Aslanov Ramil Mahir

Doctor of Laws,
Faculty of Law
Baku State University
(Baku, Azerbaijan)
aslanovram@list.ru

DOI: 10.33498/louu-2021-09-155

УДК 342.92

ISSUES CONCERNING PROTECTION OF CONFIDENTIAL INFORMATION IN THE ACTIVITIES OF STATE BODIES: LEGAL AND PRACTICAL ANALYSIS

Abstract. The word "confidentiality" is derived from the Latin word "confidentio", which means to trust. This means that the circle of persons possessing confidential information is specifically known, and that information is entrusted to these persons. Therefore, the rules for access to confidential information by third parties are established by law. Thus, to protect the confidentiality of any secret information, the law sets out specific rules that cover the legal regime of confidential information:

Criteria for classifying information as confidential information and indications of a specific type of secret. These criteria are mainly related to the content of the information, but their disclosure harms other people in any way. For instance, if the content of a state secret is directly determined by law, the commercial value of the information in a trade secret is a criterion for the essential content.

There are special legal rules for the protection of confidential information, as well as securing access to it. For instance, if a state secret is regulated by the establishment of this confidentiality regime, in case of duty related secret it is ensured by the obligation carried by the different professions representatives not to disclose the secret.

Disclosure of this information gives rise to liability. This can be a criminal, administrative or civil liability.

As mentioned in the article, in order to determine the responsibility for "data leakage" in the international exchange of information, problems should be resolved through mutual cooperation or regional control mechanisms.

Keywords: confidentiality; restricted access to information; open information; legal regime; official secret; state secret.

The interaction of information and society brings to structural changes in the regulation of society as a whole, and the information society is the greatest example of such alterations. In the information society, the proclamation of access to information and the development of security mechanisms often conflict with the confidentiality of information that is secured, namely

restricted. There are many practical problems regarding such confidential information, which are protected under different names and legal regimes, the source of which is both the dynamics of information relations and the inability of the legislature to keep up with this dynamics. The article analyzes legal and practical problems in this regard, and outlines suggestions and recommendations.

The article's objective is to analyze of the legal regime of confidential information, identify the main elements of this regime.

As a result of the generalization of the literature and legislation, the following features of the secret, which in in its turn, is considered as a legal category, can be distinguished:

– a secret is information that is known to a limited number of persons and is kept protected from other persons;

– the secret is unrevealed and confidential information, namely its disclosure to third parties is prohibited by law and therefore appropriate liability is established;

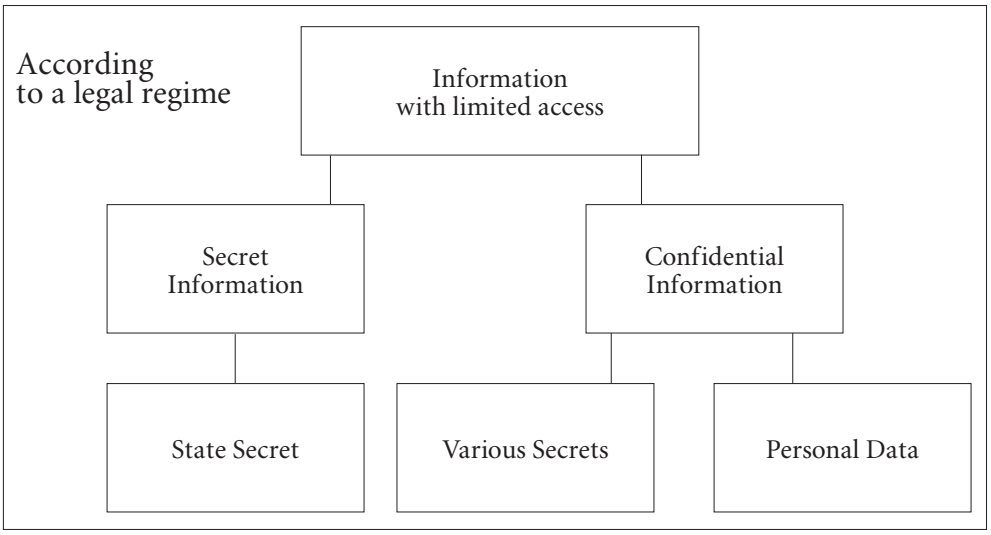
– there is both factual and legal basis for the confidentiality of information constituting the content of the secret. The legal basis is that only information, the access to which is restricted by law, can constitute the content of a secret. The factual basis is the special importance of confidential information and the fact that their disclosure is perilous for the individual, society and the state;

– the secret bears legitimate character, i. e., the protection of the confidentiality of the information that constitutes its content is determined by law. In this regard, the circle of persons responsible for the storage of this information is empowered by law, and legal liability is established for the disclosure of this information[1].

Thus, the legislature regulates the types of information that can be restricted under the term of secrecy. Therefore, it can be considered that the restricted information is an information based-legal institution and covers the following legal norms: the concept and types of restricted information; conditions and rules for determining limited access to information, as well as access to such information; legal status of information subjects with limited access; legal liability for disclosure of information constituting a secret, etc. It should also be noted that the establishment of a special legal regime for restricted types of information should not be considered a violation of citizens' freedom of information. Both international legal documents establishing human rights and freedoms, as well as the Constitution of the Republic of Azerbaijan, provide for the restriction of rights and freedoms in the manner and under the conditions established by law.

[1] A Aliyev, G Rzayeva, A Ibrahimova, B Maharramov, S Mammadrzali, *Information law. Textbook* (Nurlar 2019) 187.

In accordance with Article 34 of the Law of the Republic of Azerbaijan "On Freedom of Information", information is divided, on the one hand, into information that is open and, on the other hand, information access to which is restricted by law. As the unrestricted information is not a subject of the current research, it will not be further extended on this topic. According to the legal regime, the second group of information is divided into two types:



Therefore, the main purpose of defining the legal regime of confidential information is the protection of fundamental human rights and freedoms.

Official secret as a type of confidential information. The information intended for use during fulfilling of service is contained within the legal regime of secrecy. However, in addition, various laws and codes contain norms regarding information constituting a duty of confidentiality. For instance, confidentiality of tax informaiton, secrecy for customs, etc. Given that the legislature sets limits on the disclosure of such information and does not specify a time limit for such restrictions, it can be concluded that the term "official secret" has a broader meaning. On the other hand, it is clear from the analysis of many norms that provide for administrative and criminal liability that the object of these acts is information that is included in the official secret. For example, dissemination of information on security measures applied to judicial and law enforcement officers (Article 301 of the Criminal Code of the Republic of Azerbaijan), dissemination of information on measures taken against money laundering or terrorist financing (Article 316^2 of the Criminal Code of the Republic of Azerbaijan), illegal use of insider information by an insider (Article 420 of the Code of Administrative Offenses of the Republic of Azerbaijan), etc. In this regard, it is considered expedient to clarify the term "official secret" in the legislation.

The purpose of the confidentiality of the pre-trial investigation is, above all, to protect fundamental rights and to ensure a fair trial. In fact, this principle has a dual purpose: on the one hand, to ensure the proper conduct of the investigation and inquiry, thereby preventing violations of public order and fulfilling the constitutional obligations related to the detection of crimes and offenders, and, on the other hand, to protect persons under investigation in order to guarantee the right to confidentiality and the presumption of innocence.

For this reason, the secrecy of the pre-trial investigation is part of a logic that protects everyone's interests: the protection of evidence and witnesses, as well as the methods of investigation, if found, may prevent investigators from reaching certain conclusions. At the same time, we are talking about the isolation of witnesses, investigators and judges. In a society where public opinion is increasingly significant, the disclosure of classified information can be dangerous for the necessary impartiality of those involved in the investigation and trial. It should be noted that the main purpose of the investigation is to bring the truth to the surface. However, this avalanche of information and opinion should not harm the necessary impartiality of witnesses, investigators and judges.

Ensuring the confidentiality of the preliminary investigation means respecting the presumption of innocence to ensure that the suspects are not victims of an open trial. The presumption of innocence means that any suspect is presumed innocent until proven guilty. Violation of the judicial investigation and secrecy of the investigation is tantamount to depriving the accused of one of the most frequently violated fundamental rights. However, it is also a violation of the victims' right to secrecy. In case a crime is discovered, some injured people are at greater risk of physical or psychological harm.

The public sphere demandsincreasingly transparency. Public opinion expects full transparency from the media, due to a right to information that it considers essential. Timely submission of information may have detrimental consequences for the investigation and possible police action. An example of this is the tragic example of Hyper Cacher being taken hostage in January 2015 when a 24-hour news channel reporter discovered that people were hiding in a cold room and that this could have dramatic consequences.

The issue is that the media often obstructs criminal investigations and leaks information with unnecessary interference. Journalists who violate confidentiality are not directly liable, but can be prosecuted for obtaining information upon a breach of confidentiality, if the disclosed information can only come from a person related to that confidentiality. However, since the right of journalists not to disclose their sources is guaranteed by the European Court of Human Rights (ECHR), the chances of success in tracking the source of such information are poor.

Under the French law, the confidentiality of sources is guaranteed by the Freedom of the Press Act of 29 July 1881: only a prerogative of the public interest can give grounds for measures that infringe on the confidentiality of sources, provided they are necessary and proportionate. Thus, the goal was pursued. However, the Cour de Cassation (French Supreme Court) has issued a restrictive comment stating that 'although the investigation has been seriously violated', it cannot compromise the confidentiality of sources in order to find the perpetrators. Hereby, on the confidentiality of pre-trial investigations and inquiries the following is stated: 'without demonstrating that these interventions are based on a superior order of public interest'[2]. Although the ECtHR acknowledges that there is a legitimate interest in informing the public and that there is a greater interest than respect for the confidentiality of pre-trial investigations and inquiries, this protection is not absolute: the required condition is a good intention.

One of the most important issues is the protection of security in the exchange of information related to official secrecy. Thus, it should be taken into account that those who work with personal data can also interfere with the information unfairly. Data processors should have as little information as possible and the activities of these people should be managed by appropriate means.

In this regard, special care is required when conducting criminal registration in databases. It would be more relevant to apply more to international bases. Various Interpol databases are of special significance here. First, one can mentiong the DNA database. Countries use Interpol's DNA database to share and compare DNA profile data from crime scenes and celebrities, as well as missing and unidentified human remains. This international DNA database can be accessed directly by national authorities such as the National Central Bureau of Interpol (NCB) and forensic laboratories. As a new service, Interpol will soon offer the use of family DNA comparisons to identify missing persons.

Interpol's fingerprint database contains more than 182,000 fingerprint records (as of December 2017). Authorized users in member countries can view, send and re-verify fingerprint records protected by the global operational authorities' communication network Interpol 24/7 using a convenient automatic fingerprint identification system (ADIS). Law enforcement officers can either remove fingerprints via an electronic device, or using hand ink and paper, and then use a special scanner to store electronic information in an appropriate format. The information is then submitted to the General Secretariat of Interpol for uploading to the database. Records shall be kept and exchanged in a format prescribed by the National Institute of Standards and Technology (NIST).

The Interpol Fingerprint Block provides a service called the Automatic Fingerprint Identification System (AFIS) Gate, which allows member

[2] Criminal Chamber of the Cour de Cassation, February 25, 2014, p. 13–84.

countries to send remote fingerprint searches to the Interpol database and receive an automatic response. Automated tracking, as well as a large-scale search system, has been introduced, allowing more than 1,000 comparisons a day with Interpol's fingerprint database, which operates 24 hours a day, seven days a week.

As for Eurojust, this network takes data protection very seriously and respects the fundamental rights of all people. The Agency, which is at the forefront of investigations and trials, maintains regular contact with operational information. At a more general level, Eurojust processes different categories of personal data as part of its day-to-day administrative activities. By applying the highest standards of data protection, the Agency ensures that all information is processed with the utmost care and that the rights of individuals are always fully protected[3].

Europol can play an important role in expanding the exchange of information by helping to identify and expose criminal networks/groups. According to the European Commission, Governance co-operation is not only about co-operation between the tax authorities, including the tax authorities of non-EU countries, but also about co-operation between the EU member states' customs authorities and law enforcement agencies, which is essential for proper implementation. On 9 and 7 April 2016, the EU Commission formally adopted a VAT Action Plan to detect and reduce VAT regulations and VAT fraud in cross-border transactions. Paragraph 5 of Article 10 of the "20 Measures to Eliminate the VAT Gap" emphasizes the need to consolidate the fight against STIs.

> Do support deeper cooperation between different agencies. Fighting organized crime networks involved in fraud requires joint efforts within member states and between tax authorities and law enforcement agencies. Missing trader fraud requires a smooth exchange of information between the tax and customs authorities[4].

In almost all countries, the tax administration has the opportunity to share information with the authorities responsible for investigating tax crimes and customs. However, there are restrictions for prosecutors on the exchange of information with the police in tax offices and on non-tax investigations. At the very least, the suspect does not have to report any non-tax violations. The customs office can share information with the tax office. There are many different approaches. Some countries have direct access, while others have

[3] 'Data protection at Eurojust' *(European Union Agency for Criminal Justice Cooperation)* <https://www.eurojust.europa.eu/about-us/data-protection/data-protection-eurojust> (accessed: 16.09.2021).

[4] Communication from the Commission to the European Parliament and the Council on an Action Plan to strengthen the fight against tax fraud and tax evasion (COM (2012) 722 final of 6/12/2012) <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52012DC0722> (accessed: 16.09.2021).

restrictions that prohibit the exchange of information through tax or customs. However, there are rules by which information can be shared in the event of tax or customs violations. This confirms the exchange of information between the investigative departments of the customs authorities and other law enforcement agencies. Such exchanges are used without protection through surveys to protect confidential information.

Thus, measures to protect confidential information in the investigation of customs crimes should be implemented not only in relation to the subjects, but also in the exchange of information with relevant law enforcement agencies.

Conclusion. The article classifies the issues connected with confidentiality of information with limited access into several groups.

The problems in the first group stem from conflicts in the legal regime of various secrets, and in some cases from overlapping norms. Thus, the boundaries of various secrets contained in confidential information often collide. In one case, information relating to personal information is considered confidential during the investigation. In this case, the question of which legal regime to apply is questionable. Even many information law norms have problems and inaccuracies related to various closed information circles. For instance, a lot of information included in a bank secret includes information that is also a tax secret. In our opinion, such problems take the roots from the shortcomings of the new information society in the legal framework. It also remains dubious how information security will be protected during the exchange of information, both within the country and in contact with foreign countries, during the period of widespread use of electronic systems. The point is that the legislature has not given any legal definition of information security.

The drawbacks in the second group are related to the issue of responsibility and subjects. Determining the content of confidential information imposes a responsibility not only on the participants in the process, but also on government agencies for the non-dissemination of such information. However, in this case, there are descriptive problems related to which specific article of the criminal law is applied.

The third group of problems arise from the fact that the information is in line with the principles of openness and transparency, in case it raises the issue of ensuring human rights and freedoms as beiing an investigative secret. The point is that a transparent society and the principle of openness demands securing access to information. At the same time, freedom of expression requires it. However, in most cases, this can lead to human rights violations. For instance, the issue of reconciling securing various rights in case when negative events broadcast on various news portals. However, in general, one cannot agree with the authors who claim that such investigative information is not disseminated, as it is essential in terms of transparency of government agencies.

REFERENCES

Bibliography

Authored books

1. Aliyev A, Rzayeva G, Ibrahimova A, Maharramov B, Mammadrzali S, *Information law. Textbook* (Nurlar 2019) (in English).

Websites

2. 'Data protection at Eurojust' *(European Union Agency for Criminal Justice Cooperation)* <https://www.eurojust.europa.eu/about-us/data-protection/data-protection-eurojust> (accessed: 16.09.2021) (in English).

Раміль Махір Асланов

ПИТАННЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ У ДІЯЛЬНОСТІ ДЕРЖАВНИХ ОРГАНІВ: ПРАКТИЧНО-ПРАВОВИЙ АНАЛІЗ

Анотація. Слово "конфіденційність" походить від латинського *"confidentio"* – "довіряти". Це означає, що коло осіб, які володіють конфіденційною інформацією, конкретно відоме, і що інформація довірена цим особам. Отже, правила доступу третіх осіб до конфіденційної інформації встановлені законом. Таким чином, для захисту конфіденційності будь-якої таємної інформації закон встановлює спеціальні норми, які охоплюють правовий режим конфіденційної інформації, зокрема:

Критерії віднесення інформації до конфіденційної та вказівки на певний вид таємниці. Ці критерії переважно стосуються змісту інформації, але їх розголошення будь-яким чином шкодить іншим людям. Наприклад, якщо зміст державної таємниці прямо визначено законом, критерієм істотного змісту є комерційна цінність відомостей, що містяться у комерційній таємниці.

Існують спеціальні законодавчі норми щодо захисту конфіденційної інформації, а також забезпечення доступу до неї. Наприклад, якщо державна таємниця регулюється встановленням цього режиму таємності, то у разі службової таємниці це забезпечується зобов'язанням представників різних професій не розголошувати таємницю.

Розголошення цієї інформації тягне за собою відповідальність. Це може бути кримінальна, адміністративна чи цивільно-правова відповідальність.

Як зазначається у статті, для визначення відповідальності за "витік даних" у міжнародному обміні інформацією проблеми слід вирішувати за допомогою взаємної співпраці або регіональних механізмів контролю.

Ключові слова: конфіденційність; інформація з обмеженим доступом; відкрита інформація; правовий режим; службова таємниця; державна таємниця.