Volume 3, Issue 8, August - 2025 **ISSN (E):** 2938-3811

LIABILITY FOR INFRINGEMENT OF KNOW-HOW RIGHTS

Nadirbekova Umida Karamatdin qizi
Master at the University of World Economy and Diplomacy

Raimova Nargiza Doroyevna
Doctor of Sciences in Law, Professor of the Civil Law and International
Private Law Department of the University of World Economy and Diplomacy

Abstract
This article examines the issues of liability for the infringement of know-how rights from both legal-theoretical and practical perspectives. Know-how, as a form of trade secret, is considered an important object of intellectual property that protects the economic interests of enterprises and business entities. Violations of these rights, including unlawful disclosure, unauthorized use, or transfer to third parties, negatively affect not only the rights and interests of the owner but also the overall environment of fair competition. The article analyzes international legal norms, in particular the TRIPS Agreement, as well as the mechanisms of know-how protection in the United States, the European Union, China, and Japan.

Keywords: Know-how, trade secret, infringement of rights, legal protection, liability, international practice, cyberattack, international arbitration, confidentiality regime.

Introduction

In the conditions of the modern economy, know-how as an object of intellectual property is becoming increasingly strategic. Its peculiarity lies in the fact that know-how is often neither registered, patented, nor formally protected by copyright. However, this very feature makes it particularly vulnerable and open to violations. Therefore, the issue of infringement of know-how rights is by its nature complex, multifaceted, and manifests itself in practice in various forms. Such infringements usually occur through the unauthorized acquisition, disclosure, or use of confidential knowledge, expertise, or technologies contained in know-how.

To properly understand the concept of infringement of know-how rights, it is first necessary to determine under what conditions know-how may enjoy legal protection. Article 39 of the TRIPS Agreement defines know-how as "information that is secret, has commercial value, and is subject to reasonable steps for its protection [1]." These three criteria—secrecy, economic value, and protective measures—must be present for knowledge to be recognized as "know-how" and legally protected. If such information is disclosed, stolen, or used without authorization, then an infringement of know-how rights is deemed to have occurred.

Infringement of know-how rights can be divided into two main categories: internal and external violations. Internal violations are committed by persons within the enterprise or organization, such as employees, managers, or partners. For example, an employee who learns technological

Web of Scientists and Scholars: Journal of Multidisciplinary Research

secrets during employment may, after leaving the company, transfer this knowledge to a competitor or establish their own company based on it. Although confidentiality agreements with employees may partially limit such situations, proving them in court often becomes complicated. Especially when the know-how is not properly documented, employees may try to present it as part of their general professional knowledge.

External violations are typically committed by competitors, third parties, or individuals using technical means to commit unlawful acts. Examples include a competitor illegally acquiring a new product formula through industrial espionage, hacking IT systems to steal know-how information, or selling engineering designs to another company. In some cases, former employees may act as intermediaries in such violations. Particularly for digital know-how objects such as algorithms, software, and technological designs, cyberattacks aimed at extracting confidential data are becoming increasingly common.

Another significant form of violation is unauthorized disclosure, where a person shares know-how information with third parties or makes it public. Such "publication" destroys the confidential status of know-how, depriving the owner of exclusive usage rights. For instance, if someone publishes a production technology on social media or reveals it in a press interview, this also constitutes a violation. This situation has frequently been encountered in U.S. judicial practice: in *Henry Schein, Inc. v. Cook* (2015), a former employee was held liable for disclosing company plans and client databases through LinkedIn.

Unauthorized use of know-how is another common form of violation. In such cases, the information may not be disclosed but is used for commercial purposes. This too constitutes a violation, as it harms the legitimate interests of the owner, even if the information was not stolen. This is particularly critical in the pharmaceutical and IT industries: for example, if a company uses a confidential drug formula to develop a similar product and profit from it, it is considered a clear infringement.

It should be emphasized that infringement of know-how rights may sometimes occur unintentionally or unknowingly. For instance, if a company hires a new employee who applies know-how acquired at a previous workplace, this may form the basis for a lawsuit. In U.S. courts, such situations are often evaluated under the "inevitable disclosure doctrine," which sometimes imposes temporary restrictions on employees' activities[2]. While this approach remains controversial in international practice, it has not yet been incorporated into Uzbekistan's legislation.

In Uzbekistan, proving the infringement of know-how rights is often complicated. First, the existence of know-how and its ownership must be established in court. In many cases, such knowledge is not properly documented, included in internal regulations, or clearly distinguished in technical documents. Furthermore, evidence of protective measures must also be presented. For example, did the enterprise have employees sign confidentiality agreements? Were internal servers password-protected? Were confidential documents stored separately? Each of these factors constitutes essential evidence in protecting know-how in court.

In cases where production secrets, particularly know-how, are violated, the first legal recourse available to the injured party is civil liability. This is because, in the system of intellectual

property rights, especially regarding trade secrets, the protection mechanism is largely based on property rights. According to Article 985 of the Civil Code of the Republic of Uzbekistan, any damage caused to a person's property or to a legal entity, including lost profits, must be fully compensated by the person responsible for the unlawful act (or omission) [3]. Infringement of know-how rights is assessed precisely under this principle. In such cases, the injured party identifies the damage, its cause, and the responsible person, and files a claim in court.

The concept of damage in know-how disputes is interpreted broadly. It includes not only direct financial losses but also lost profits, reduced competitiveness, harm to reputation, and missed commercial opportunities. Especially in cases where competitors unlawfully acquire know-how and use it in their business, calculating the exact amount of damage becomes highly complex. Therefore, in both international practice and national court proceedings, the scale and type of damage are determined with the assistance of expert evaluations. For instance, if a competitor steals a secret of new product development and brings the product to market earlier than the injured party, the revenue gained during that period is considered as lost profits.

Compensation typically takes two forms: actual damage (factual losses) and lost profits (anticipated but unrealized income). Uzbek legislation and court practice require precise proof of actual damage. For instance, contracts, production costs, or sales turnover may be submitted as evidence. Proving lost profits is more complex and often relies on approximate calculations. Therefore, in some countries (the United States, Germany, Japan), courts may impose, in addition to proven damages, a fair compensation amount determined by the court.

In certain cases, liability is not limited to compensation but may include additional obligations imposed by the court. These may involve destroying or returning confidential information, suspending commercial activities, or removing information from advertising materials. Such protective measures are consistent with Articles 42–45 of the TRIPS Agreement, which emphasize restoring the rights and interests of the infringed party.[1]

Within civil liability, parties often attempt to resolve disputes through pre-trial mechanisms such as negotiations, mediation, or arbitration. This approach is common among business entities, as it saves both time and costs, while also preventing further disclosure of know-how secrets. The UNCITRAL Model Law on International Commercial Arbitration and the regulations of international arbitration institutions (such as ICC and LCIA) provide specific procedures for resolving know-how disputes through arbitration[4]. In Uzbekistan, the Law on International Commercial Arbitration allows for such mechanisms, though their practical application remains limited.

International practice demonstrates that effective civil liability in know-how disputes requires three key factors: (1) clear and documented identification of know-how; (2) the establishment of a legal confidentiality regime (e.g., contractual obligations, confidentiality agreements, password-protected systems, etc.); and (3) the ability to collect evidence of violations and initiate legal proceedings. Without these, information may be considered unprotected and denied recognition as know-how in court.

Web of Scientists and Scholars: Journal of Multidisciplinary Research

Illegal acquisition, use, or disclosure of production secrets, including know-how, may lead not only to civil liability but also to criminal liability. This is particularly the case where such actions cause substantial harm, are repeated, or are committed by organized groups, resulting in severe damage to the economic interests of others.

The main elements of criminal liability are illegality and intent. If a person inadvertently or accidentally gains access to another's trade secret, there may be no grounds for criminal liability. However, if the person deliberately acquires, uses, or transfers know-how information for personal gain or to harm another, this constitutes a crime. For instance, if an employee secretly copies production technology and later transfers it to a competitor, this qualifies as a criminal act. With modern technology, such actions have become easier through hacking, spyware emails, or copying files to portable devices.

In leading jurisdictions such as the United States, Germany, Japan, and China, criminal protection of know-how is highly regulated. For example, under the U.S. *Economic Espionage Act* (1996), theft of trade secrets is considered a federal crime punishable by up to 10 years of imprisonment. According to this law, any person who acquires, uses, or discloses a trade secret for personal benefit or for the benefit of foreign organizations or governments is subject to severe penalties. Particularly in the context of industrial espionage or foreign economic sabotage, such actions are regarded as "economic espionage[5]."

Moreover, criminal liability may apply not only to those who acquire or disclose such information but also to third parties who knowingly use it. For example, if a company accepts know-how information from a competitor without verifying its legality and uses it, the company may be deemed complicit in the crime. This is why large corporations carefully verify the origins, intellectual property status, and legality of any new technologies they adopt.

International reports published by the World Bank and WIPO highlight that criminal liability serves as one of the most important psychological and preventive measures in the protection of know-how rights. If employees or competitors are aware of potential criminal liability, they are far less likely to commit such violations. This enhances the investment climate, innovation capacity, and competitiveness of enterprises.

In international judicial practice, when reviewing cases involving production secrets, courts focus primarily on the commercial value of the information, compliance with confidentiality requirements, protective measures undertaken by the owner, and the methods used to acquire the information. In some countries, such as the United States, the EU, and Japan, specialized intellectual property courts handle such cases, where technological complexity is deeply analyzed. In China, since 2019, specialized intellectual property courts have been established specifically for know-how disputes, utilizing expert analysis, technically trained judges, and digital tools to clarify cases.[6]

In Uzbekistan, such disputes remain relatively rare in judicial practice. However, with the expected growth of competition and the number of technology-based companies, the application of laws in this area will expand. Learning from foreign experience, incorporating electronic evidence, and defining clearer criteria for identifying know-how in judicial practice will be essential. At the same time, international practice shows that the most crucial factor in

protecting production secrets is the preventive measures taken by the owner in advance: encryption, contractual obligations, restricted access, and regular audits. Only when such measures are sufficiently documented will courts recognize information as know-how and impose liability on violators[7].

Thus, improving the system of know-how protection requires clarifying legal frameworks, aligning criminal and administrative sanctions with international standards, and strengthening preventive and digital protection measures. This will reduce violations of trade secrets and foster a culture of respect and protection for intellectual property in the country.

References:

1. Agreement on Trade-Related Aspects of Intellectual Property Rights (as amended on 23 January 2017), https://www.wipo.int/wipolex/en/text/500864
2. Pooley, J. Secrets: Managing Information Assets in the Age of Cyberespionage. Verus Press, 2015.
3. Civil Code of the Republic of Uzbekistan. Tashkent: Yuridik Adabiyotlar Publish, 2024, 616 pages.
4. UNCITRAL Model Law on International Commercial Arbitration (1985), with amendments as adopted in 2006, https://uncitral.un.org/sites/uncitral.un.org/files/mediadocuments/uncitral/en/19-09955_e_ebook.pdf
5. U.S. Economic Espionage Act (18 U.S. Code §1831–1839), 1996.
6. DIRECTIVE (EU) 2016/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2016, https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng
7. Intellectual Property: Textbook / Responsible editors: Doctor of Law, Professor O. Oqyulov; Doctor of Philosophy in Law (PhD), Associate Professor N.E. Gafurova // Team of authors. – Tashkent: TSUL Publishing House, 2019. – 588 p.