) require a license and annual reporting on activities requiring licensing.<sup>20</sup>

The license and annual reporting requirements also apply to the transfer of regulated dual-use items to areas under the control of the Palestinian Authority (PA).<sup>21</sup> Israeli residents or corporations who engage in brokering regulated activities between foreign entities are subject to similar requirements.<sup>22</sup>

Israeli citizens, residents, and corporations are further prohibited from engaging in brokering activities between foreign entities in violation of a resolution of the Security Council of the United Nations forbidding or limiting the transfer of combat equipment or missile equipment to named entities.<sup>23</sup>

---

<sup>16</sup> Id. § 223B(b).

<sup>17</sup> Id. § 223B(c).

<sup>18</sup> Id. § 223B(d).

<sup>19</sup> Id. §§ 223C, 223D.

<sup>20</sup> Defense Export Control Law, 5767-2007, SH 5767 No. 2105 p. 398, § 6(b), Nevo, <https://perma.cc/CFF2-JQTN> (in Hebrew, by subscription), unofficial English translation at Ministry of Defense website (MOD), <https://perma.cc/9XQQ-TFYV>.

<sup>21</sup> Defense Export Control Law § 20.

<sup>22</sup> Id. § 21.

<sup>23</sup> Id. § 22; see Notice of the United Nations Security Council Resolutions Prohibiting or Restricting Transfer of Combat or Missile Equipment, in Accordance with the Defense Export Control Law, 5767-2007, MOD, <https://perma.cc/E23K-7DFH> (in Hebrew).

Under the Defense Export Control (Licensing) Regulations, 5768-2008, an application for a license must include:

Details of the equipment, knowledge or service subject to the application, its source, manufacturer, classification, customer and destination country, **end user and end use**, information about agents or intermediate users, information about firm financing, information about manufacturers, marketers and contractors, details of equipment, components, knowledge or service originating from a foreign country and information on the need for foreign government approvals for further export, declarations regarding missile equipment, declarations regarding encryption, manufacturer's approval or approval of the ministry's authorized entity if the equipment is Israel Defense Forces surplus, additional statements as appropriate, information about the purpose of the transaction, information about compatibility between the application for an export license and a marketing license granted, copy of contracts or orders or information about them, all as required on the form . . . .

The applicant shall notify the division in writing, immediately, of any change in the application data submitted [if] a decision has not yet been made. Notification of a change in details or a change in the application data after a decision is made on the application will be reported to the Authority within 30 days.<sup>24</sup>

b. Penalties

i. Criminal Penalty

The export of defense equipment in the absence of a license, or in violation of conditions enumerated in a license, is punishable by three years of imprisonment or a fine at a rate of three times of the amount prescribed in the Penal Law (226,000 NIS, about US \$66,145), or five years of imprisonment, or a fine at a rate of 50 times the amount prescribed in the Penal Law, in cases of aggravating circumstances specified by the Law.<sup>25</sup>

ii. Civil Fines

The Defense Export Control Law also authorizes the licensing authority, upon "reasonable grounds to assume that an act or a failure to act, that is set out as an offense . . . has occurred . . . to impose a civil fine in the amount of 15% of the fine set out . . . upon the person who commits the act or who fails to act."<sup>26</sup>

Therefore, for the purpose of a civil fine, a "reasonable grounds" level of proof is sufficient and does not require the level of proof beyond reasonable doubt that is required for a criminal conviction.

---

<sup>24</sup> Defense Export Control (Licensing) Regulations, 5778-2008, KT 6778 No. 6646 p.460, as amended, §§ 3, 7, Takdin, <https://perma.cc/6EYW-545V> (in Hebrew; translation and emphasis by author).

<sup>25</sup> Defense Export Control Law §§ 32, 33.

<sup>26</sup> Id. §§ 35-43.

### iii. Liability of Corporate Officers

The Law requires corporation officers to supervise and do anything possible to prevent violation of licensing requirements by the corporation or by its employees (duty of care) and subjects offenders to fines.<sup>27</sup>

When an offense has been committed by a corporation or by its employees, the burden of proof that he or she has not violated the duty of care is on the corporate officer.<sup>28</sup>

### C. Filing False Customer Information to Banking Entities

The Penal Law defines forgery, among other things, as “making a document presumed to be that which it is not, and may be misleading.”<sup>29</sup> The forging of a document containing information about a person or corporation, with intent to defraud, is punishable by imprisonment for three years.<sup>30</sup>

The registration of a false detail or the omission to list an item required to be registered in a corporation's document, by a founder, director, member, or clerk of a corporation, with intent to defraud, or the omission of listing an item required for registration, with intent to defraud, is punishable by imprisonment for five years.<sup>31</sup>

Banking entities are subject to additional identification requirements under the Money Laundering Prohibition Law, 5760-2000<sup>32</sup> and the Money Laundering Prohibition Order (Obligations to Identify, Report and Manage Registrations of Service Providers in Financial Assets and Credit Service Providers to Prevent Money Laundering and Terrorist Financing), 5778-2018.<sup>33</sup>

## III. Examples of Convictions of Violations of Export Controls or Economic Espionage

### A. Submission of Import or Export Documents that are Fraudulent or Containing False Items

On Dec. 8, 2019, the Be'er-Sheva Magistrate's Court sentenced a company owner to 30 months in prison, a lengthy probation period, and a fine of NIS 270,000 (about US\$ 78,945), for committing VAT and customs offenses involving imports from China. Charges against the defendant

---

<sup>27</sup> Id. § 34.

<sup>28</sup> Id.

<sup>29</sup> Id. § 414.

<sup>30</sup> Id. § 419.

<sup>31</sup> Id. §§ 418-423.

<sup>32</sup> Money Laundering Prohibition Law, 5760-2000, SH 5760 No. 1753 p. 293, as amended, Nevo, <https://perma.cc/9DRK-UDRM> (in Hebrew, by subscription).

<sup>33</sup> Money Laundering Prohibition Order (Obligations to Identify, Report and Manage Registrations of Service Providers in Financial Assets and Credit Service Providers to Prevent Money Laundering and Terrorist Financing), 5778-2018, KT 5760 No. 7964 p. 1084, Nevo, <https://perma.cc/5S8Y-DP5R> (in Hebrew, by subscription).

included the unlawful smuggling of toy guns by misleading customs authorities and omitting their inclusion in the import declaration. Toy guns require testing by Israel's Institute of Standards to ensure public safety.<sup>34</sup>

## **B. Export of Defense Equipment**

A July 2, 2018 decision by the Tel Aviv district court rejected an appeal over a civil fine in the amount of 500,000 NIS (about US\$ 146,215) levied against the petitioners for exporting defense equipment in the absence of a license.<sup>35</sup>

The petitioners argued that they had been engaged in the sale of scrap and unusable products purchased from waste dealers, who in turn purchased the products from the IDF or the Ministry of Defense after the scrap and unusable products had been disqualified by military examiners. The petitioners further claimed that the products in question did not constitute fighting or military equipment subject to defense licensing requirements since they had been taken out of use and disqualified by the IDF, and sold by weight.<sup>36</sup>

The court rejected the claim that the products were not subject to defense export controls. Considering the petitioners' long-term and extensive experience in the field, the Court determined that when there was a concern whether certain items needed an export license, in light of the fact that they originated in the IDF, the petitioners had to contact the MOD's Content Committee to examine whether they were regulated items.<sup>37</sup>

## **C. Extradition to the US on Charges of Exporting US Military Spare Parts to Third Parties Through Israel**

On August 28, 2016, the Supreme Court rejected an appeal over the approval of a US request to extradite a person charged with exporting, through others, US military spare parts from the US to Israel, and US military spare parts from Israel to a third country, without permission from the competent authority.<sup>38</sup>

The lower court determined that the appellant's alleged actions would have constituted offenses under Israeli law had the appellant exported from Israel the same defense equipment without authorization from the Israeli Ministry of Defense, and transferred money to Israel to finance the purchase. Under such circumstances, he could be prosecuted in Israel for a number of offenses for which the penalty exceeds one year of imprisonment. These include relevant defense export

---

<sup>34</sup> Crim. C (MS BS) 15265-03-11 National Department for Customs and VAT Tel-Aviv v. Kesem Hayevu Ltd., Nevo, <https://perma.cc/7MQ5-AXNB> (in Hebrew, by subscription).

<sup>35</sup> Adm. (DC TA) 29544-02-16 Arye Cohen v. Ministry of Defense, Nevo, <https://perma.cc/4P3H-CRSN> (in Hebrew, by subscription).

<sup>36</sup> Id. p. 5.

<sup>37</sup> Id. para. 4.3.

<sup>38</sup> Crim. A 7742/15 Anonymous v. Attorney General, State of Israel the Judicial Authority (SIJA), <https://perma.cc/Y7KU-X2C3> (in Hebrew).

control and anti-money laundering legislation as well as violations of the Penal Law's licensing requirements for import and export of firearms.<sup>39</sup>

#### **D. Sale of Materials, Knowledge and Equipment to Iran**

In a decision rendered by Israel's Supreme Court on December 5, 2000, the Court rejected an appeal against a conviction of offenses under chapter F of the Penal Law, involving assisting and attempting to assist an enemy state in its war against Israel, and providing information to the enemy with the intention of harming state security.<sup>40</sup>

The appellant was convicted of engaging in the sale to Iran of materials, knowledge, and equipment for the establishment of chemical warfare plants between 1990-1994. The Court rejected the appellant's contention that he had been unaware of the nature of his actions and of the circumstances, namely that he was dealing in chemical warfare agents with an enemy state. The evidence showed, the Court held, that the appellant had acted while disguising the nature of the transactions and hiding them from the Israeli security forces, using code words and hiding places, and therefore was aware of the seriousness of his actions.<sup>41</sup>

According to the decision, sections 99 and 111 of the Penal Code require an element of special intent, namely, that the perpetrator intends to harm state security and acts with intent to assist the enemy in its war against Israel. The Court held that there was no requirement to prove a mental element of motive. Although the appellant's direct motive and desire to assist the enemy and harm the security of the state were not proven, the appellant understood the severe consequences of his actions, and expected them with a high probability.<sup>42</sup>

#### **E. Unauthorized Transfer of Dual Use Products to the Palestinian Authority**

In a decision rendered by the Supreme Court on Sep. 21, 2015, the Court rejected an appeal against the conditions of imprisonment of a person convicted by the Be'er Sheva district court in the transfer of dual-use products to the Palestinian Authority. Details of the district court decision, however, were classified as "confidential."<sup>43</sup>

---

<sup>39</sup> Id.

<sup>40</sup> Crim. A 6411/98 Manvar v. State of Israel, 55(2) PD 150, Nevo, <https://perma.cc/3Z6H-TTVQ> (in Hebrew, by subscription); A reference to this decision is made in this report even though it preceded the five-year period of review of examples requested, as the relevant Penal Law provisions have not been amended in the period commencing with the date of the decision.

<sup>41</sup> Id. pp. 150-151

<sup>42</sup> Id.

<sup>43</sup> Request 5932/15 Yasin v. State of Israel, SIJA, <https://perma.cc/XB5K-YZ5H>; text in Nevo links to the conviction by the Be'er Sheva district court, indicating the file is confidential, <https://perma.cc/DR8K-XEYY>.

# Kazakhstan

*Peter Roudik*  
*Director of Legal Research*

*Iana Fremer*  
*Legal Information Analyst*

**SUMMARY** There is no comprehensive legislation on commercial espionage in Kazakhstan. If the information in question is classified as a state secret, its gathering and divulging is prosecuted as espionage in cases where this information is transferred to foreign states or foreign organizations. In all other cases, commercial secrets are protected under civil law. Theft of commercial information can be prosecuted as a crime if elements of other criminal actions were present when these acts were committed. Fraudulent activities by banks and private corporations are prosecuted administratively and generally punishable by fines unless substantial damage has been inflicted by these actions. Procedural guidance on handling these cases was issued by Kazakhstan’s Supreme Court in 2020. Information on specific crimes committed in the area of economic espionage and export control is usually classified and not available from public sources.

## I. Economic Espionage Legislation

There is no specific economic espionage legislation in Kazakhstan. The Criminal Code of Kazakhstan defines espionage as transferring information that contains state secrets to a foreign state or foreign organization as well gathering, stealing, and storing such information with the purpose of transferring it later to foreigners. The code prescribes imprisonment for a period of 10 to 15 years, with confiscation of the accused person’s property, as a punishment for commitment of this crime.<sup>1</sup>

The content of information that can be classified as a state secret is defined in the Kazakh Law on State Secrets.<sup>2</sup> It may include any information related to military, economic, scientific, and technical activities, if dissemination of this information has been restricted by the state.<sup>3</sup> A detailed list of economic and scientific information that can be classified is included in article 12 of the Law on State Secrets.<sup>4</sup> Illegal gathering of information that may include state secrets without committing the crime of espionage, i.e., without transferring this information to foreign

---

<sup>1</sup> Criminal Code of the Republic of Kazakhstan, Code of the Republic of Kazakhstan, adopted on July 16, 1997, No. 167, art. 166, <https://perma.cc/PWF6-CYF3> (unofficial translation).

<sup>2</sup> Law of the Republic of Kazakhstan No. 349-1 of Mar. 15, 1999, on State Secrets (last amended July 1, 2021), Adilet.kz, <https://perma.cc/MY8E-KT28>.

<sup>3</sup> Id. art. 1.

<sup>4</sup> Id. art. 12.

states, organizations, or their representatives, is a crime punishable by imprisonment for a period of up to five years, with additional professional restrictions.<sup>5</sup>

Commercial secrets are protected by civil law and the Code of Entrepreneurship, which prohibit illegal receipt, distribution or usage of information containing commercial secrets. What constitutes a commercial secret, how can it be used, who can have access to this information, measures to protect it, and other similar issues should be defined by the business entity. A business entity is not required to provide information containing commercial secrets to government institutions and officials in the course of business registration or government oversight. The government is also prohibited from divulging commercial secrets that become known to the authorities.<sup>6</sup>

A general overview of what should constitute a commercial secret can be found in the Civil Code of Kazakhstan. These are

- production secrets (know-how),
- production technologies,
- management models, and
- methods to increase profits.<sup>7</sup>

The illegal receipt and divulgence of commercial or banking secrets constitutes a crime if the secret information was received by one of the following ways:

- stealing documents,
- blackmailing or bribing people who have access to secrets,
- intercepting the means of communication,
- illegally penetrating a computer system or network, or
- using any special technical means.

This crime is punished by a fine, restrictions on the perpetrator's freedom, correctional labor, or imprisonment for up to one year.<sup>8</sup>

---

<sup>5</sup> Criminal Code art. 185.

<sup>6</sup> Code of Entrepreneurship of the Republic of Kazakhstan, adopted on Oct. 29, 2015, No. 375-V ZRK, art. 28, <https://perma.cc/BHC5-F4KX> (unofficial translation).

<sup>7</sup> Civil Code of the Republic of Kazakhstan, adopted on Dec. 27, 1994, art. 126.1., <https://perma.cc/95AH-XVZV> (in Russian).

<sup>8</sup> Criminal Code art. 200.

## II. Prosecution of Fraudulent Activities of Private Corporations

Corporate registration is mandatory in Kazakhstan and is regulated by the Law on State Registration of Legal Entities.<sup>9</sup> Violating the registration rules or conducting business without registering or obtaining proper licenses is considered illegal entrepreneurship. It constitutes an administrative violation (misdemeanor), which is punished by a fine. The amount of the fine depends on the amount of inflicted damage or the amount of illegally received profits.<sup>10</sup> In a case where these amounts are especially large, the case will be reclassified as a crime and prosecuted under article 190 of the Criminal Code, which provides for increased fines. The same acts, if committed by a group of people or by a person previously convicted for the same violations, are punishable by imprisonment for a period of up to five years.

Similar regulations apply to illegal banking activities.<sup>11</sup> There are comparable regulations imposing penalties for violation of export rules.<sup>12</sup> In addition to imposing fines, the law prescribes the confiscation of illegally exported goods.<sup>13</sup>

## III. Examples of Convictions for Violations of Export Controls or Economic Espionage

Espionage-related cases are investigated by the Kazakhstani National Security Committee. The jurisdiction of the National Security Committee includes export control issues if such cases might affect national security.<sup>14</sup> Information on these cases is usually classified. Details of these cases are not publicized, and court trials are not open to the public. A database of the court decisions was established on the Kazakh Supreme Court website only recently, and it does not appear to be complete. The only source of information on this type of court decision appears to be media reports, which are limited due to the lack of information disclosed by authorities.

In July 2019, the *Wall Street Journal* reported about espionage accusations against a Kazakhstan government advisor who allegedly shared classified information available to him with China's intelligence service. The article speculated that this prosecution demonstrated Kazakhstan's growing concerns about China's influence and understanding of Kazakhstan's vulnerability.<sup>15</sup> Another ongoing espionage investigation was reported on April 19, 2022, by a Kazakh business information web portal, *Capital*. Citing sources on the National Security Committee, it reported

---

<sup>9</sup> Law of the Republic of Kazakhstan No. 2198 of Apr. 17, 1998, on State Registration of Legal Entities, Branches, and Representations, <https://perma.cc/5WK4-NKR9> (in Russian).

<sup>10</sup> Code of Administrative Violations, Law of the Republic of Kazakhstan No. 235-V of July 5, 2014, art. 153, <https://perma.cc/35QG-GQSB> (in Russian).

<sup>11</sup> Code of Administrative Violations art. 155; Criminal Code art. 191.

<sup>12</sup> Code of Administrative Violations arts. 151, 156(5).

<sup>13</sup> Id. art. 153.

<sup>14</sup> Law of the Republic of Kazakhstan No. 2710 of Dec. 21, 1995, on Bodies of National Security in the Republic of Kazakhstan (last amended July 1, 2021), art. 12, <https://perma.cc/N69K-L8EF> (in Russian).

<sup>15</sup> Thomas Grove, *A Spy Case Exposes China's Power Play in Central Asia*, *Wall St. J.*, July 10, 2019, <https://perma.cc/5VH4-ESQ5> (by subscription).

that a group of persons, including a foreign citizen, was arrested in Kazakhstan on suspicions of gathering and divulging information that contained state secrets.<sup>16</sup>

In January 2020, the Supreme Court of Kazakhstan issued a ruling on selected issues related to the application of the laws in economic crime cases. The ruling serves as a procedural guideline for lower courts and defines rules on how to handle such cases, e.g., how to decide whether or not a crime has been completed, what constitutes an attempt to commit a crime, how to calculate the damages, and to what degree fraudulent information can be disregarded.<sup>17</sup>

---

<sup>16</sup> *A Group of Persons Is Detained for Espionage, State Treason, and Disclosing State Secrets*, Capital.kz, Apr. 19, 2022, <https://perma.cc/A7NM-6YXP> (in Russian).

<sup>17</sup> Supreme Court of Kazakhstan, Ruling No. 3 of Jan. 24, 2020, <https://perma.cc/UW26-TW4Y> (in Russian).

# Kyrgyz Republic

*Iana Fremer*  
*Legal Research Analyst*

**SUMMARY** There is no comprehensive legislation on commercial espionage in the Kyrgyz Republic. If the information in question is classified as a state secret, its gathering and divulging is prosecuted as espionage in cases where this information is transferred to foreign states or foreign organizations. In all other cases, commercial secrets are protected under a number of the state laws, including the Law on Trade Secrets, Law on the Protection of the State Secrets, and Law on Export Control criminalizing the passing to foreign countries of economic information that damages the state's economic interests and the unauthorized disclosure of trade secrets.

Fraudulent activities by banks and private corporations are prosecuted administratively and generally punishable by fines unless substantial damage has been inflicted by these actions.

In the Kyrgyz Republic, information on specific crimes committed in the area of economic espionage is usually classified and not available from public sources.

## I. Economic Espionage Legislation

There is no specific economic espionage legislation in the Kyrgyz Republic. Espionage in the Kyrgyz Republic is regulated generally under the Criminal Code.<sup>1</sup>

### A. Criminal Code of Kyrgyzstan

The Criminal Code defines espionage as the collection, theft, transfer, or keeping for the purpose of transfer to a foreign state, a foreign organization, or their representatives information constituting a state secret, and also the transfer or collection of other information under the order of a foreign intelligence service, to the detriment of the external security of the Kyrgyz Republic.<sup>2</sup>

Under Kyrgyz law, only a foreign citizen or stateless person can be convicted of this crime, which is punishable by 12 to 20 years of prison. The code prescribes imprisonment for a period of 10 to 20 years with confiscation of property if these deeds have been committed by a foreign national or a stateless person.<sup>3</sup>

---

<sup>1</sup> Criminal Code of the Kyrgyz Republic (Criminal Code), No. 19, adopted Feb. 2, 2017, last amended May 12, 2021, art. 308, <https://perma.cc/FT7B-JZP9> (in Russian).

<sup>2</sup> Id. art. 308.

<sup>3</sup> Id.

## **B. Law on Protection of the State Secrets**

The content of information that can be classified as a state secret is defined in the Kyrgyz Law on the Protection of the State Secrets.<sup>4</sup> It may include any information related to military, economic, scientific, political, and technical activities, if dissemination of this information has been restricted by the state.<sup>5</sup> A detailed list of the powers of state bodies, local government bodies, and organizations to ensure protection of state secrets is included in article 6 of this law.<sup>6</sup>

In addition, article 28 of the law provides that any individual who discloses classified information, misrepresents the secrecy level of information, or commits other information security violations is subject to criminal, administrative, or disciplinary action.<sup>7</sup>

Under the Criminal Code, a Kyrgyz citizen who discloses state secrets or gives any other assistance to a foreign state or foreign organization to the detriment of the republic's security commits high treason. This crime is punishable by imprisonment for a period of 12 to 20 years with confiscation of property.<sup>8</sup>

Article 317 of the code sets forth punishments for disclosure of information constituting a state or military secret in the absence of high treason or espionage. It includes negligent disclosures. Persons entrusted with such secrets or who learn them through their work can be punished for disclosure by correctional labor, fines, and restriction of freedom for up to six months or imprisonment for up to two years and a ban on holding certain positions or engaging in certain activities for a period of two years.<sup>9</sup>

The transfer of economic, scientific, and technical or other data constituting an official secret or collecting data for the purpose of transferring it to foreign organizations or their representatives by persons with access to this data through their official positions, work, or by any other way is punishable by imprisonment for up to three years.<sup>10</sup> Imprisonment for up to eight years may be imposed on the individuals when the same acts entail large property damage to state or public organizations or cause grave consequences.<sup>11</sup>

## **C. Law on Trade Secrets**

The Law on Trade Secrets defines trade secrets as non-state secret information related to the production, technology, management, financial, and other activities of an economic entity whose

---

<sup>4</sup> Law of the Kyrgyz Republic on the Protection of the State Secrets, No. 210, adopted Nov. 2, 2017, <https://perma.cc/AP77-QHNX> (in Russian).

<sup>5</sup> Id. art. 1, paras. 1-6.

<sup>6</sup> Id. art. 7.

<sup>7</sup> Id. art. 28.

<sup>8</sup> Criminal Code art. 316.

<sup>9</sup> Id. art. 317, para. 1.

<sup>10</sup> Id. art. 318.

<sup>11</sup> Id.

disclosure could be damaging to state interests.<sup>12</sup> The protection of trade secrets covers physical and legal entities of the Kyrgyz Republic and other states engaged in entrepreneurial activities in the Kyrgyz Republic.<sup>13</sup>

Under this law, trade secrets are related to the economic interests and information about various aspects and fields of production and economic, administrative, scientific, technical, financial, or business activities of a business entity.<sup>14</sup> The law declares that transferring information constituting a trade secret to third parties will incur disciplinary, administrative, or criminal liability unless the transfer is authorized by the head of the business entity.<sup>15</sup>

The Criminal Code provides that unlawful disclosure or use of commercial or bank secrets without their holder's consent by a person to which such information is known due to professional or service duties is punishable by fines or up to 100 hours of public service.<sup>16</sup> Criminal prosecution of this type of offense will occur at the request of the aggrieved commercial organization or individual entrepreneur.<sup>17</sup>

The Code of the Administrative Violations of the Kyrgyz Republic also includes provisions prescribing fines for illegal disclosure or use of information constituting a commercial, banking, or other secret without the consent of the owner.<sup>18</sup>

In addition, the Civil Code states that persons who have illegally obtained any information containing official or commercial secrets in violation of a labor contract or a civil law contract, and employees or counterparts who have revealed such information, are obligated to make compensation for the resulting damages.<sup>19</sup>

---

<sup>12</sup> Law on Trade Secrets of the Kyrgyz Republic, No. 27 of Mar. 30, 1998 (in redaction of Laws of the KR of June 26, 1998, No. 83, July 31, 2007, No. 125, June 26, 2009, No. 192), art. 1, para. 1, <https://perma.cc/8SG9-9ZXN> (unofficial translation).

<sup>13</sup> Id. art. 4.

<sup>14</sup> Id. art. 5.

<sup>15</sup> Id. arts. 12(2), 14.

<sup>16</sup> Criminal Code art. 221.

<sup>17</sup> Id.

<sup>18</sup> Code on Administrative Violations of the Kyrgyz Republic (Code on Administrative Violations), No. 128, adopted Oct. 28, 2021, last amended Apr. 22, 2022, art. 323, <https://perma.cc/L8VK-YUB8> (in Russian).

<sup>19</sup> Civil Code of the Kyrgyz Republic, No. 15, adopted May 8, 1996 (amended by the Laws of the Kyrgyz Republic of Apr. 29, 1997, No. 29 and Oct. 15, 1997, No. 76), art. 34, <https://perma.cc/R25H-J8TZ> (unofficial translation).

## II. Prosecution of Fraudulent Activities of Private Corporations

### A. Law on State Registration of Legal Entities

Corporate registration is mandatory in the Kyrgyz Republic and is regulated by the Law on State Registration of Legal Entities.<sup>20</sup> Government registration is required for the creation of a legal entity and introducing changes to its founding documents.<sup>21</sup> Violation of registration rules is an administrative violation (misdemeanor) punishable by a fine.

The Code on Administrative Violations details the penalties for legal entities and their branches (representative offices) for submission of false registration and re-registration information.<sup>22</sup> The amount of a fine depends on the amount of damage inflicted or the amount of illegally received profits.<sup>23</sup>

### B. Law on Licensing System in the Kyrgyz Republic

Conducting business without obtaining proper licenses is considered illegal entrepreneurship according to the Law on Licensing System in the Kyrgyz Republic.<sup>24</sup>

Article 15 of this law states that licenses are required for activities and operations such as export and import, production, transmission, distribution, and sale of specific goods.

The Criminal Code provides that carrying out business activities without a mandatory license or in violation of the license requirements, if such activity causes significant damage to individuals, organizations, or the state or is connected to extraction of a large amount of income, is punishable by fines or imprisonment for up to three years.<sup>25</sup> The same act is punishable by up to five years of imprisonment if committed by an organized group or a person previously convicted for illegal entrepreneurship or illegal banking activities.<sup>26</sup>

Carrying out entrepreneurial activities without a license is also punishable under the Code of Administrative Violations.<sup>27</sup> Imprisonment for up to five years and a fine of 500 to 800 minimum monthly wages may be imposed for conducting banking activities without registration or a

---

<sup>20</sup> Law of the Kyrgyz Republic on State Registration of Legal Entities, Branches (Representative Offices), No. 57, adopted Dec. 26, 2008, last amended May 22, 2015, arts. 1, 11, <https://perma.cc/7RFY-T94M> (in Russian), <https://perma.cc/G6MN-FTU8> (unofficial translation).

<sup>21</sup> *Id.*

<sup>22</sup> Code on Administrative Violations art. 441.

<sup>23</sup> *Id.*

<sup>24</sup> Law on Licensing System in the Kyrgyz Republic, No. 195, adopted Oct. 28, 2013, last amended Jan. 21, 2022, <https://perma.cc/3XYA-D2QK> (in Russian).

<sup>25</sup> Criminal Code art. 211.

<sup>26</sup> *Id.*

<sup>27</sup> Code on Administrative Violations art. 284.

license when a license is mandatory or with violation of licensing requirements if the conduct caused large damage to individuals, organizations, or the state.<sup>28</sup>

### C. Law on Export Control

Under the Law on Export Control, foreign economic operations involving the export, import, and re-export of controlled items are subject to mandatory licensing.<sup>29</sup>

Businesses that engage in unauthorized transactions related to the export, import, and re-export of controlled items and the shipment of such items through the territory of the Kyrgyz Republic without the appropriate permit will incur liability.<sup>30</sup> The following are other punishable activities:

- noncompliance or improper compliance with the instructions of authorized agencies,
- obstruction of officials of authorized export control agencies in the performance of their duties,
- unwarranted refusal to furnish information requested by the authorized agencies for export control purposes,
- deliberate distortion or concealment of such information,
- violation of the established record keeping procedure, and
- provision of false information to the authorities to obtain a license in order to carry out certain types of entrepreneurial activities.

These actions, whether committed by individuals or legal entities, are punishable by fines.<sup>31</sup>

### III. Examples of Convictions for Violations of Export Controls or Economic Espionage

Espionage-related cases are investigated by the Kyrgyzstani National Security Committee (GKNB). The jurisdiction of the GKNB includes export control issues if such cases might affect national security.<sup>32</sup>

Reportedly, in cases of espionage or high treason, where the fact of disclosing classified documents has to be established, courts order independent evaluation of the documents in question to verify whether they actually contain secret information. In some cases, different

---

<sup>28</sup> Id. art. 181, para. 1.

<sup>29</sup> Law of the Kyrgyz Republic on Export Control, No. 30, adopted Jan. 23, 2003, arts. 10-15, <https://perma.cc/8FU4-3L9D>.

<sup>30</sup> Id.

<sup>31</sup> Code on Administrative Violations art. 285.

<sup>32</sup> Law on Bodies of National Security of the Kyrgyz Republic, No. 1362-XII, adopted Jan. 11, 1994, last amended Jan. 22, 2021, art. 15, <https://perma.cc/4XTC-Y8A4> (in Russian).

subject matter experts selected by the prosecution and defense can conduct this evaluation several times.<sup>33</sup>

There is limited information available on espionage cases in the Kyrgyz Republic. However, several recent articles published in open media discuss either espionage or the related national security laws.

In April 2021, the Kyrgyz Service of Radio Liberty reported about espionage accusations against Marat Kazakpayev, a Kyrgyz political analyst, and Marat Toktouchikov, an ex-head of the Kazakh diaspora in the Kyrgyz Republic, who served as an advisor to the Kazakhstani government. According to the article, the GKNB detained both individuals on suspicion of high treason.<sup>34</sup>

Details of the criminal case have not been disclosed because of the GKNB's assertion that the materials involved are classified. The Pervomaisky District Court of Bishkek sanctioned detention of the accused pair for the duration of the investigation.<sup>35</sup>

---

<sup>33</sup> *Kyrgyz Judiciary Does Not Want to Make Errors*, Slovo Kyrgyzstana (Jan. 16, 2008), <https://perma.cc/UX63-SZP9> (in Russian).

<sup>34</sup> Ernist Nurmatov, *What Is the Reason for the Arrest of a Political Scientist Suspected of Treason?*, Radio Free Europe/Radio Liberty (Apr. 15, 2021), <https://perma.cc/FK5S-V7L3> (in Russian).

<sup>35</sup> *Spies and Traitors: Who and for What Are Accused of Treason in Kyrgyzstan?*, 24.kg (Apr. 16, 2021), <https://perma.cc/F4ZQ-DKEC> (in Russian).

# Mongolia

Louis Myers\*  
Legal Reference Librarian

**SUMMARY** The Criminal Code of Mongolia includes provisions on the crime of espionage, but does not differentiate economic espionage. Some crimes defined in the code, mainly under its national security and economic crimes chapters, have elements similar to those of the crime of espionage. Other laws, like the Customs Law, the Company Law, and the Law on Non-Bank Financial Activities detail conduct potentially including economic espionage activities that can be prosecuted under the Criminal Code.

## I. Introduction

Espionage in Mongolia is regulated generally under the Criminal Code of Mongolia.<sup>1</sup> Foreign persons are subject to the same criminal law procedures as Mongolian citizens.<sup>2</sup>

### A. Law on Criminal Procedure

Regarding crimes of espionage, Mongolia's Law on Criminal Procedure gives special investigatory authority to the General Intelligence Agency. This is a special delegation of investigatory powers that goes beyond the investigative powers of the regular police force.<sup>3</sup> There are also specific procedures when the accused is an entity or business.<sup>4</sup> Mongolian legal authorities interpret the law as requiring an individual or entity to provide information about a crime to prosecuting authorities in specific situations.<sup>5</sup>

---

\* At present, there are no Law Library of Congress research staff members versed in Mongolian. This report has been prepared by the author's reliance on practiced legal research methods and on the basis of relevant resources currently available in the Law Library and online.

<sup>1</sup> Criminal Code of Mongolia of 2017, <https://perma.cc/5YFC-QW7G>. Although this report is based on the 2017 version of the code, which is available on the Mongolian State website, it should be noted that articles 162 and 164 of the apparently superseded Criminal Code of 2002 addressed engaging in illegal businesses and illegal obtainment of financial or business secrets, respectively. The 2002 version of the code is available on the Legislationonline website, <https://perma.cc/E2G2-SX8K>.

<sup>2</sup> Law on Criminal Procedure art. 1.2(4), <https://perma.cc/86TR-BU8Z>; see also Law of Mongolia on the Legal Status of Foreign Nationals art. 7, and art. 37.1.10, which states that a foreign citizen will be deported for acting against the national interest of Mongolia, <https://perma.cc/BBK4-JKC2>.

<sup>3</sup> Law on Criminal Procedure art. 6.1.

<sup>4</sup> Id. art. 20.1.

<sup>5</sup> Gen. Council Cts. Mongolia, *The Mongolian Benchbook: A Practical Manual for Judges* 38 (1998). The commentary suggests an obligation to report embezzlement of property.

## B. Criminal Code of Mongolia

The Criminal Code of Mongolia contains the bulk of the laws related to espionage in Mongolia. The code also provides general guidance on punishments for crimes. Generally, espionage is considered a grave crime under Mongolian law and carries with it significant jail time.<sup>6</sup> The criminal code applies equally to Mongolian and foreign citizens, except when specifically stated otherwise. Liability for conduct is found in article 2 of the code.<sup>7</sup>

Espionage is considered a crime against national security in Mongolia. Under article 19.10 of the criminal code, “‘Espionage’ refers to perform [sic] tasks of foreign intelligence agency, the action that persuades a citizen of Mongolia to collaborate with foreign intelligent services and stealing, gathering, saving or transferring the data, documents, [or] objects constituting a state or military secret.”<sup>8</sup>

Under Mongolian law, only a foreign national or stateless person can be convicted of this crime, which is punishable by 12 to 20 years of prison.<sup>9</sup>

The crime of high treason, however, can only be committed by a Mongolian citizen. High treason includes, among other things, any act that is found detrimental to the national security of Mongolia, or an act where a citizen collaborates with a wartime enemy.<sup>10</sup> It is also a crime for a Mongolian citizen to engage in the same conduct that is defined as espionage, however, it is termed “illegal cooperation with a foreign intelligence agency” rather than espionage.<sup>11</sup> Stealing state secrets is also separately criminalized, if the conduct would not otherwise give rise to a charge of espionage.<sup>12</sup>

Chapter 18 of the criminal code deals with economic crimes. Article 18.4, Infringement of Rights of the Holders of an Invention, Industrial Design, or Utility Model Certificate, provides for punishment when unauthorized use of the intellectual property results in damages.<sup>13</sup> The Law of Mongolia on Patent provides for intellectual property rights in inventions, industrial designs, and utility models.<sup>14</sup>

---

<sup>6</sup> Criminal Code of Mongolia art. 2.6, <https://perma.cc/5YFC-QW7G>.

<sup>7</sup> Id. art. 2.

<sup>8</sup> Id. art. 19.10.

<sup>9</sup> Id.

<sup>10</sup> Id. art. 19.1.

<sup>11</sup> Id. art. 19.4.

<sup>12</sup> Id. art. 19.11-13; the Law on State and Official Secrets is also discussed in more detail later in ch. 19 of the code.

<sup>13</sup> Id. art. 18.4.

<sup>14</sup> Law of Mongolia on Patent, <https://perma.cc/R67F-GP7W>.

The code also contains provisions protecting electronic information from hacking. Article 26 criminalizes several acts, including illegal transfer of electronic information.<sup>15</sup> If that action is taken with regard to a state secret, a longer prison sentence is allowed.<sup>16</sup>

### C. Customs Law of Mongolia

The Customs Law of Mongolia regulates the import and export of goods into and out of Mongolia.<sup>17</sup> Violations can be punished with civil as well as criminal penalties. These laws provide special police powers to customs officials, allowing them broader investigatory abilities than those possessed by other law enforcement officials in Mongolia.<sup>18</sup>

Broadly speaking, anything entering and exiting the country is subject to customs control within the “customs frontier,” which is the border areas of Mongolia.<sup>19</sup> The law also permits the parliament and government of Mongolia to restrict exportation of goods; goods so restricted are to be coded using the Harmonized Commodity and Description and Coding System.<sup>20</sup> As of 2005, the Mongolian government prohibited export of drugs and narcotics (and raw materials and equipment to produce them); dangerous chemicals; and raw hides, skins, and cashmere; and imposed export taxes on various commodities.<sup>21</sup>

Beginning at article 241, the law provides various procedures customs officials must take to verify what is entering and leaving the country. The law also provides customs officials with a wide spectrum of methods to ensure that customs obligations have been met and specific procedures to inspect certain goods (e.g., hazardous substances).<sup>22</sup> Individuals found in violation of the Customs Law are subject to disciplinary sanctions such as financial penalties and forfeiture of goods unless the actions qualify as criminal.<sup>23</sup>

### D. Law on State and Official Secrets

The Law on State and Official Secrets includes provisions protecting information with national security significance.<sup>24</sup> Article 13 provides the kinds of information that should be classified as

---

<sup>15</sup> Id. art. 26.1.

<sup>16</sup> Id.

<sup>17</sup> Law on Customs of Mongolia, <https://perma.cc/H4VH-S4VE>.

<sup>18</sup> Law on Criminal Procedure art. 1.8 provides general rules for searches; the Law on Customs of Mongolia art. 247 contains rules on searches of persons. Law on Criminal Procedure art. 30.7 (2.8) provides investigatory power to customs officials. Art. 24.1 provides a general overview of searches in Mongolia.

<sup>19</sup> Law on Customs art. 3.

<sup>20</sup> Id. art. 8.1-3;.

<sup>21</sup> See *Trade Policy Review: Mongolia* World Trade Organization, (Feb. 2005), at 12, <https://perma.cc/6CBA-XT3U>.

<sup>22</sup> Law on Customs art. 246.5.1.

<sup>23</sup> Id. art. 290.2.

<sup>24</sup> Law on State and Official Secrets, <https://perma.cc/82X3-GBW7>.

state secrets. The list includes information on economic security; the national treasury, resources fund, and currency supply; and scientific and technological research that has implications for national security. Article 13 also covers information security, which includes proprietary information on government encryption and important resource management such as clean water. Article 39 of the state secrets law provides various civil punishments for breaches and states that serious breaches are subject to punishment under the criminal code.<sup>25</sup>

Article 6.4 places an obligation on citizens to notify the government of any disclosures of a state secret. It does not state that noncitizens have the same obligation. As discussed in Section I.B. above, however, a charge of espionage can be brought against foreign citizens.

### **E. Law on Company**

The Law on Company provides the framework for establishing business organizations in Mongolia.<sup>26</sup> It details the process for registering a company, defines a subsidiary company, and describes their respective liabilities.<sup>27</sup> Article 82 sets forth standards to ensure transparency to shareholders and in business dealings, for example, maintaining records and documentation of the board of directors.<sup>28</sup> Article 84 provides the duties of the governing persons of a company. These duties include the protection of the company's confidential information. Companies are frequently overseen by auditors, whose duties are also provided in the Law of Company.<sup>29</sup> It appears that any claim stemming from a breach of these duties would be criminal as well as civil in nature.<sup>30</sup> Article 100.1 states that liability is found under the Criminal Code or the Law on Violations.<sup>31</sup>

### **F. Law on Investment**

The Law on Investment provides the framework for domestic and foreign investment in Mongolian businesses. Although the law defines both foreign and domestic investors, it does not distinguish between the two as it relates to their rights as investors.<sup>32</sup> However, if the foreign investor is a foreign state-owned entity, it must receive permission from the Mongolian government before engaging in any transaction.<sup>33</sup> Foreign state investors are subject to somewhat stricter guidelines than are other investors. For example, article 22.4.1 specifically prohibits any

---

<sup>25</sup> State secrets provisions are contained in art. 19.11-13 of the Criminal Code of Mongolia.

<sup>26</sup> Law on Company, <https://perma.cc/644K-D6SR>.

<sup>27</sup> *Id.* art. 6.

<sup>28</sup> *Id.* art. 82.2.1.

<sup>29</sup> *Id.* arts. 94-99.

<sup>30</sup> *Id.* art. 100; see also Criminal Code of Mongolia art. 9.

<sup>31</sup> Law of Company art. 100.1, referencing the Law on Violations.

<sup>32</sup> Law on Investment art. 3.1.2-4, <https://perma.cc/2WMX-TF8P>.

<sup>33</sup> *Id.* art. 4.3; see art. 21 for specific criteria a state entity must satisfy for investment.

activities that jeopardize Mongolia's national security.<sup>34</sup> Any violation of the investment law, regardless of the nature of the investment, is subject to civil and criminal penalties.<sup>35</sup>

## G. Law on Intellectual Property

The Law on Intellectual Property provides the framework for protection of intellectual property and regulates the use of intellectual property for economic use.<sup>36</sup> The definition of intellectual property includes industrial property.<sup>37</sup> Industrial property rights are specifically protected under this law.<sup>38</sup> Industrial property rights broadly include inventions, innovations, and industrial designs.<sup>39</sup> This law also protecting against disclosure by an authorized representative of intellectual property-related secrets to the public.<sup>40</sup> Further, the Mongolian government is responsible for supporting the international protection of intellectual property rights.<sup>41</sup> The law provides civil and criminal penalties for violations.<sup>42</sup>

## II. Cases on Espionage and Related Laws

There is limited information available on the outcomes of espionage cases in Mongolia, and no recent cases of economic espionage were located in news sources. However, several recent articles discuss matters involving espionage or the related national security laws. An article published in March 2022 reports that a cyber-espionage group based in China, "Mustang Panda," targets nongovernmental organizations operating in Mongolia.<sup>43</sup> In February, a Mongolian activist was arrested for allegedly breaching national security. It is unclear what specific charges the Mongolian General Intelligence Agency will bring.<sup>44</sup>

---

<sup>34</sup> Id. art. 22.4.1.

<sup>35</sup> Id. art. 23.

<sup>36</sup> Law of Mongolia on Intellectual Property art. 1.1, <https://perma.cc/X5SH-VH2Z>.

<sup>37</sup> Id. art. 3.1.1.

<sup>38</sup> Id. art. 5.1.2.

<sup>39</sup> Id. art. 7.

<sup>40</sup> Id. art. 16.7.

<sup>41</sup> Id. art. 22.1.4.

<sup>42</sup> Id. art. 26.

<sup>43</sup> Ravie Lakshmanan, *Chinese 'Mustang Panda' Hackers Spotted Deploying New 'Hodur' Malware*, Hacker News (Mar. 23, 2022), <https://perma.cc/3HLE-WBHS>.

<sup>44</sup> *Arrest of Mongolian Activist and Outspoken Critic of China Sparks Outrage*, WION (Feb. 22, 2022), <https://perma.cc/KE3G-HMKV>.

# Peru

*Graciela Rodriguez-Ferrand*  
*Senior Foreign Law Specialist*

**SUMMARY** Perú does not provide a specific penalty for economic espionage. However, it does punish the revealing of business secrets through espionage. The filing of fraudulent corporate information, the filing of fraudulent import-export documentation, and the filing of false client information to banking institutions are subject to imprisonment and fines.

## I. Economic Espionage

There are no specific provisions against economic espionage in Perú. However, the unauthorized passing of secret industrial information is sanctioned under the Ley de Represión de la Competencia Desleal (Law for the Repression of Unfair Competition) (LRCD).<sup>1</sup>

An action aimed at revealing or exploiting a business secret without the owner's consent is considered a violation of the LRCD, whether the secret was accessed illegally or by authorization but subject to confidentiality.<sup>2</sup> Acquiring business secrets through espionage, inducing violation of confidentiality, or any similar conduct also constitutes a violation.<sup>3</sup> Business espionage declared as such by the Comisión de Fiscalización de la Competencia Desleal of the Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual is subject to a fine and the owner's right to seek compensation in civil litigation.<sup>4</sup>

## II. Fraudulent Corporate Filing

Under the Penal Code, a manager or representative of a legal entity who provides fraudulent information about the entity to the detriment of the entity or third parties is subject to imprisonment for one to four years.<sup>5</sup> The same penalty applies to an internal or external balance sheet auditor who fails to report irregularities or wrongful accounting.<sup>6</sup>

An administrator or manager of a legal entity who provides fraudulent information about the entity to the authorities is subject to a penalty of not more than two years and a fine.<sup>7</sup>

---

<sup>1</sup> Decreto Legislativo 1044 que Aprueba la Ley de Represión de la Competencia Desleal, El Peruano (EP), June 25, 2008, <https://perma.cc/DQE7-7JY2>.

<sup>2</sup> Id. art. 13.1.

<sup>3</sup> Id. art. 13.2.

<sup>4</sup> Id. arts. 24, 52-58.

<sup>5</sup> Decreto Legislativo 635/1991, Código Penal art. 198, EP, Apr. 8, 1991, <https://perma.cc/KW89-94BJ>.

<sup>6</sup> Id. art. 198-A.

<sup>7</sup> Id. art. 242.

The Ley General de Sociedades (Law on Corporations) provides that corporate managers are responsible for damages caused to the entity, shareholders, and third parties for violation of the obligation to provide accurate and true information about the entity.<sup>8</sup>

### III. Fraudulent Filing of Import-Export Documentation

Under the Ley de los Delitos Aduaneros (Law on Customs Crimes), anyone who files fraudulent information concerning customs operations is subject to imprisonment for five to eight years.<sup>9</sup> The penalty is increased for filing fraudulent information about the identity of a recipient or supplier or false addresses.<sup>10</sup>

A legal entity responsible for such actions will be subject to penalties such as temporary or permanent closure of the establishment, cancelation of its license to operate, or dissolution.<sup>11</sup> If the wrongdoing involves a foreign person, he or she may be expelled from the country.<sup>12</sup>

### IV. Filing False Customer Information to Banking Entities

According to the Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros (General Law on the Financial System and the Insurance System and Organic Law of the Superintendency of Banking and Insurance), providing false information to a banking institution to obtain financing is punishable by imprisonment from one to four years and a fine, applicable under the Penal Code for the crime of financing through false information.<sup>13</sup>

No special evidentiary threshold rules have been found other than the general rule, which requires that the judge be certain of the defendant's criminal responsibility after all the evidence has been produced. Once the judge is certain about the defendant's culpability, the initial presumption of innocence is overcome.<sup>14</sup>

We were unable to locate any information on convictions in Perú for economic espionage.

---

<sup>8</sup> Ley 26887 General de Sociedades arts. 190.3-.4, 190.7, EP, Nov. 19, 1997, <https://perma.cc/M7PP-UJKD>.

<sup>9</sup> Ley 28008 de Delitos Aduaneros arts. 4-5, EP, June 19, 2003, <https://perma.cc/22LV-AKH8>.

<sup>10</sup> Id. art. 10.h.

<sup>11</sup> Id. art. 11.

<sup>12</sup> Id. art. 12.

<sup>13</sup> Ley 26702 Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros art. 179, <https://perma.cc/BV4Z-PNKA>; Código Penal art. 247.

<sup>14</sup> Arsenio Oré Guardia, 2 *Derecho Procesal Peruano* 332 (Lima 2016).

# South Korea

Sayuri Umeda  
Senior Foreign Law Specialist\*

**SUMMARY** South Korea has four laws to protect technologies from unauthorized transfers: the Unfair Competition Prevention and Trade Secret Protection Act, the Industrial Technology Protection Act, the Small Business Technology Protection Act, and the Defense Technology Security Act.

Filing fraudulent corporate registration information is punishable under the Criminal Act. Filing fraudulent import/export documentation is punishable under the Foreign Trade Act. Filing false customer information with banking entities is punishable under the Act on Real Name Financial Transactions and Confidentiality.

## I. Technology Protection Laws

The Republic of Korea (South Korea) has tightened technology security to protect its key technologies from leaking abroad.<sup>1</sup> There are four laws to protect technologies from unauthorized transfers. They are overlapping in some parts.<sup>2</sup>

### A. Unfair Competition Prevention and Trade Secret Protection Act

The Unfair Competition Prevention and Trade Secret Protection Act (UCPTSPA)<sup>3</sup> is the primary law protecting against economic espionage. The UCPTSPA protects trade secrets from infringement. It defines a trade secret as “information, including a production method, sale method, useful technical or business information for business activities, which is not known publicly, is managed as a secret, and has independent economic value.”<sup>4</sup> Infringement of trade secrets means any of the following acts:

- (a) An act of acquiring trade secrets by theft, deception, coercion, or other improper means (act of improper acquisition), or subsequently using or disclosing the trade secrets

---

\* At present, there are no Law Library of Congress research staff members versed in Korean. This report has been prepared by the author’s reliance on practiced research methods and on the basis of relevant resources currently available in the Law Library and online.

<sup>1</sup> Sung-min Kim, *S. Korea to Tighten Measures to Protect Key Industries from Tech Leaks*, Arirang (Dec. 23, 2021), <https://perma.cc/W3A6-3CT7>.

<sup>2</sup> Sun He Yun et al., 韓国での営業秘密保護関連法律の動向と課題 (*Trade Secret Protection Relevant Laws Trends and Challenges*), 日本知財学会誌 (13(1) IPAJ Bull. 47 (2016), <https://perma.cc/6SS9-K3JF>.

<sup>3</sup> Unfair Competition Prevention and Trade Secret Protection Act (UCPTSPA), Act No. 5621, Dec. 31, 1998, amended by Act No. 17727, Dec. 22, 2020, <https://perma.cc/7TJA-SNKJ>.

<sup>4</sup> Id. art. 2, para. 2.

- improperly acquired, including informing any specific person of the trade secret while under a duty to maintain secrecy;
- (b) An act of acquiring trade secrets or using or disclosing the trade secrets improperly acquired, with knowledge of the fact that an act of improper acquisition of the trade secrets has occurred or without such knowledge due to gross negligence;
  - (c) An act of using or disclosing trade secrets after acquiring them, with knowledge of the fact that an act of improper acquisition of the trade secrets has occurred or without such knowledge due to gross negligence;
  - (d) An act of using or disclosing trade secrets to obtain improper benefits or to cause damage to the owner of the trade secrets while under a contractual or other duty to maintain secrecy of the trade secrets;
  - (e) An act of acquiring trade secrets, or using or disclosing them with the knowledge of the fact that they have been disclosed in the manner prescribed in item (d) or that such disclosure has been involved, or without such knowledge due to gross negligence;
  - (f) An act of using or disclosing trade secrets after acquiring them, with the knowledge of the fact that they have been disclosed in a manner prescribed in item (d) or that such disclosure has been involved, or without such knowledge due to gross negligence<sup>5</sup>

A person who damages the business interest of a person who possesses trade secrets through an intentional or negligent infringement of trade secrets is liable for compensation for such damage.<sup>6</sup>

The UCPTSPA also provides criminal sanctions. A person who commits any of the following acts is punishable by imprisonment for not more than 10 years or by a fine not exceeding 500 million won (about US\$390,000):

- acts committed for the purpose of making an improper profit or causing damage to a person who possesses trade secrets by:
  - acquiring, using, or leaking trade secrets to any third party,
  - unauthorized release of trade secrets,
  - continuing to possess trade secrets even after a request to delete or return them by the rightful owner of such trade secrets,
- acquiring trade secrets by theft, fraud, intimidation, or other improper means, and
- acquiring or using trade secrets with knowledge of the commission of one of these acts.<sup>7</sup>

The fine is increased to two to 10 times the amount of proprietary benefits if the amount equal to 10 times the amount of proprietary benefits acquired by the violation exceeds 500 million won.<sup>8</sup> If a person who committed one of these acts uses trade secrets in a foreign country or commits the act while knowing that trade secrets will be used in a foreign country, the punishment is increased to imprisonment for not more than 15 years or a fine not exceeding 1.5 billion won (about US\$1.18 million). The fine is increased to two to 10 times the amount of proprietary

---

<sup>5</sup> Id. art. 2, subpara. 3.

<sup>6</sup> Id. art. 11.

<sup>7</sup> Id. art. 18, para. 1.

<sup>8</sup> Id. art. 18, para. 2.

benefits when the amount equal to 10 times the amount of proprietary benefits acquired by the violation exceeds 1.5 billion won.<sup>9</sup>

Persons who have divulged any confidential information learned in the course of performing their duties are punishable by imprisonment for not more than one year or by a fine not exceeding 10 million won (about US\$7,800).<sup>10</sup>

## **B. Industrial Technology Protection Act**

The Act on Prevention of Divulgence and Protection of Industrial Technology (Industrial Technology Protection Act, ITPA) was enacted in 2006.<sup>11</sup> "Industrial technology" means technologies that the heads of an administrative agencies recognize in accordance with specified laws and regulations, including "national core technology" as designated under article 9 of ITPA.<sup>12</sup> National core technology is technology that "has high technological and economic values in the Korean and overseas markets or brings high growth potential to its related industries," and consequently, its "leak abroad could have a material adverse effect on national security and development of the national economy."<sup>13</sup> The minister of Trade, Industry and Energy (minister of MTIE) designates it after deliberation by the Industrial Technology Protection Committee.<sup>14</sup> The selection is made by the MTIE or relevant central governmental administrative agencies.<sup>15</sup>

Each institution that has and manages national core technology must take measures to prevent divulgence of national core technology as specified by the government.<sup>16</sup> Where an institution developed national core technology with government subsidies, it must obtain an approval from the minister of MTIE before it exports the national core technology to a foreign enterprise.<sup>17</sup> When a government subsidy is not involved, it must report the export in advance, instead of issuing an approval.<sup>18</sup>

---

<sup>9</sup> Id.

<sup>10</sup> Id. art. 18, para. 4.

<sup>11</sup> Act on Prevention of Divulgence and Protection of Industrial Technology (ITPA), Act No. 8062, Oct. 27, 2006, amended by Act No. 16476, Aug. 20, 2019, <https://perma.cc/H23M-26Y8>.

<sup>12</sup> Id. art. 2, para. 1.

<sup>13</sup> Id. art. 2, para. 2.

<sup>14</sup> The Industrial Technology Protection Committee was established under the jurisdiction of the minister of MTIE to deliberate on matters regarding preventing divulgence of, and protecting, industrial technology. Id. art. 7, para. 1.

<sup>15</sup> Id. art. 9, para. 1.

<sup>16</sup> Id. art. 10, para. 1.

<sup>17</sup> Id. art. 11, para. 1.

<sup>18</sup> Id. art. 11, para. 4.

ITPA prohibits obtaining industrial technology by improper means or infringement.<sup>19</sup> Depending on the act committed, a violator may be punished by up to 15 years imprisonment, a fine not exceeding 1.5 billion won, or both.<sup>20</sup>

### C. Small Business Technology Protection Act

The Act on Support for Protection of Technologies of Small and Medium Enterprises (SBTPA) was enacted in 2014.<sup>21</sup> “Technologies of small and medium enterprises’ means technologies or management information having independent economic value necessary for developing, producing, disseminating, and using the products or services produced or to be produced by small and medium entrepreneurs.”<sup>22</sup>

Small and medium enterprises (SMEs) that suffer an infringement of their technology may report it to the Ministry of SMEs and Startups and request that the ministry take necessary measures.<sup>23</sup> The ministry may recommend mediation or arbitration by the Commission for Mediation and Arbitration of Disputes on Technologies of SMEs.<sup>24</sup> The ministry may request the relevant organizations or business entities to submit materials for an investigation of infringement of a technology or have public officials enter offices, places of business, and other necessary places to investigate records, documents, facilities, and other items.<sup>25</sup> A person who fails to submit such materials, submits false materials, or refuses, obstructs, or evades an investigation is subject to an administrative fine not exceeding 10 million won.<sup>26</sup> Where the ministry finds considerable grounds to determine that there has been infringement of technologies by a respondent, and damage has already occurred or failure to take action is likely to cause irreversible damage, it may recommend that the respondent suspend the act of suspected infringement, prevent recurrence in the future, and take corrective measures within 30 days.<sup>27</sup> Where the respondent fails to comply with the recommendation, the ministry may publish the subject of the recommendation.<sup>28</sup>

---

<sup>19</sup> Id. art. 14, para. 1.

<sup>20</sup> Id. art. 36.

<sup>21</sup> Act on Support for Protection of Technologies of Small and Medium Enterprises (SBTPA), Act No. 12696, May 28, 2014, amended by Act No. 17559, Oct. 20, 2020, <https://perma.cc/2TJK-HWN7>.

<sup>22</sup> Id. art. 2.2.

<sup>23</sup> Id. art. 8-2, para. 1.

<sup>24</sup> Id. art. 8-2, para. 3. The Commission for Mediation and Arbitration of Disputes on Technologies of SMEs was established under the jurisdiction of the Ministry of SMEs and Startups based on the SBTPA to mediate and arbitrate disputes related to the protection of technologies of SMEs. Id. art. 23.

<sup>25</sup> Id. art. 8-2, para. 4.

<sup>26</sup> Id. art. 35, para. 1.

<sup>27</sup> Id. art. 8-3, para. 1.

<sup>28</sup> Id. art. 8-3, para. 3.

#### D. Defense Technology Security Act

Under the Defense Technology Security Act, “defense technology” means “a technology requiring protection for national security among the defense science and technologies related to the defense industry, as designated and publicly announced by the Minister of Defense Acquisition Program Administration.”<sup>29</sup> The Defense Acquisition Program Administration (DAPA) is an administrative center specializing in defense acquisition.<sup>30</sup>

Persons who commit one of the following offenses are punishable by imprisonment for not more than 10 years or by a fine not exceeding 1 billion won (US\$780,000):<sup>31</sup>

- Improperly acquiring, using, or disclosing defense technology; and
- Acquiring, using, or disclosing defense technology, knowing the involvement of one of activities listed above.<sup>32</sup>

If a person intended using defense technology or causing its use in a foreign country, the person is punishable by imprisonment for not more than 20 years or by a fine not exceeding 2 billion won (US\$1.56 million).<sup>33</sup>

A person who acquires, uses, or discloses defense technology by gross negligence without knowing the involvement of one of criminal activities above is punishable by imprisonment for not more than five years or by a fine not exceeding 500 million won (about US\$390,000).<sup>34</sup>

When one of the following persons divulges or misuses confidential information regarding defense technology, he or she is punishable by imprisonment for not more than seven years, suspension of qualification for not more than 10 years, or by a fine not exceeding 70 million won (US\$55,000):<sup>35</sup>

- An executive, employee, or other related persons, such as professors, researchers and students, of an institution that owns defense technology or conducts a research and development project related to defense technology; and
- A member of the Defense Technology Security Committee who deliberates on the security of defense technology.

---

<sup>29</sup> Defense Technology Security Act, Act No. 13632, Dec. 29, 2015, amended by Act No. 15052, Nov. 28, 2017, art. 2, sub-para. 1, <https://perma.cc/4MS5-BZYL>.

<sup>30</sup> *About DAPA*, DAPA, <https://perma.cc/J5LU-6CET>.

<sup>31</sup> Defense Technology Security Act art. 21, para. 2.

<sup>32</sup> *Id.* art. 10.

<sup>33</sup> *Id.* art. 21, para. 1.

<sup>34</sup> *Id.* art. 10, art. 21, para. 3.

<sup>35</sup> *Id.* art. 21, para. 4.

## II. Evidentiary Legal Threshold and Penalty for Certain Cases

There is no provision setting a special evidentiary threshold for the following cases. Therefore, the general criminal law standard (beyond a reasonable doubt)<sup>36</sup> applies.

### A. Filing Fraudulent Corporate Registration Information

Incorporation of a stock company must be registered. Matters to be registered include the objectives, company name, total number of shares authorized to be issued by the company, location of main office, amount of capital, and names of directors.<sup>37</sup> Filing fraudulent corporate registration information is punishable under the Criminal Act.<sup>38</sup> A person who makes an untrue statement to a public official, thereby causing a false entry to be made in a registration certificate, is punishable by imprisonment for not more than three years or by a fine not exceeding 7 million won (about US\$5,500) under the act.<sup>39</sup>

### B. Filing Fraudulent Import/Export Documentation

Under the Foreign Trade Act, goods designated as “strategic items” by the Minister of Trade, Industry and Energy to maintain peace and security require approval or permission for exportation or importation.<sup>40</sup>

A person who obtains export permission for a designated strategic item by fraud or other improper means is punishable by imprisonment for not more than three years or by a fine not exceeding three times the value of the goods.<sup>41</sup> The same punishment applies to a person who obtains “situational permission”<sup>42</sup> by fraud or other improper means for goods that are not strategic items but “have high potential for being appropriated for manufacturing, developing, using, or storing weapons of mass destruction”<sup>43</sup> despite the person’s awareness or suspicion that the importer or end user of the goods intends them for such use.<sup>44</sup>

---

<sup>36</sup> *Criminal*, Supreme Court of Korea, <https://perma.cc/E23U-Z7FG>.

<sup>37</sup> Commercial Act, Act No. 1000, Jan. 20, 1962, amended by Act No. 17362, June 9, 2020, art. 317, <https://perma.cc/5GT7-HJW5>.

<sup>38</sup> Criminal Act, Act No. 293, Sept. 18, 1953, amended by Act No. 17511, Oct. 20, 2020, <https://perma.cc/BF54-DRF4>.

<sup>39</sup> Id. art. 228, para. 2.

<sup>40</sup> Foreign Trade Act, Act No. 8356, Apr. 11, 2007, amended by Act No. 16422, Apr. 30, 2019, art. 19, para. 2, <https://perma.cc/6VVR-EA82>.

<sup>41</sup> Id. art. 53, para. 2, subpara. 3.

<sup>42</sup> Permission under conditions prescribed by presidential decree. Id. art. 19, para. 3.

<sup>43</sup> Id.

<sup>44</sup> Id. art. 53, para. 2, subpara. 5.

A person who exports or imports “designated goods”<sup>45</sup> by obtaining approval or being exempted from such approval by fraud or other improper means is punishable by imprisonment for not more than three years or by a fine not exceeding 30 million won (US\$23,370).<sup>46</sup> The same punishment applies to a person who obtains approval of exportation of an “industrial plant”<sup>47</sup> by fraud or other improper means.<sup>48</sup>

### C. Filing False Customer Information to Banking Entities

The Act on Real Name Financial Transactions and Confidentiality prohibits a person from performing financial transactions under the name of another person for the purpose of concealing illegitimate property, money laundering, financing terrorism, and other evasions of the Act on Reporting and Using Specified Financial Transaction Information.<sup>49</sup> A violator is punishable by imprisonment for not more than five years or by a fine not exceeding 50 million won (about US\$39,000).<sup>50</sup>

## III. Cases

Examples from the past five years of convictions based on violations of export controls or for economic espionage were not located. The National Intelligence Service has detected 99 cases of attempted industrial espionage from January 2017 to February 2022.<sup>51</sup>

---

<sup>45</sup> The designation is made to fulfill obligations under treaties, protect biological resources, promote economic cooperation with trading partner countries, seamlessly supply materials for national defense, or develop science and technology. Id. art. 11, para. 1.

<sup>46</sup> Id. art. 54, item 3.

<sup>47</sup> Machinery, equipment, and devices for management of a business. Id. art. 32.

<sup>48</sup> Id. art. 54, item 8.

<sup>49</sup> Act on Real Name Financial Transactions and Confidentiality, Act No. 5493, Dec. 31, 1997, amended by Act No. 15929, Dec. 11, 2018, art. 3, para. 3, <https://perma.cc/G39W-DAA3>. Act on Reporting and Using Specified Financial Transaction Information, Act No. 6516, Sep. 27, 2001, amended by Act No. 17880, Jan. 5, 2021, <https://perma.cc/Y4LJ-MEFM>.

<sup>50</sup> Act on Real Name Financial Transactions and Confidentiality art. 6.

<sup>51</sup> Yonhap, *Spy Agency Detects 99 Cases of Attempted Industrial Spying for Five Years*, Korea Herald (Apr. 2, 2022), <https://perma.cc/9Z4L-7HAL>.

# Tajikistan

*Peter Roudik  
Director of Legal Research*

**SUMMARY** The Tajik Law on Commercial Secrets appears to be the governing act in protecting economic information. It defines what content constitutes secret information and provides the rules for establishing secrecy protection regimes. Various sectoral laws may define additional information as confidential. The basic rule is that a party responsible for damages caused by disclosing economic information must pay compensation. No rules establishing punitive damages have been found. Under specific circumstances, the illegal collection and disclosure of information containing commercial or banking secrets may be recognized as a crime. Fraudulent activities by private corporations are prosecuted as misdemeanors unless these actions did not inflict serious or very serious damage. No information about the handling of crimes discussed in this report by Tajik courts has been located.

## I. Economic Espionage Legislation

In 2008, the Law on Commercial Secrets was passed in Tajikistan. This law defines commercial secrets as information that would enable its holder to increase revenues, avoid unjustified expenditures, retain its market position, or receive other economic benefits.<sup>1</sup> The regime of commercial secrecy is introduced by the holder of the secrets individually and may apply to any information of a “scientific, technological, technical, production, financial, and economic nature.”<sup>2</sup> The holder of information must establish the rules for access to and protection of information containing commercial secrets. It is an information holder’s obligation to maintain records on the transfer of this type of information to third persons.

Tajik civil legislation protects confidential information that has real or potential commercial value because of its nondisclosure, restricted access, or the protection measures taken by the information holder. Under article 153 of the Tajik Civil Code, individuals who unlawfully obtain access to such information or disclose it in breach of contract requirements are required to make recompense for the consequent damage.<sup>3</sup>

Persons gaining illegal access to information containing commercial or banking secrets are subject to criminal penalties if their conduct contain the following qualifying actions:

---

<sup>1</sup> Law of the Republic of Tajikistan on Commercial Secrets of June 18, 2008, (Law on Commercial Secrets), art. 3, <https://perma.cc/D59M-XHT3>.

<sup>2</sup> *Id.*

<sup>3</sup> Civil Code of Tajikistan, adopted June 30, 1999, pt. 1, art. 153, Akhori Madjlisi Oli Respubliki Tadjikistan [Official Gazette (O.G.)] 1999, No. 6, <https://perma.cc/JXR8-XPUD> (in Russian).

- gathering information by stealing documents,
- bribing or threatening individuals who have access to this information or their relatives,
- penetrating computer systems and electronic networks by special technical means, or
- employing other illegal means to access information for its disclosure or unlawful use.

These acts are punishable by heavy fines or imprisonment for a term of up to two years.<sup>4</sup>

Disclosure of secret commercial or banking information constitutes a crime if it was committed to obtain personal material benefits by a person who had access to this information due to his or her professional activity or official position. If the disclosure inflicted serious damage on a commercial organization or an individual entrepreneur, the perpetrator is subject to imprisonment for up to three years and a ban on performing specific professional activities for the next five years. This crime is considered a crime of private prosecution, and an investigation can be initiated only upon a request submitted by the commercial organization or an individual businessperson who suffered the damage.<sup>5</sup>

The Law on Commercial Secrets prohibits classifying the following kinds of information as secret:

- information that can be found in a company's registration and licensing documents,
- information about receipt of government funds or work under government contracts,
- information related to occupational, industrial, and environmental safety,
- information about the remuneration of employees,
- information about the legal violations committed by an enterprise, and
- other information specified in Tajik laws.<sup>6</sup>

## II. Prosecution of Fraudulent Activities of Private Corporations

Corporate registration is mandatory in Tajikistan and is regulated by the Law on State Registration of Legal Entities and Individual Entrepreneurs.<sup>7</sup> Violating the registration rules or conducting business or banking operations without registering or obtaining proper licenses is considered illegal entrepreneurship. It constitutes an administrative violation (misdemeanor), which is punishable by a fine. The amount of the fine depends on the amount of inflicted damage or the amount of illegally received profits.<sup>8</sup>

---

<sup>4</sup> Criminal Code of Tajikistan, adopted May 21, 1998, art. 277, O.G. 1998, No. 6, Items 68-70, <https://perma.cc/234R-DS3B> (in Russian).

<sup>5</sup> Id. art. 278.

<sup>6</sup> Law on Commercial Secrets art. 5.

<sup>7</sup> Law of the Republic of Tajikistan of May 19, 2009, on State Registration of Legal Entities and Individual Entrepreneurs, O.G. 2009, No. 5, Item 316, <https://perma.cc/T7RS-HU3K>.

<sup>8</sup> Code of the Republic of Tajikistan on Administrative Violations, adopted Dec. 31, 2008, arts. 504, 510, 511, & 515, O.G. 2008, No. 12(1), Item 990, <https://perma.cc/7AH7-2JFM> (in Russian).

In cases where illegal entrepreneurship results in obtaining large or especially large amounts of profit, or the illegal entrepreneurship is committed by a person or group previously convicted of the same offense, the case is reclassified as a crime and prosecuted under article 259 of the Criminal Code. It provides for increased fines or imprisonment for a period of up to five years. Similar penalties apply to illegal banking activities.<sup>9</sup>

### III. Examples of Convictions for Violations of Export Controls or Economic Espionage

While reports in open source media remain the main source of information about major court decisions issued in Tajikistan, no information on court decisions related to the protection of commercial secrets or the resolution of cases involving illegal entrepreneurship has been located. Local newspapers periodically report on espionage investigations conducted by the Tajik security authorities and accuse government bodies of using espionage charges against local academics.<sup>10</sup> Similarly, migrants from neighboring states are reportedly detained and accused of espionage to use them as “bargaining chips” in resolving disputes with those states.<sup>11</sup> Some local media report on intensified Chinese espionage masked by economic activities.<sup>12</sup>

---

<sup>9</sup> Criminal Code of Tajikistan art. 263.

<sup>10</sup> Umed Babakhanov, *How I Almost Became a Spy*, Globalvoices.org (July 5, 2014) (Chris Rickleton, trans.), <https://perma.cc/RD4X-HA6P>.

<sup>11</sup> “Probably They Want to Exchange Us.”: Kyrgyz Nationals Expect a Trial in Tajikistan, Radio Azattyk (Oct. 30, 2021), <https://perma.cc/C74F-RRV8> (in Russian).

<sup>12</sup> Salman Rafi Sheikh, *China Looks to Tajik to Spy Afghan Terror Risks*, Asia Times (Nov. 8, 2021), <https://perma.cc/PSK6-8B7N>.

# Turkey

*Kayahan Cantekin*  
*Foreign Law Specialist*

**SUMMARY** Economic espionage is not specifically criminalized in Turkish law. The Turkish Penal Code includes an espionage offense that arguably covers certain acts that can be considered as acts of economic espionage, however, support for this interpretation is scarce in the literature and is not discussed in high court precedent. There has been one reported instance in the last five years where alleged acts that are arguably of the nature of economic espionage have been prosecuted under this offense. However, this prosecution appears to be unusual. Certain acts of economic espionage may be prosecuted under another offense in the Turkish Penal Code that criminalizes the unauthorized disclosure of trade secrets and intellectual property by persons who have access to the information by virtue of their employment or profession. This offense is not formulated as an espionage offense and is penalized with a comparatively light sanction. This report provides information on certain provisions of the Turkish Commercial Code, Anti-Smuggling Law, and Banking Law setting forth penalties for the filing of fraudulent corporate registration information, import/export documentation, and banking customer information. The evidentiary threshold is the general standard of prosecution under the Criminal Procedure Code, which governs the prosecution of all offenses discussed in this report.

## I. Overview

In Turkish law, there is no specific legislation formally regulating or otherwise criminalizing “economic espionage,” broadly defined as the unauthorized obtaining or disclosing of confidential or secret (non-defense-related) economic, industrial, or commercial information on behalf of a foreign state or organization.<sup>1</sup> Several offenses applying to “military and political espionage” and the protection of state secrets exist in the Turkish Penal Code (TPC),<sup>2</sup> but this framework does not appear to cover activity that can be classified as economic espionage, at least explicitly. Some legal commentators have called attention to this gap in the law.<sup>3</sup> Nevertheless,

---

<sup>1</sup> See Uğur Arslan, *Devlet Sırlarına Karşı Suçlar ve Casusluk Suçları* [Offenses Against State Secrets and Espionage Offenses] 581, 591 (2021) (Ph.D. Thesis, Hacettepe University), <https://perma.cc/QA8H-JBE5> (distinguishing the concept of economic espionage from the Turkish legal concept of “military and political espionage” with reference to 18 U.S.C. ch. 90, § 1831 et seq. as an example related to the former).

<sup>2</sup> *Türk Ceza Kanunu* [Turkish Penal Code (TPC)], Law No. 5237, Official Gazette (O.G.) No. 25611, Oct. 12, 2004, <https://perma.cc/7MGF-ZZFB>. The best publicly available translation of the TPC accessible to the Law Library is the 2016 translation published by the Council of Europe, which is available at <https://perma.cc/5SQ5-UPT8>. Although the translation is of good quality, there are occasional inconsistencies in word choice, and the text does not reflect post-2016 amendments (which are not relevant to the subject of this report). This translation is used in this report where possible.

<sup>3</sup> See, e.g., Arslan, *supra* note 1, at 581; Mehmet Yayla, *Devlet Sırlarına Karşı Suçlar ve Casusluk* [Crimes Against State Secrets and Espionage] 73-74 (2010) (Ph.D. Thesis, Ankara University), <https://perma.cc/Q58M->

there is some evidence suggesting that, at a minimum, one “political espionage” offense may be applicable to at least some acts that can be considered “economic espionage.” We were unable to find any judicial precedent that indicates acts of economic espionage are normally prosecuted under any offense related to espionage or violation of state secrets. Research found only one reported instance in the last five years where suspects were indicted for espionage offenses and offenses against state secrets on the basis of alleged acts that seem to involve solely the unauthorized disclosure of commercial information to foreign private parties.<sup>4</sup>

Nonetheless, the TPC includes an offense that specifically criminalizes the disclosure of confidential economic, industrial, or commercial information to unauthorized persons in the context of the protection of commercial and trade secrets. Although not formulated as an espionage offense, this offense may apply to certain acts that would typically constitute elements of economic espionage.<sup>5</sup>

Certain provisions of the Turkish Commercial Code, Anti-Smuggling Law, and Banking Law setting forth penalties for the filing of fraudulent corporate registration information, import/export documentation, and banking customer information are also presented in this report.<sup>6</sup>

## II. Espionage Legislation

### A. Espionage Offenses and “Offenses Against State Secrets”

Espionage and unauthorized disclosure or use of information protected as state secrets are criminalized by a number of offenses provided in the TPC.<sup>7</sup> These offenses generally apply to the unauthorized obtaining or using of certain classes of information that constitute “state secrets.”<sup>8</sup>

---

MU9G. (Nevertheless, Yayla suggests that article 333 of the TPC may function to counter economic espionage. This does not appear to be practical, for reasons explained in Section II.A.2, *infra*.)

<sup>4</sup> See Section IV, *infra*.

<sup>5</sup> See discussion of article 239 of the TPC in Section II.B, *infra*.

<sup>6</sup> See Section III, *infra*.

<sup>7</sup> TPC arts. 326, 327, 329, 332-334, & 339.

<sup>8</sup> While the TPC does not provide a definition of “state secret,” other legislation provides slightly varying but overlapping definitions of the concept. See Court of Cassation, 16th Criminal Chamber, 2016/6690 E., 2018/604 K., Mar. 8, 2018, for an overview of definitions provided in legislation and the literature, albeit refraining from reaching an exhaustive synthetic definition. Nevertheless, the definitions provided in the Criminal Procedure Code (CPC) and the 2006 State Secrets Law bill (apparently abandoned) appear to be representative of the general tendency. Article 47 CPC provides “[i]nformation that, due to its nature, may harm the foreign relations of the State, the national defense, or national security or may endanger the constitutional order and foreign relations shall be considered state secrets,” while article 3 of the bill provided “[i]nformation and documents that, should it be disclosed or obtained, due to its nature, may harm the foreign relations of the State, the national defense, or national security, or may endanger the constitutional order and foreign relations, and for these reasons must remain secret.” *Ceza Muhakemesi Kanunu (CPC)*, Law No. 5271, O.G. No. 25673, Dec. 17, 2004, <https://perma.cc/U8U2-ZVHR>; *Devlet Sırrı Kanunu Tasarısı*, Legislative Session No. 24/2, Bill No. 1/484, <https://perma.cc/9ATD-VPLD>. Note that these definitions do not specifically invoke the commercial interests of the state. See also Rukiye Akkaya Kia, *Devlet Sırrı, Kimin Sırrı? (State Secret, Whose Secret?)*, 19 *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 749 (Special Issue 2013),

The offenses do not require an intent to engage in espionage, which is interpreted as obtaining confidential information without authorization on behalf of a foreign state or organization for transmission of the information to the third party to Turkey's detriment.<sup>9</sup> Espionage offenses,<sup>10</sup> on the other hand, require the intention to commit espionage defined as such.<sup>11</sup>

### 1. *Espionage Offenses*

The following are the espionage offenses provided in the TPC:

- Securing information that, due to its nature, must be kept confidential for reasons relating to the security or domestic or foreign political interests of the state, for the purpose of political or military espionage (art. 328).
- Disclosing information that, due to its nature, must be kept confidential for reasons relating to the security or domestic or foreign political interests of the state, for the purpose of political or military espionage (art. 330).
- Securing information that, due to its nature, must be kept confidential for reasons relating to the security, or domestic or foreign political interests of another foreign state (art. 331; for this offense to be applicable to a non-Turkish national, the securing of the information must occur in Turkey – the offense applies to Turkish nationals extraterritorially).
- Securing, for the purpose of military or political espionage, information that, due to its nature, must be kept confidential and the disclosure of which is prohibited by a regulatory act of a competent authority in accordance with the law (art. 335).
- Disclosing, for the purpose of military or political espionage, information that, due to its nature, must be kept confidential and the disclosure of which is prohibited by a regulatory act of a competent authority in accordance with the law (art. 337).
- Enabling or facilitation of the commission of any of the above offenses due to a failure to exercise due care and attention (art. 338).

The subject matter of these six “espionage offenses” is limited in scope to “military and political espionage.” Moreover, other than the article 335 and 337 offenses, which require the relevant information to be classified by a positive act by a state authority, espionage offenses protect information that “relates to the domestic or foreign political interests” of the Turkish state or a foreign state.

“Military espionage” in the context of the espionage offenses refers to “the collection of military information to the benefit a foreign state and to the detriment of the State of the Republic of

---

<https://perma.cc/3DDN-VC5W> (criticizing the indeterminacy of the concept of “state secret” in Turkish law and expressing disappointment with the paucity of research on the subject in the Turkish literature).

<sup>9</sup> See Court of Cassation, 16th Criminal Chamber, 2016/6690 E., 2018/604 K., Mar. 8, 2018; Arslan, *supra* note 1, at 575.

<sup>10</sup> TPC arts. 328, 330, 331, 335, 337, & 338.

<sup>11</sup> With the exception of art. 338, which is formulated as a criminal negligence offense.

Turkey.”<sup>12</sup> On the other hand, there appears to be some lack of clarity as to the precise scope of “political espionage” and as to whether it relates to at least some classes of economic information. The explanatory memorandum accompanying the TPC defines “political espionage” as the collection, to the benefit of a foreign state and to the detriment of the Turkish state and its citizens and residents, of “all information related to public health, *financial information*, and information concerning national morale, that must be kept secret” (emphasis added).<sup>13</sup> There is no clear indication in court or prosecutorial practice that the reference to *financial information* in the explanatory memorandum is taken as referring to economic, industrial, commercial, or financial information that is not otherwise directly related to national defense and public order and security. The literature appears to be equally silent or equivocal.<sup>14</sup> Finally, there appears to be limited legislative guidance and no judicial guidance regarding the proper interpretation of the concept of “domestic or foreign political interests” that limit the type of information protected by the relevant espionage offenses. However, this language, in the context of the rest of the TPC, appears to exclude purely economic and commercial interests that are not directly related to the defense of the state and the maintenance of the constitutional order.<sup>15</sup>

In light of the above, an indictment that reportedly was brought in 2020 under article 328, discussed in Section IV below, appears to be uncharacteristic. Nevertheless, if the reports are accurate, it is illustrative of article 328’s potential to be used against alleged acts of economic espionage.

## 2. Offenses Against State Secrets

In addition to the espionage offenses, the TPC provides for a class of offenses that involve the violation of state secrets and certain other types of information that the law requires be kept confidential. Four offenses criminalize the unauthorized destruction and alteration or falsification of documents “relating to the security of the State or the domestic and foreign political interests of the State,” in various configurations.<sup>16</sup> Economic information is excluded from the scope of these offenses, and therefore, they are not applicable to economic espionage.

---

<sup>12</sup> Court of Cassation, 16th Criminal Chamber, 2016/6690 E., 2018/604 K., Mar. 8, 2018 (quoting the explanatory memorandum of the TPC, Türk Ceza Kanunu Tasarısı Gerekçesi (Explanatory Memorandum for a bill to adopt the Turkish Penal Code), Legislative Session No. 22/2, Bill No. 1/593, <https://perma.cc/N3XW-MD4D>).

<sup>13</sup> TPC Explanatory Memorandum, explanations to article 388 (enacted as article 328).

<sup>14</sup> Nevertheless, Arslan suggests that, if prosecuted, acts of economic espionage should theoretically be prosecuted under the article 328 (instead of article 239, see Section II.B below) because of the legislature’s apparently broad definition of “political espionage,” although elsewhere in his text he argues that political espionage appears to be distinguished in the broader context of the law from economic espionage, which is not explicitly criminalized in the code and thus should not be prosecuted in accordance with the principle of *nulla poena sine lege* (no punishment without law) as explanatory memoranda are not law. See Arslan, *supra* note 1, at 580 fn. 1443, 597.

<sup>15</sup> Cf. Arslan at 269; also compare TPC art. 305(4) (defining “fundamental national interests” as “the independence, territorial integrity, national security, and the fundamental characteristics of the Republic as provided in the Constitution”).

<sup>16</sup> This formulation is common to arts. 326, 327, 329, and 339. While the definition of “domestic and foreign political interests of the State” is (like the concept of “state secret” as discussed above) not clearly and precisely defined in the TPC or other legislative and judicial sources, the explanatory memorandum of the TPC explicitly distinguishes between “political interests” and “economic, and cultural [interests]” and excludes the latter

Another provision makes it a crime for persons to use or cause to be used, without authorization and for their own benefit or that of another, “scientific discoveries or new inventions, or industrial innovations that state security necessitates to be kept confidential” that the persons have obtained by virtue of their office.<sup>17</sup> The prominent view in the legal literature appears to be that “office” should be interpreted as “public office,” and therefore that the offense can only be committed by public servants or persons otherwise charged with public service.<sup>18</sup> Furthermore, the reference to “state security” is likely to be interpreted to refer to the defense of the country and the maintenance of the constitutional order and its functioning.<sup>19</sup> There appears to be no significant guidance in the legislative history or judicial precedent suggesting that this provision covers economic and industrial information that is not closely related to national defense and the fundamental state interest in public order and security. Likewise, the “necessitates to be kept confidential” formulation appears to be interpreted as the information being analogous to a “state secret,” which in Turkish practice appears to presumptively exclude information that is purely of economic, financial or commercial importance, rather than directly endangering foreign relations, the national defense, or the constitutional order.<sup>20</sup>

## B. Offense Against Commercial and Trade Secrets (Article 239 TPC)

Article 239 of the TPC criminalizes the disclosure to an unauthorized person of confidential banking information, confidential customer information, and trade secrets, “including scientific discoveries and inventions and industrial applications,” by a person who is in possession of such information by virtue of his office, profession, or trade. The offense is punishable by one to three years of imprisonment and a fine. The offense can also be committed by persons who are in possession of the relevant information illegally. Significantly, where the information is disclosed

---

from the intended scope of the offenses using this formulation. Because economic interests are explicitly excluded, and no judicial precedent appears to suggest otherwise, it can be inferred with some certainty that the offenses listed in these articles do not apply to acts of economic espionage. Therefore, this report does not discuss the applicability and interpretation of these offenses in detail and concludes that they do not apply to acts typical of economic espionage. Nevertheless, according to the media article mentioned in Section IV, *infra*, reporting on a trial wherein suspects were prosecuted for acts typical of economic espionage, at least some suspects were reported to have been charged with an article 327 crime. As discussed in Section IV, *infra*, this practice appears to be unusual. Article 327 states, “Any person who secures information that, due to its nature, is to be kept confidential for reasons relating to the security or domestic or foreign political interests of the State shall be sentenced to a penalty of imprisonment for a term of three to eight years.”

<sup>17</sup> TCP art. 333.

<sup>18</sup> Zeki Hafizoğulları & Özgür Küçüktaşdemir, *Devlet Sırlarına Karşı Suçlar ve Casusluk* [Crimes Against State Secrets and Espionage], 2 *Başkent Üniversitesi Hukuk Fakültesi Dergisi* 123, 152-53 (2015), <https://perma.cc/6FAJ-LBF6>; Hacı Sarıgüzel, *Devlet Sırlarına Karşı Suçlar ve Casusluk Suçları* [Crimes Against State Secrets and Espionage Crimes] 286 (2016) (Ph.D. Thesis, Kocaeli University, <https://perma.cc/78XW-44PQ>; cf. TPC Explanatory Memorandum, explanations to art. 394 (enacted as art. 333) (“Offenders can be a public servant or other person mandated with public service. . . .” The ambiguity introduced by the “can be” formulation exists in the Turkish text, but this statement appears to be consistently interpreted as indicating an exclusive class of offenders in the literature).

<sup>19</sup> Arslan, *supra* note 1, at 365; cf. Hafizoğulları & Küçüktaşdemir, *supra* note 18, at 153.

<sup>20</sup> See discussion in note 8, *supra*; Arslan, *supra* note 1, at 105; cf. Zeki Hafizoğulları & Muharrem Özen, *Türk Ceza Hukukunda Devlet Sırrına Genel Bir Bakış* [An Overview of the Concept of State Secret in Turkish Criminal Law], 68(1) *Ankara Barosu Dergisi* 21, 24 (2010), <https://perma.cc/LLW9-DW5U>.

to an unauthorized foreign person not resident in Turkey or such person's agents, the penalty is enhanced by one-third, and the prosecution of the offense is not conditioned on a complaint by the victim, which is the otherwise necessary for prosecution. Finally, any person who coerces by use of force or threat the disclosure of protected information is punishable by three to seven years in prison. All said, the article 239 offense is not formulated as an espionage offense, which means the disclosure is not required to be made on behalf of a foreign state or organization to the detriment of the Turkish state.<sup>21</sup>

### C. Export Control Legislation

Communiqué No. 96/31 of the Prime Minister's Undersecretariat of Foreign Trade provides the list of goods whose export out of Turkish customs borders is prohibited or subject to permit and designates the agencies that are responsible for issuing permits.<sup>22</sup> The procedures for the issuance of permits are generally provided by the specialized legislation that designates the goods in question for inclusion in the restricted goods list of Communiqué No. 96/31. For example, the rules and principles governing the issuance of export permits and oversight for the export of nuclear dual-use technologies, which is restricted by inclusion in Communiqué No. 96/31, is provided in the Regulation on Nuclear Export Control.<sup>23</sup>

Violations of the export control rules are punishable under article 3(8) of the Anti-Smuggling Law, which criminalizes the export of goods whose export is prohibited by law.<sup>24</sup> The offense is punishable by one to three years in prison and a criminal fine, unless the act constitutes a more serious offense.<sup>25</sup>

---

<sup>21</sup> But see Arslan, *supra* note 1, at 597 (arguing that an article 328 charge is a theoretically more appropriate option than an article 239 charge for prosecution of economic espionage because of the legislature's apparent intent to include at least financial information within the scope of "political espionage," although also arguing that an act of economic espionage could not be prosecuted under the current language of the law, see discussion at note 14, *supra*).

<sup>22</sup> İhracı Yasak ve Ön İzne Bağlı Mallara İlişkin Tebliğ (İhracat 96/31), O.G. No. 22762, Sept. 19, 1996, as amended, <https://perma.cc/ZSE8-F23P>.

<sup>23</sup> Nükleer İhracat Kontrolü Yönetmeliği, O.G. No. 31038, Feb. 13, 2020, <https://perma.cc/UAE2-HZR5>. This regulation is part of Turkey's legal framework for the peaceful use of nuclear power in accordance with Turkey's obligations under the Nuclear Non-Proliferation Treaty. *Id.* arts. 9-10.

<sup>24</sup> Kaçakçılıkla Mücadele Kanunu [Anti-Smuggling Law (ASL)], Law No. 5607, O.G. No. 26479, Mar. 31, 2007, <https://perma.cc/P7F5-RAXZ>.

<sup>25</sup> *Id.* art. 3(8). A more serious offense that might be particularly relevant to the application of article 3(8) of the ASL is provided in article 174 of the TPC, which criminalizes the export, without the permission of the competent authorities, of "nuclear, radioactive, chemical or biological substances which have explosive, burning, corrosive, harmful, suffocating or toxic properties, or are capable of causing permanent illness [or] items or equipment which are necessary for the production, or processing, of these substances" (emphasis added). The export control regime certainly covers some goods that fall under the scope of this provision. The offense is punishable by three to eight years of imprisonment and a fine.

### III. The Standard of Prosecution and Penalties for Certain Specified Offenses

#### A. General Standard of Prosecution

The general standard of prosecution under the Criminal Procedure Code governs the prosecution of all offenses discussed in this report.<sup>26</sup>

The criminal process starts with the investigation phase.<sup>27</sup> If, at the end of the investigation, the prosecutor has gathered evidence establishing “sufficient suspicion” that the suspect has committed a crime, the public prosecutor must prepare an indictment to be filed with the appropriate criminal court.<sup>28</sup> “Sufficient suspicion” denotes a medium level of suspicion within the system of the CPC; it refers to a level of suspicion that is stronger than the “reasonable suspicion” that is necessary for the prosecutor to initiate a criminal investigation but weaker than the “strong suspicion” that is required for the court to order certain security measures such as pretrial detention. The indictment must explain the events that constitute the charged crime, connecting them with the evidence presented in the indictment. The indictment must include not only points that are unfavorable to the defendant but also favorable points.<sup>29</sup> The indictment must include in its conclusion a clear statement indicating which of the penalties and security measures provided in the law are being requested. If, by the end of the investigation phase, the prosecutor has not gathered evidence that establishes sufficient suspicion, or if there is no legal possibility for adjudicating the offense, the prosecutor must issue a “no ground for prosecution” decision.<sup>30</sup> A criminal action cannot be brought for the same acts for which a no ground for prosecution decision has been issued unless new evidence comes to light that establishes sufficient suspicion and a criminal court justice of the peace orders the resumption of the criminal process.<sup>31</sup>

#### B. Filing Fraudulent Corporate Registration Information

Making statements or submitting documents that include a misrepresentation of facts with an intention that the false information be recorded in the national trade registry is punishable by an administrative fee of 2,000 Turkish liras (about US\$129).<sup>32</sup> However, if misrepresentations are made in furtherance of an offense provided in the TPC, the public prosecutor may press charges under the latter.<sup>33</sup> Public officials discovering a potentially fraudulent misrepresentation in the national trade registry are required to notify the public prosecutor.<sup>34</sup> Offenses that might be

---

<sup>26</sup> See CPC, *supra* note 8.

<sup>27</sup> Id. art. 160.

<sup>28</sup> Id. art. 170(2).

<sup>29</sup> Id. art. 170(5).

<sup>30</sup> Id. art. 172(1).

<sup>31</sup> Id. art. 172(2).

<sup>32</sup> Türk Ticaret Kanunu [Turkish Commercial Code (TCC)], Law No. 6102, as amended, art. 38, O.G. No. 27846, Feb. 14, 2011, <https://perma.cc/MM8W-MLGA>.

<sup>33</sup> TPC art. 5.

<sup>34</sup> TCC art. 51.

particularly relevant in the TPC are provided in articles 204 (“counterfeiting official documents”), 206 (“providing false information in the course of the issuance of an official document”), and 207 (“counterfeiting private documents”).

The TPC article 204 offense criminalizes the counterfeiting or fraudulent alteration or emendation of an official document and the use of such a document. The offense is punishable by two to five years in prison. While fraudulently created corporate documents prepared to be registered in the trade registry would not be considered as “official documents” under this offense (as they are not prepared by a public official), and would be subject to prosecution per se under the article 207 offense that criminalizes the same actions with relation to private documents (punishable by one to three years of imprisonment), it appears that, in practice, the offender may be charged under article 204 where the counterfeited private document is used to cause the creation of an official document.<sup>35</sup> It is not clear whether a falsified corporate document is thus “officialized” by registration in the national trade registry. Nevertheless, the article 206 offense may also be relevant in this context, criminalizing the submission of false information to a public official in order to obtain an official document, which is punishable by three months to two years in prison.

### C. Filing Fraudulent Export/Import Documentation

Article 3 of the ASL sets forth a number of customs violation offenses that are particularized according to goods being trafficked in and out of the customs borders illegally and the method of illegal trafficking.<sup>36</sup> One particularly relevant smuggling offense provided under article 3 of the ASL was introduced in Section II.C above. Article 4 of the ASL provides aggravating factors for the smuggling offenses provided in article 3. Two aggravating factors may be relevant: Article 4(5) provides that, where the smuggling offense is committed by the use of a falsified document, the offender will additionally be charged with the relevant counterfeiting document offense (see the explanation of these offenses above). Article 4(7) provides that, if the goods involved in the smuggling offense are of a nature that might “endanger the political, *economic*, or military security” (emphasis added), the penalty for the smuggling offense must not be less than 10 years of imprisonment, unless the act constitutes a more serious offense.

### D. Filing False Customer Information with Banking Entities

Under the Banking Law, it is an offense to submit falsified information to entities regulated under the law that results in the entities publishing or providing to auditors and courts mandatory documents that contain false information.<sup>37</sup> The offense is punishable by one to three years in prison.<sup>38</sup> Note that, according to the conceptual merger rule provided in the Banking Law, if an

---

<sup>35</sup> Hasan Tahsin Gökcan, *Özel Belgede Sahtecilik Suçu (TCK M.207) [Criminal Forgery of Private Document (TCK Article 207)]*, 68(1) Ankara Barosu Dergisi 209, 222 (2010), <https://perma.cc/J7ZW-VZUY>.

<sup>36</sup> ASL arts. 3(1)-(2), 4.

<sup>37</sup> Bankacılık Kanunu [Banking Law], Law No. 5411 art. 155, O.G. No. 25983bis, Nov. 1, 2005, <https://perma.cc/WCV4-6YYN> (unofficial English translation).

<sup>38</sup> Id.

offender commits another offense by the same action that is criminalized under the Banking Law, the offender must be convicted only of the offense with the heavier penalty.<sup>39</sup>

#### IV. Examples from the Past Five Years of Convictions Based on Violations of Export Controls or for Economic Espionage

As explained above, Turkish law does not provide for specific rules concerning economic espionage. Nevertheless, the Turkish daily *Sabah* reported in December 2020 that six individuals were indicted for periodically providing information to a foreign company regarding Turkey's natural gas imports. According to the news report, a trial commenced in the Istanbul Court of Serious Crimes. The defendants included an executive of an energy company and the son of a retired Council of State judge. The report specifically states that information regarding Turkey's natural gas imports is secret.<sup>40</sup> The report also states that the main suspects, including the executive of the energy company, were charged with a TPC article 328 offense and that several other suspects were charged with an article 327 offense in relation to the same acts.<sup>41</sup>

We were unable to find any information as to the status or outcome of the case. We were also unable to find any report of a conviction made public in the last five years resulting from the violation of the export control regime.

#### V. Conclusion

Economic espionage is not specifically criminalized in Turkish law. The TPC includes espionage offenses and offenses related to the violation of state secrets. While this framework does not explicitly cover acts that can be considered economic espionage, there is some support in the legal literature for the possibility of prosecuting acts of economic espionage under article 328's espionage offense. There are also strong counterarguments to this interpretation of article 328, however, and the majority view appears to be that the TPC framework does not criminalize acts typical of economic espionage. That said, we were able to identify one instance where unauthorized disclosure of economic information belonging to a private company reportedly was prosecuted under article 328, with an unknown outcome. In light of the paucity of supporting high court precedent and support in the legal literature, this prosecution appears to be uncharacteristic. It can be considered a case in which economic espionage is marginally a factor because the sensitive nature of the information concerned—energy imports—is more directly relevant in the context of national security.

The TPC's article 239 offense appears more appropriate for prosecuting acts of economic espionage than provisions regarding espionage and state secret offenses. Article 239 essentially criminalizes the unauthorized disclosure of trade secrets and intellectual property by persons

---

<sup>39</sup> Id. art. 161.

<sup>40</sup> Fatih Ulaş, *Enerji casusluğu çetesi ilk kez hakim karşısında! Ayda 1500 TL'ye devletin gizli bilgilerini sattılar . . .* [The Energy Espionage Gang Is Before the Judge for the First Time! They Sold Confidential Information of the State for TL 1500 per Month . . .], *sabah.com.tr* (Dec. 23, 2020), <https://perma.cc/36GY-MF29>.

<sup>41</sup> Id. The report also states that the court decided to conduct the trial in closed hearings due to the secret information involved. As is the ordinary practice in Turkey, the indictment has not been made public.

privity to confidential material by virtue of their positions. A significant feature of this offense is that, while the prosecution of disclosure to a foreign person not resident in Turkey is not conditioned on the complaint of the victim, prosecution of disclosure to other persons is. Another feature of the article 239 offense is that the penalties are much lighter than those set forth for the espionage and state secret offenses.

# Turkmenistan

*Peter Roudik*  
*Director of Legal Research*

**SUMMARY** The Turkmen Law on Commercial Secrets appears to be the governing act in protecting economic information. It defines what content constitutes secret information and provides the rules for establishing secrecy protection regimes. Various sectoral laws may define additional information as confidential. Punishment for illegal access to and disclosure of information containing commercial and banking secrets is provided by the Criminal Code. Fraudulent activities by private corporations are prosecuted as misdemeanors unless these actions did not inflict serious or very serious damage. No information about the handling of crimes discussed in this report by Turkmen courts has been located, mainly because of maintaining the confidentiality of judicial proceedings.

## I. Economic Espionage Legislation

In 2000, the Law on Commercial Secrets was passed in Turkmenistan. This law defines commercial secrets as “information about economic, financial, technological, industrial, and other activity of an enterprise, organization or individual businessperson, which is not a state secret, if its disclosure or transfer would damage business interest and activities” of the business in question.<sup>1</sup> The law applies to protecting commercial secrets of foreign legal entities and their branches working in Turkmenistan.<sup>2</sup> According to the law, a commercial secret must have the following characteristics:

- real or potential commercial value for the information holder because of its nondisclosure to third persons,
- not widely known or publicly accessible, and
- protected confidentiality of the information through purposefully developed measures, such as establishing internal rules for usage and access, the marking of documents, record keeping, etc.<sup>3</sup>

The following information can be classified as a commercial secret:

- information on the technologic, organizational, marketing, advertising, intellectual, and other specific aspects of a business,

---

<sup>1</sup> Law of Turkmenistan on Commercial Secrets of Dec. 19, 2000, (Law on Commercial Secrets), art. 1, <https://perma.cc/4RNM-P7GR> (in Russian).

<sup>2</sup> Id. art. 2.

<sup>3</sup> Id. art. 4.

- information about professional, business, financial, and other interests of the organization,
- information about the organization's management structure, financing sources, concluded contracts, prices, customers, and suppliers,
- non-patented scientific projects developed by the organization or enterprise,
- databases and computer programs created by staff or owners of the business,
- accounting documents, and
- other information classified as a commercial secret in accordance with national legislation.<sup>4</sup>

In regard to bank secrecy, the law states that information about a bank's customers, their transactions and accounts, allocation of a bank's assets, and financial resources for banking operations are recognized as commercial secrets.<sup>5</sup>

Information containing commercial secrets can be disclosed to government officials performing oversight functions, insurance companies, investigators, and judges.<sup>6</sup>

The holder of information must establish the rules for access to and protection of information containing commercial secrets. This information can be divided into the following four categories: for official use, confidential, strictly confidential, and for the recipient only. It is an information holder's obligation to maintain records on the transfer of this type of information to third persons.<sup>7</sup>

The law states that officials, employees, and other physical and legal persons should be liable for violating rules concerning the usage, disclosure, preservation, and protection of commercial or banking secrets.<sup>8</sup> Under article 250 of the Turkmen Criminal Code, individuals who are convicted for unlawful access to such information or its disclosure are subject to varied punishments depending on the specifics of the crime committed. Correctional labor for up to two years is prescribed for collecting information containing commercial or banking secrets with the purpose of illegal usage or disclosure, if this was done by stealing documents, bribing or threatening individuals who have access to this information or their relatives, or intercepting information in communications networks. The same actions committed with the purpose of receiving personal financial gains are punishable by higher fines or correctional labor for a period of up to two years, if such actions inflicted significant damage on the information holder.<sup>9</sup>

---

<sup>4</sup> Id. art. 7.

<sup>5</sup> Id.

<sup>6</sup> Id. art. 11.

<sup>7</sup> Id. art. 8, 9.

<sup>8</sup> Id. art. 17.

<sup>9</sup> Criminal Code of Turkmenistan, adopted June 12, 1997, art. 250, <https://perma.cc/CP56-RW94> (in Russian).

## II. Prosecution of Fraudulent Activities of Private Corporations

Corporate registration is mandatory in Turkmenistan and is regulated by the Law on Companies.<sup>10</sup> Conducting business activities without registration, possession of a license when obtaining proper licenses is required, or violation of licensing conditions is considered illegal entrepreneurship. It constitutes an administrative violation (misdemeanor), which is punishable by a fine with a possible confiscation of means of business, products, and raw materials. The amount of the fine depends on the amount of inflicted damage or the amount of illegally received profits. Heavier fines and a detention for a term of up to 15 days are foreseen for repeated violations. The large amount of damage is the monetary amount equal to the sum in the range of between 100 and 500 average monthly worker salaries.<sup>11</sup> The exact amount of an average monthly worker salary is established by the Turkmen government annually. Cases where illegal entrepreneurship results in inflicting large damage on individuals, organizations, or the state, or obtaining profits exceeding an amount equal to 500 average monthly worker salaries are recognized as criminal offenses punishable by a fine or correctional labor for a term of up to two years.<sup>12</sup> Criminal punishment for illegal banking activities is heavier and may include imprisonment for a period of up to one year. A punishment in the form of a three-year imprisonment is prescribed for the same crime if committed by a group of people.<sup>13</sup> Prosecution of illegal entrepreneurship is conducted under general rules established by criminal procedural legislation. No special evidentiary threshold is prescribed.

Export violations are not specified as a crime by Turkmen legislation; however, goods transferred through the customs border without following the established rules are considered contraband. The prescribed punishment for contraband is imprisonment for up to 10 years. The length of the imprisonment depends on the category of transferred goods and other qualifying characteristics.<sup>14</sup>

Submission of false information and documents required for business and tax registration by an individual and delayed submission of information required for business control and taxation by a head of a legal entity constitute separate misdemeanors punishable by fines.<sup>15</sup>

## III. Examples of Convictions for Violations of Export Controls or Economic Espionage

According to a report by the European Bank for Reconstruction and Development (EBRD), the “executive dominates the judiciary, and the law requires that all judicial decisions be kept confidential.” As the EBRD report says, “[t]he extent to which the courts are used to resolve

---

<sup>10</sup> Law of Turkmenistan on Companies, No. 28 of June 15, 2000, arts. 14-16, <https://perma.cc/DWC3-AATC> (in Russian).

<sup>11</sup> Code of Turkmenistan on Administrative Violations, adopted Sept. 13, 2013, art. 283, <https://perma.cc/8X5B-UMQQ> (in Russian).

<sup>12</sup> Criminal Code of Turkmenistan, adopted June 12, 1997, art. 239, <https://perma.cc/CP56-RW94> (in Russian).

<sup>13</sup> *Id.* art. 240.

<sup>14</sup> *Id.* art. 254.

<sup>15</sup> Code on Administrative Violations art. 286.

commercial or other disputes in Turkmenistan is not known, as court decisions, case files and most court data are not publically [sic] available, even to lawyers.”<sup>16</sup>

Espionage-related cases are investigated by the Turkmenistan State Committee for National Security. The jurisdiction of the committee includes export control issues if such cases might affect national security.<sup>17</sup> Information on these cases is classified, and no reports about court decisions issued in Turkmenistan were located in Turkmen open source media. The Turkmen branch of Radio Free Europe/Radio Liberty reported about alleged attempts by Turkmen authorities to recruit individuals in Uzbekistan to provide information about Russian and Chinese companies operating in Uzbekistan. Uzbek television reported about “unfriendly activities” by Turkmen special services against Uzbekistan. Reportedly, several employees of Uzbek enterprises located along the Uzbek-Turkmen border were accused of espionage for Turkmenistan in 2013-2014.<sup>18</sup>

---

<sup>16</sup> EBRD, *Commercial Laws of Turkmenistan: An Assessment by the EBRD* (July 2014), <https://perma.cc/FUA7-KVZG>.

<sup>17</sup> Law of Turkmenistan No. 283 of Mar. 21, 2012, on Bodies of National Security in Turkmenistan (last amended Aug. 22, 2020), art. 3, <https://perma.cc/8VRP-Q2Q7> (in Russian).

<sup>18</sup> Khurmat Babadzhanov, *Relatives of a Former Uzbek Serviceman Accused of Espionage for Turkmenistan Demand His Release from Prison*, Radio Ozodlik (Mar. 19, 2021), <https://perma.cc/7Q8K-P9LA> (in Russian).

# United Arab Emirates

*George Sadek*  
*Foreign Law Specialist*

**SUMMARY** There does not appear to be any comprehensive law in the United Arab Emirates (UAE) criminalizing economic espionage. However, there are a number of federal laws criminalizing the passing to foreign countries of economic information that damages the state's economic interests and the unauthorized disclosure of trade secrets. Those laws include the UAE's penal code, commercial corporations law, and patent protection law. In 2018, the UAE's General Prosecution Office charged British academic Matthew Hedges under the Emirati penal code with spying for MI6, a United Kingdom intelligence agency. The prosecution alleged that Hedges jeopardized the UAE's economic security.

## **I. Federal Laws on Economic Espionage and Unauthorized Disclosure of Industrial Secrets**

There does not appear to be any comprehensive law in the United Arab Emirates (UAE) criminalizing economic espionage. However, there are a number of federal laws criminalizing the passing of information to a foreign country that damages the state's economic interests and the unauthorized disclosure of trade secrets.

### **A. Federal Decree-Law No. 7 of 2016 Amending the Penal Code**

#### *1. Passing Information to a Foreign Country That Damages the State's Economic Interests*

The UAE's federal laws do not appear to mention specifically the act of procuring sensitive or foreign-controlled technologies. However, they criminalize the act of passing information to foreign countries that would damage the economic interests of the state.

Federal Decree-Law No. 7 of 2016 punishes persons who provide any type of information to an enemy of the UAE. It states, "Any person who assists the enemy or a country or a hostile group or a group with intent to harm the security of the State, by giving information or assists as a guide thereof shall be sentenced to death."<sup>1</sup>

Furthermore, under article 155 of the law, any person who communicates or seeks to communicate with a foreign country or any of its agents to damage the military, political, or economic interests of the UAE faces life imprisonment. In wartime, the punishment for the offense is execution.

---

<sup>1</sup> Federal Decree-Law No. 7/2016 Amending Federal Law No. 3 of 1987 on the Penal Code, issued on Sept. 18, 2016, art. 152, <https://perma.cc/N2DW-EUNW> (in Arabic); <https://perma.cc/YP3M-MF5L> (unofficial English translation).

## 2. *Unauthorized Disclosure of Secrets*

The Emirati penal code punishes unauthorized disclosure of secrets. Any persons who, by virtue of their profession, craft, position or art, are entrusted with a secret and divulge it, whether for their own interest or that of another person, are punishable by imprisonment for not less than one year, a fine of not less than 20,000 dirhams (about US\$5,450), or both. If the person disclosing a secret is a government employee, the penalty is imprisonment for up to five years.<sup>2</sup>

### **B. Federal Law No. 2 of 2015 on Commercial Corporations**

The UAE's law on commercial corporations, Federal Law No. 2 of 2015, penalizes any persons who disclose secret information related to their professions. However, it does not criminalize the act of collecting information on private organizations or third-party countries. The UAE's penal code also does not criminalize such information gathering.

Federal Law No. 2 of 2015 provides sanctions against any person who commits the unauthorized disclosure of a company's trade secret or uses a trade secret for personal gain by imprisonment for up to six months, a fine between AED50,000 and AED500,000 (about US\$13,600 to US\$136,000), or both.<sup>3</sup>

### **C. Federal Law No. 17 of 2002 on the Regulation and Protection of Industrial Property for Patents and Industrial Designs**

The UAE's patent law, Federal Law No. 17 of 2002, prohibits the unauthorized disclosure, use, or publication of "know-how" concerning industrial secrets, drawings, and designs.<sup>4</sup> The law does not specify sanctions for its violation but such disclosures may be treated as violations of Law No. 7 of 2016 and Law No. 2 of 2015, discussed above.

## **II. Federal Law on Fraudulent Activities of Private Corporations**

Federal Law No. 2 of 2015 on commercial corporations regulates the activities of private corporations operating in the UAE. It imposes the penalties of imprisonment and fines against violators.

### **A. Providing False Information Pertaining to a Private Corporation**

It appears that the law on private corporations does not specifically criminalize the acts of filing fraudulent corporate registration information, filing fraudulent import-export documentation, or filing false customer information to banking entities. However, it criminalizes the general act of providing false information related to a private corporation.

---

<sup>2</sup> Id. art. 379 of the penal code as amended.

<sup>3</sup> Federal Law No. 2 of 2015, issued on June 30, 2015, art. 369, <https://perma.cc/TAQ2-Q5QC> (in Arabic); <https://perma.cc/CCX3-FFVG> (unofficial English translation).

<sup>4</sup> Law No. 17 of 2002 on the Regulation and Protection of Industrial Property for Patents, Industrial Designs, & Models, issued on Nov. 19, 2002, (as amended by Federal Law No. 31 of Oct. 1, 2006), art. 42, <https://perma.cc/2F6M-DCB9> (in Arabic); <https://perma.cc/Y6KU-VTKF> (unofficial English translation).

The law makes any person shown to have intentionally provided false information in the bylaws of a private corporation, prospectus in shares, or in any documents related to the corporation punishable by imprisonment for between six months and three years, a fine between AED200,000 and AED1 million (about US\$54,500 to US\$272,300), or both. Furthermore, any person affiliated with the private corporation who signs and distributes such false information is also subject to such punishment.<sup>5</sup>

Moreover, the law imposes criminal penalties against any manager or director of a private corporation who intentionally provides false information concerning the company's budget, profits and losses account, or financial reports, or who fails to correct material inaccuracies in such documents in order to hide the actual financial position of the company. Violators can be punished by imprisonment ranging between six months and three years, a fine between AED100,000 and AED500,000 (about US\$27,200 to US\$136,000), or both.<sup>6</sup>

Similarly, any person who in bad faith overestimates the capital shares paid in kind by the founders or partners is punishable by a term of imprisonment between six months and three years, a fine between AED500,000 and AED1 million (about US\$136,000 to US\$272,300), or both.<sup>7</sup>

#### **B. Failure to Provide Information to Inspectors or Auditors**

The law on private corporations penalizes a chief executive officer or general manager of a private corporation who intentionally fails to provide documents or information to inspectors or auditors examining the activities and transactions of the corporation. Violations are punishable by imprisonment for three months to two years, a fine between AED10,000 and AED100,000 (about US\$2,700 to US\$27,200), or both.<sup>8</sup>

#### **C. Failure to Register, to Maintain an Account Record, or to Amend Corporate Information**

The law on private corporations imposes a fine of AED1,000 (about US \$270) per day on public joint stock companies that fail to register with a capital market in the UAE.<sup>9</sup> Similarly, it imposes a fine of between AED50,000 and AED500,000 (about US\$13,600 to US\$136,000) against private corporations that do not keep accounting records reflecting their commercial transactions.<sup>10</sup> Additionally, private corporations that fail to register with the state will be fined between AED100,000 and AED500,000 (about US\$27,200 to US\$136,000).<sup>11</sup> Any private corporation that fails to timely amend its memorandum and articles of association to adhere to the provisions of the law on commercial corporations can be fined AED2,000 (about US\$540) per day.<sup>12</sup>

---

<sup>5</sup> Federal Law No. 2 of 2015, art. 361.

<sup>6</sup> Id. art. 364.

<sup>7</sup> Id. art. 362.

<sup>8</sup> Id. art. 365(2).

<sup>9</sup> Id. art. 341.

<sup>10</sup> Id. art. 348.

<sup>11</sup> Id. art. 355.

<sup>12</sup> Id. art. 357.

### III. Convictions Based on Violations of Espionage Laws

In 2018, the UAE's General Prosecution Office charged British academic Matthew Hedges under the Emirati penal code with spying for MI6, a United Kingdom intelligence service. The prosecution alleged that Hedges jeopardized the economic security of the UAE.<sup>13</sup>

Hedges was first arrested in May 2018 after an Emirati man reported to the police that Hedges had been asking about sensitive information.<sup>14</sup> According to news articles, Hedges was accused of collecting confidential information about government companies and the royal family.<sup>15</sup>

The Federal Court of Appeal's criminal chamber in Abu Dhabi found Hedges guilty of the charges. It sentenced him to life imprisonment. However, Hedges was released on bail pending Federal Supreme Court review of his case.<sup>16</sup>

In November 2018, UAE President Khalifa bin Zayed Al Nahyan pardoned Hedges. On the same day, the UAE reportedly released a video recording in which Hedges admitted he was an "active officer" for MI6. He left the UAE after receiving the presidential pardon.<sup>17</sup>

---

<sup>13</sup> UAE Charges UK Academic with Spying, German News Agency (Oct. 15, 2018), <https://perma.cc/5PED-LAEX>.

<sup>14</sup> UAE Government: Powerful and Compelling Evidence of Matthew Hedges' Guilt, National (Nov. 23, 2018), <https://perma.cc/2NDW-YZTQ>.

<sup>15</sup> Shireena Al Nowais, *British Spy Matthew Hedges Pardoned by UAE Government*, National (Nov. 27, 2018), <https://perma.cc/M67M-WRCF>.

<sup>16</sup> Shireena Al Nowais, *British Spying Trial: Matthew Hedges Sentenced to Life in Jail by Abu Dhabi Court*, National (Nov. 22, 2018), <https://perma.cc/XBM9-85UW>.

<sup>17</sup> Al Nowais, *British Spy Matthew Hedges Pardoned by UAE Government*, *supra* note 15.

# Uzbekistan

*Peter Roudik  
Director of Legal Research*

**SUMMARY** The Uzbek Law on Trade Secrets appears to be the governing act in protecting economic information. It defines what content constitutes secret information and provides the rules for establishing secrecy protection regimes. Various sectoral laws may define additional information as confidential. Punishment for illegal access to and disclosure of information containing commercial and banking secrets is provided by the Criminal Code. Fraudulent activities by private corporations are prosecuted as misdemeanors unless these actions did not inflict serious or very serious damage. No information about the handling of crimes discussed in this report by Uzbek courts has been located, although Uzbek legal scholars report about the steady increase in the number of economic espionage cases.

## I. Economic Espionage Legislation

The definition of trade secrets was introduced in Uzbek legislation by the Civil Code of Uzbekistan, which defined them as “information having commercial value in scientific, technological, industrial, financial, and other areas due to its non-disclosure to third persons, who have no free access to this information through legal means, if the holder of the secrets took measures to protect its confidentiality,” and provided for their civil law protection.<sup>1</sup>

The same definition was repeated in the 2014 Law on Trade Secrets of Uzbekistan.<sup>2</sup> This law identified legal mechanisms to address trade secrecy related issues and stipulated guiding principles for handling trade secrets. According to the law, a trade secret must have the following characteristics:

- real or potential commercial value for the information holder because of its nondisclosure to third persons,
- not widely known or publicly accessible,
- do not contain state or other secrets protected by law, and
- protected confidentiality of the information through purposefully developed measures.<sup>3</sup>

---

<sup>1</sup> Civil Code of the Republic of Uzbekistan, art. 98, adopted Dec. 21, 1995, *Vedomosti Olij Mazhlis Respubliki Uzbekistan* (official gazette), 1996, No. 2, Item 56, <https://perma.cc/JV4K-PF82> (in Russian).

<sup>2</sup> Law No. 374 of the Republic of Uzbekistan on Trade Secrets of Sept. 11, 2014 (Law on Trade Secrets), art. 3, <https://perma.cc/3SAW-E6DP> (in Russian).

<sup>3</sup> *Id.* art. 4.

The Law does not define what information can be classified as trade secrets, leaving up to the secret owner to decide the content and depth of the secrets.<sup>4</sup> However, the Law prescribes what type of information cannot be classified as trade secrets. These are:

- information about contracts subject to government registration and budget funding,
- information that can be found in the company's registration and licensing documents,
- information related to occupational, industrial, and environmental safety,
- information about the revenues, employment, use of volunteers, and remuneration of employees for non-commercial organizations,
- information about the legal violations committed by an enterprise, and
- other information specified in Uzbek laws.<sup>5</sup>

Information containing commercial secrets can be requested by government officials performing oversight functions. The refusal to provide this information in response to government requests can be disputed in a court.<sup>6</sup> The government is also prohibited from divulging commercial secrets that become known to the authorities. The law requires government officials to take measures preventing the disclosure of trade secrets they received.<sup>7</sup>

The relevant legislation does not specify bank secrecy, which is regulated by a separate law on banking secrecy. This law extends general rules for protecting confidential information to banking operations.<sup>8</sup>

The Law on Trade Secrets states that persons should be liable for violating rules concerning trade secrets.<sup>9</sup>

Protection of confidential information is regulated by article 191 of the Uzbek Criminal Code. This provision of the Criminal Code establishes two related but separate felonies. One prosecutes crimes related to illegal collecting of confidential scientific, industrial, economic, trade, or other similar information in any form with the purpose of its further use, and the other one criminalizes the intentional divulgence and use of confidential information of the same character without the information owner's consent, if these actions inflict serious damage to the business. Both crimes are punished by fines, obligatory public works, or correctional labor for a period of up to three

---

<sup>4</sup> Id.

<sup>5</sup> Id. art. 5.

<sup>6</sup> Id. art. 15.

<sup>7</sup> Id. art. 16.

<sup>8</sup> Law No. 530 of the Republic of Uzbekistan on Banking Secrecy of August 30, 2003, art. 18, <https://perma.cc/S736-QZ4Z> (in Russian).

<sup>9</sup> Law on Trade Secrets art. 19.

years. Sentencing guidelines provide for a less severe punishment for the crime of information gathering.<sup>10</sup>

The Code does not specify the qualifying method for divulging of trade secrets. It can be done orally or in written form, using mass media or social networks. It could also be done by inaction if the established secrecy protection regime has been violated by a responsible person.<sup>11</sup> According to a Uzbek law professor, the liability for divulgence of confidential information applies to a person who has access to this information in the course of his or her business duties. The illegal gathering of trade secrets becomes a crime if this information is collected through illegal means, such as stealing of documents, bribing, or threatening officials.<sup>12</sup>

If a disclosure of trade secrets inflicts material damage to the secret's owner without serious consequences, this action is recognized as a misdemeanor and is prosecuted under the Code of Administrative Violations. Varied fines are imposed for divulging trade secrets, and breaching the secrecy of communications, notarial activities, and banking operations. Higher fines are imposed on individuals if they commit this violation in the course of their official duties. Much higher fines are prescribed if personal or private information is disclosed.<sup>13</sup>

In 2016, the Uzbekistan State Committee on Privatization, Business Development, and Anti-Monopolistic Activities issued guidelines on handling confidential information containing trade secrets. These guidelines serve as a model document for businesses and, among other issues, prescribe procedures for designating people having access to corporate confidential information, define duties of officials responsible for protecting trade secrets, establish rules for determining the content of trade secrets and the period of its validity, provide for protocols to issue permits to use trade secrets, and prescribe mechanisms for protecting trade secrets.<sup>14</sup>

If trade secrets are related to information about the creation of weapons of mass destruction, means of their delivery, or other armaments, weapons, or military equipment, this information is subject to export control rules established by the Cabinet of Ministers and implemented by the External Trade Ministry.<sup>15</sup>

---

<sup>10</sup> Criminal Code of the Republic of Uzbekistan, adopted Sept. 22, 1994, last amended Jun. 23, 2022, art. 191, <https://perma.cc/5YKA-BW96> (in Russian).

<sup>11</sup> Nargiza Raimova, *On The Features of Criminal Legal Protection of Commercial Secret of An Enterprise Under the Legislation of The Republic of Uzbekistan*, Research, Justicemaker.ru, <https://perma.cc/LNF6-GXDA> (in Russian).

<sup>12</sup> Id.

<sup>13</sup> Code of Administrative Violations of the Republic of Uzbekistan, adopted on May 7, 1994, last amended May 18, 2022, art. 46, <https://perma.cc/28V2-76N2> (in Russian).

<sup>14</sup> Order of the Uzbekistan State Committee on Privatization, Business Development and Anti-Monopolistic Activities No. 01/26/40 of June 21, 2016 on Approval of the Model Regulation on Compliance with the Trade Secrecy Regime for Enterprises and Organizations, <https://perma.cc/F5HP-65Y7> (in Uzbek).

<sup>15</sup> Law of the Republic of Uzbekistan No. 658 of Aug. 26, 2004 on Export Control, art. 3, <https://perma.cc/4TQ5-GY49> (in Russian).

## II. Prosecution of Fraudulent Activities of Private Corporations

Corporate registration is mandatory in Uzbekistan and is regulated by the Government Regulation on State Registration of Enterprises.<sup>16</sup> Conducting business activities without registration, providing false information to the registering authorities, not possessing a license when obtaining proper licenses is required, or violation of licensing conditions is considered illegal entrepreneurship and/or a violation of licensing requirements. These acts constitute an administrative violation (misdemeanor), which is punishable by fines with a confiscation of the “objects of the violation.”<sup>17</sup> A separate misdemeanor is not informing the state about a change of business address, banking information, or re-registration of an enterprise.<sup>18</sup> The amount of the fine depends on the amount of inflicted damage or the amount of illegally-received profits.

Cases where entrepreneurial activities result in receipt of uncontrolled income in an especially large amount constitute a criminal offense of illegal entrepreneurship punishable by a fine, correctional labor, restrictions on freedoms, or imprisonment for a term of up to five years.<sup>19</sup> A heavier punishment is foreseen for acceptance of illegal investments.<sup>20</sup> Receipt of an especially large income from activities subject to licensing without applying for a license elevates this violation to the level of a crime punishable by fines and mandatory correctional labor.<sup>21</sup>

Prosecution of illegal entrepreneurship is conducted under general rules established by criminal procedural legislation. No special evidentiary threshold is prescribed. The qualifying characteristic for prosecuting a crime is the amount of income received by the perpetrator. It is measured in the equivalents to the annual government-established conventional monetary units used for calculation of government payments. A large amount constitutes the equivalent of between 300 and 500 conventional monetary units, and an especially large amount is above 500 units.<sup>22</sup> Since June 1, 2022, one unit equals Uzbekistani Sums 300,000 (approximately US\$27.50).<sup>23</sup>

Export violations are not specified as a crime by Uzbek legislation; however, transferring goods through the customs border without following the established rules is considered criminal if committed in a large amount and after punishing the perpetrator under the Code of Administrative Violations mentioned earlier. The prescribed maximum punishment for this

---

<sup>16</sup> Resolution No. 66 of Feb. 9, 2017 on the Republic of Uzbekistan Cabinet of Ministers on Approving the Procedure for State Registration of Subjects to Entrepreneurship, <https://perma.cc/A8Q6-GY7R> (in Russian).

<sup>17</sup> Code of Administrative Violations arts. 165, 176.

<sup>18</sup> Id. art. 176(2).

<sup>19</sup> Criminal Code of the Republic of Uzbekistan art. 188.

<sup>20</sup> Id. art. 188(1).

<sup>21</sup> Id. art. 190.

<sup>22</sup> Id. Section 8.

<sup>23</sup> Decree of the Republic of Uzbekistan President No. 138 of May 20, 2022 on Increase of the Amount of Salaries, <https://perma.cc/DR4U-L3QN> (in Russian).

offense is imprisonment for up to 8 years. The length of the imprisonment depends on the category of transferred goods and other qualifying characteristics.<sup>24</sup>

### III. Examples of Convictions for Violations of Export Controls or Economic Espionage

Reportedly, during the period of 1997-2014, the number of registered trade secrecy violations in Uzbekistan increased 13 times, however, the existing statistic does not reflect real numbers of how widespread are economic espionage activities. A survey conducted among Uzbek entrepreneurs showed that only 54% of businessmen are ready to contact law enforcement authorities if economic espionage is suspected. The remaining 46% of respondents said that they would resolve the issue by themselves or use private security firms. They explained their position by the fear that if a secrecy breach would become known through court proceedings, this may undermine their business reputation even further.<sup>25</sup>

Espionage-related cases are investigated by the Uzbekistan State Security Service. The jurisdiction of the Service includes protection of national security in the spheres of economy, science, social life, and information. It is responsible for monitoring the secrecy regime in state organizations and institutions.<sup>26</sup> Information on these cases is usually classified, and media reports based on information provided by the State Security Service are the only sources of information.<sup>27</sup> Foreign media often report on using espionage related charges by the authorities in prosecuting members of political opposition.<sup>28</sup> Investigation of corruption in Uzbek businesses was reported by the Organized Crime and Corruption Reporting Project.<sup>29</sup>

---

<sup>24</sup> Criminal Code of the Republic of Uzbekistan art. 182.

<sup>25</sup> Nargiza Raimova, *supra* note 11.

<sup>26</sup> Law of the Republic of Uzbekistan No. 471 of Apr. 5, 2018, on State Security Service in the Republic of Uzbekistan, arts. 5, 24, <https://perma.cc/6F5K-3Z74> (in Russian).

<sup>27</sup> See, e.g., *Former Defense Ministry Official and His Wife Charged with Treason*, Kun.Uz (Jul. 17, 2020), <https://perma.cc/UC3D-G36J>.

<sup>28</sup> See, e.g., *Uzbekistan: Former Defense Ministry Journalist Sentenced to 12 Years In Prison*, Eurasianet (Mar 4, 2020), <https://perma.cc/7DL8-54GK>; RFE/RL's Uzbek Service, *Former Uzbek Military Think-Tank Chief Gets 12 Years in Prison for Treason*, RadioFreeEurope/RadioLiberty (May 27, 2020), <https://perma.cc/955N-JMFC>.

<sup>29</sup> *A Top Uzbek Official, a Leading Businessman – and the Unknown Woman Who Ties Them Together*, The Organized Crime and Corruption Reporting Project (2021), <https://perma.cc/474E-NT5F>.