CONTEMPORARY APPROACHES TO INFORMATION CLASSIFICATION IN UKRAINE

Solodka Olena

DOI: https://doi.org/10.61345/1339-7915.2025.1.18

Annotation. The article deals with the contemporary approaches of information classification in information society, including the factors that determine the necessity of this process, its characteristics and main directions of implementation.

The aim of the work is to study and analyze modern approaches of information classification in Ukraine.

It is said that with the development of modern information and communication technologies and their applications in all areas of life, with an increasing quantity and quality of information, the recognition of the right to information as one of the fundamental human rights in the information society its necessary to provide the contemporary approaches to information classification that must take into account the gaps and conflicts of legal regulation of secret information not only across a state, but also at the international level, factors of informatization of modern society and the fundamental principles of freedom of access to information. But it is complicated by russian aggression and the regime of martial law in Ukraine.

Therefore, the analysis indicates that the modern legal secrecy regime should be characterized by the following features: clear grounds for classifying information defined by the law; the right to restrict access to information is only for authorized person (the owner and the person who has the right to own, use and dispose); the degree of restriction of access and the level of protection of classified information is always marked with its importance for the individual, society, state and is proportinal with the losses that may be incurred in case of its disclosure; information protection should provide benefits to the owner and usually justify the money spent on its defense; circulation of sensitive information is carried out in the defined regime space; unauthorized dissemination of sensitive information is a prerequisite for its vulnerability; aging of secret information provides a mandatory revision of access limit levels to such information; the status of “secrets” imposes a duty, not a right for its protection and limitation in distribution.

Key words: information, right to information, information classification, access to information, legal regime of secrets, information protection.

1. Introduction.

Today the fundamental dependence of human life, society and state on information exchange, secure information and telecommunication systems, technologies and tools operation has actually formed. Information and knowledge have become a strategic resource, compatible with the use of traditional resources and access to them has become a major factor in social and economic development. People also cannot imagine its existence without modern information technologies, which are progressing every day, using them in various spheres of social relations. The above stipulates the development of information society, the emergence of which is usually associated with the following factors: the transformation of information into the subject of mass consumption, the use of information as an economic resource and the introduction of information technologies to all areas of production and management of public life.

2. Analysis of scientific publications.

Some aspects of the investigated problem (the development of the system of information classification; types of classified information; specifics of the information classification in Ukraine, etc.) were carried out by modern scientists: Arkhipov O.E., Kaspersky I.P. [1], Rozvadovsky O.B. [2], Semenyuk O.G. [3], Kots D. V. [4] and others. However, the development of the information society requires the study of modern approaches to solving these problems.

3. The aim of the work is to study and analyze modern approaches of information classification in Ukraine.

4. Review and discussion.

In the information society the right of access to information is recognized as one of the fundamental human and civil rights that is reflected in relevant documents of international community (in particular in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights and Fundamental Freedoms protection).

Thus, Article 10 of the European Convention [5] defines that everyone has the right to freedom of expression, that is reflected in domestic legislation [6, 7, 8]. This right includes freedom to hold opinion, to exchange data and ideas without interference of public authority and regardless of borders. The question of extraterritoriality is extremely important in the development of modern information communication, including Internet, which absolute advantages are: possibility to exchange interactively large amounts of information at high speed; the efficiency of providing information to potential users; technical and financial accessibility; general democracy of Internet resources.

However, it should be noted that the development of the information society may have both positive and negative effects, and to avoid them, the government should regulate the process of its formation: on the one hand, by creating conditions of free access to information for their citizens, on the other hand – by protecting sensitive data that means establishing proper balance between the need for the free exchange of information and the acceptable limits of its distribution.

The legal regime of secrecy is one of the most important institutions of law, which makes it possible to determine the extent of information security that correlate with the interests of individuals, society and the state; as well as the limits for permitted intrusion into the sphere of private interest without breaking the law. The efficiency of measures, implemented by the state in the shere of secrets, directly depends on the normal functioning of the state legal institutions, including the legal regulation of information relations.

At the same time, the status of secrecy limits the fundamental human right to information in the information society that raises a question about the necessity of transforming legal secrecy regimes according to current challenges.

In modern society, it is extremely important to protect personal data, which is a part of the legal privacy regime, because people's life and health, honor and dignity, inviolability and security are recognized as the highest social values.

Active use of Internet technologies that make authorities and citizens communication significantly more effective (forums, newsgroups, e-mail, electronic archives, the introduction of search engines etc.) and provide administrative services through the system of e-governing, which according to the research, generates three categories of problems in the field of personal data protection. They are: the problem of gathering information, the issue of personal data use and disclosure and some security problems. In the absence of boundaries in the information space the problem can not be

solved effectively only at the national level and thus, the international community must work out adequate measures.

For example, in Ukraine, after bringing the legislation on personal data protection in line with European standards, all information about a person became as sensitive information, making it difficult to provide legal protection and imposes additional liabilities on the authorized persons. To solve this problem, it is necessary to distinguish between general data and sensitive information as European regulations prohibit the collection of the latter type.

At present, there are some questions about systematization of legal relations associated with the transition of personal data in the possession of other subjects, for example, when a person submits personal information to the hospital, state institution, notary services etc. In this case a necessity of mandatory fixing of personal data transformation status appears.

In addition, the extreme popularity of the social networks as a means of communication between people from different parts of the country and the world actualizes the issue of illegal collection of personal data.

Practice shows that the process of obtaining personal data today becomes a separate field of activities aimed at gathering, processing and dissemination of personal data on a commercial basis. For example, experts estimate the world market currently reaches more than 3 billion dollars. Information about the person, his/her financial status, habits etc. are actually accessible to anyone.

Today the question of securing the right to provide consumers with the ability to control how their personal data is processed by companies is of great importance, because the collectors of personal information, such as advertising agencies, not always request permission from the clients to collect their personal data.

In this perspective, the question of legalization of the possibility to remove information on request of its owner, representing the so-called "right to be forgotten" is actual.

The sense of the "right to be forgotten" includes the right to remove personal data if its owner desires, privacy by default, the possibility of withdrawing or modifying personal data of the person deceased.

In particular, the default privacy rule provides that users of social networking sites need to consent to the publication of their personal data. A practice that their personal information is public by default (i.e., if you select "private mode" in the settings) should be declared illegal. Privacy by default also prohibits the transfer of users' personal data to different applications available in social networks.

Legal implementation of the "right to be forgotten" is complicated by rapid pace of conversion of such information from its owner to other users, by development of artificial intelligence technologies etc. Today the issue of the possibility of withdrawing or amending personal data of the person deceased remains controversial (for example, how to determine the fact of death).

Closely related to the issue of personal data is the legal regime of bank secrecy, which is changing in recent years due to the worldwide trend towards "transparency" of financial and banking information, stipulated by the need to fight against legalization of proceeds from crime, terrorist financing, corruption. At present a bank secrecy should be a set of interrelated legal mechanisms, that, on the one hand, allow preventing the disclosure and misuse of bank secret, and on the other hand – provide ample opportunities to the law enforcement agencies to detect and prevent criminal acts linked with money laundering.

In an increasingly urgent international cooperation, integration and globalization trends state secret protection at the international level is an acute issue. Overall interstate exchange of classified information is governed by international agreements of mutual protection of classified information. All these agreements contain a provision stating that the parties in accordance with their national law shall take all necessary measures to protect secret information transmitted or created, and provide the same protection that is expected when dealing with their own secret information with the relevant degree of secrecy, namely provide: procedure for mutual protection of classified information (in accordance with domestic law, acts of international organizations, agreed rules);

obligations of the parties to ensure the protection of received classified information, including preventing access to third parties and the use of classified information for purposes inconsistent with the purposes of transfer of such information; the procedure for granting access to classified information of representatives of the parties; commitment to classifying, changes in the degree of confidentiality, declassification of classified information (material carriers of information); order of transfer of classified information; commitment to mutual informing of violation of the requirements concerning the protection of classified information and measures to bring guilty persons to responsability; time limits to undertake to ensure mutual protection of classified information; requirements for executive agreements, concluded between the parties, authorizing transmission of secret information (material carriers of information); the settlement of disputes; identifying of the parties entrusted with the implementation of cooperation under the contract.

At first glance, the analysis of these provisions defines proper order of state secrets protecting while transferring to another state, however, we agree with the scientists who consider it necessary to normalize the state secret mandatory status in the law of the State to which it is transferred. Particularly acute is the issue that arises in the case of any reasons for bringing a party to legal liability. To resolve this issue some European countries apply two alternative approaches in their legislation: either a reference to the secret of the union state (group of states) is included in the definition of state secret and thus, their status equalizes (Latvia, Germany) or a note about a particular country is made in the Criminal Code (France).

According to experts, the first approach is more constructive, so it is better not to make the reference for the separate state (their number may vary), but use general definition.

Another important aspect of the treatment of state secrets is the question of aging of such information, which requiries elaboration of permanent secret review mechanism and transfer of classified information from one type to another, as neglecting of this aspect will lead to unnecessary information classification, the accumulation of big amount of secret information and unnecessary spendings for its protection that violates the basic criteria for restricting access to information.

In this context it should be added, that unification of the types of classified information is the important issue, as differences in the secrecy of information create problems with the timing and order of protection of such information in case of transfer to another state.

The analysis set out above indicates, that there have already appeared objective conditions that stipulated the necessity of secrets legal regime transformation. There are: the processes of integration and globalization; extraterritorial information sphere under different legal rules, that define legal secrets regimes; rapid development of information technologies and their use in everyday life; mass consumption of information and its exchanges; the use of information in illegal purposes; unauthorized collection of personal data; aging of information.

Therefore, the objective conditions of legal regime transformation of secrets in the information society require the following issues: unification of types of sensitive information and requirements to its protection at the international level; legal regulation on the personal data protection in information networks, providing practical realization of the principle of extraterritoriality of law in this area, establishing the control over personal data; determination of classified information transition procedures from one type to another; reduction of classified information; legalisation of the status of state secrets in the legislation of the country to which it is transmitted under agreements of mutual protection.

At the same time, we believe that the elaborated principles providing public access to information must promote the process of legal regime transformation of secrets in the information society, including [2]:

Principle 1. Maximum disclosure. The principle of maximum disclosure establishes a presumption that all information held by public bodies should be subject to disclosure and that this presumption may be overcome only in very limited circumstances. Public bodies have an obligation to disclose information and every member of the public has a corresponding right to receive information.

Principle 2. Obligation to publish. Freedom of information implies not only that public bodies accede to requests for information but also that they publish and disseminate widely documents of significant public interest, subject only to reasonable limits based on resources and capacity.

Principle 3. Promotion of open government. Informing the public of their rights and promoting a culture of openness within government are essential if the goals of freedom of information legislation are to be realised.

Principle 4. Limited scope of exceptions. All individual requests for information from public bodies should be met unless the public body can show that the information falls within the scope of the limited regime of exceptions. A refusal to disclose information is not justified unless the public authority can show that the information meets a strict three-part test (look below).

Principle 5. Processes to facilitate access. A process for deciding upon requests for information should be specified at three different levels: within the public body; appeals to an independent administrative body; and appeals to the courts. All public bodies should be required to establish open, accessible internal systems for ensuring the public's right to receive information.

Principle 6. Costs. The cost of gaining access to information held by public bodies should not be so high as to deter potential applicants, given that the whole rationale behind freedom of information laws is to promote open access to information. It is well established that the long-term benefits of openness far exceed the costs.

Principle 7. Open meetings. Freedom of information inclu des the public's right to know what the government is doing on its behalf and to participate in decision-making processes. Freedom of information legislation should therefore establish a presumption that all meetings of governing bodies are open to the public.

Principle 8. Disclosure takes precedence. The law on freedom of information should require that other legislation be interpreted, as far as possible, in a manner consistent with its provisions. Where this is not possible, other legislation dealing with publicly-held information should be subject to the principles underlying the freedom of information legislation.

Principle 9. Protection for whistleblowers. Individuals should be protected from any legal, administrative or employment-related sanctions for releasing information on wrongdoing. "Wrongdoing" in this context includes the commission of a criminal offence, failure to comply with a legal obligation, a miscarriage of justice, corruption or dishonesty, or serious maladministration regarding a public body. It also includes a serious threat to health, safety or the environment, whether linked to individual wrongdoing or not.

In addition, in order to create legally limited information access, you have to meet three requirements of three-part test, proposed by international non-governmental organization Article 19, namely [9]: it must relate to a legitimate aim listed in the law, such ads must threaten to cause substantial harm to the specified legitimate aim; damage that may be caused to the aim must be greater than the public interest in receiving information.

The legitimate goal is to be justified by an exhaustive list of legal grounds for restricting access to information. These reasons are usually due to the interests of national security, territorial integrity or public safety, the need for the prevention of disorder or crime, the protection of public health, reputation or rights of others, preventing the disclosure of information received in confidence, maintaining the authority and impartiality of the judiciary.

Although, for example in accordance with Article 32 of the Constitution of Ukraine [6], no one shall be subjected to interference with his privacy, family, except as provided by the Constitution of Ukraine: collection, storage, use and dissemination of confidential information about a person without her consent are not allowed, except the cases determined by law, and only in the interests of national security, economic prosperity and human rights. Thus, on the one hand, the Constitution of Ukraine provides comprehensive reasons for the possible legitimate intervention in private and family life of the person, on the other hand – outside the legal field there are questions of detailed national security interests, as the actual legislative definition of the term.

When considering the damage, one should pay attention to the issues such as advantages of using data that must be classified as secret as well as the costs of such data protection compared with a loss that may be incurred in case of its disclosure.

Today the problem of economic study of possible harm from disclosure or leakage of sensitive information and its expression in money equivalent and thus classification of information remains topical. At the same time, it should be noted that not necessarily eve ry harm from disclosure of the information can be calculated in monetary terms. Moreover, it is hardly possible to define it appropriate from both moral and legal side, the calculation of economic damages and other legal consequences, which in particular is the threat to human life and the possibility of an armed conflict, in the same units [1].

The theme of social significance is updated whenever there are legitimate grounds for restricting access to certain information and there is a need for the right of the public to know about it. Recognition of publicly necessary information ought to be the indisputable legal fact, which would allow to ask questions about the distribution of such information without the consent of its owner. However, the need to determine this legal construction is necessary, as prooving in court the fact that certain classified information is socially necessary is the basis for the decision to provide this information upon request. With the establishment of the fact that certain classified information is of public interest, the person may be exempt from liability for the dissemination of such information.

The subject of public interest is information that indicates the threat to national sovereignty and territorial integrity; ensures the implementation of constitutional rights, freedoms and duties; demonstrates the possibility of human rights violations, leading the public astray, environmental and other negative consequences of actions (inefectiveness) of individuals or legal persons, etc. It means that in each case it must be determined what information is socially necessary, that is the subject of public interest.

The problem is that the term "subject of public interest" is an estimated category. Thus, when deciding whether information is socially necessary, it is recommended to take into account the fact that the public interest means the possibility of the practical benefits of public disclosure of certain information. So, the question of public information importance appears in the following cases:

– certain public information was improperly classified as restricted access information and there is a need to obtain it;

– although some information is confidential in nature at the same time, as this information is socially necessary (information about the private lives of senior officials) this information, if it is available to the public authorities, can be provided at the request, or be published by the media;

– when the person is prosecuted for distribution of classified information.

5. Conclusions.

Therefore, the analysis of the above provisions indicates that the modern legal secrecy regime should be characterized by the following features: clear grounds for classifying information defined by the law; the right to restrict access to information is only for authorized person (the owner and the person who has the right to own, use and dispose); the degree of restriction of access and the level of protection of classified information is always marked with its importance for the individual, society, state and is proportinal with the losses that may be incurred in case of its disclosure; information protection should provide benefits to the owner and usually justify the money spent on its defense; circulation of sensitive information is carried out in the defined regime space; unauthorized dissemination of sensitive information is a prerequisite for its vulnerability; aging of secret information provides a mandatory revision of access limit levels to such information; the status of "secrets" imposes a duty, not a right for its protection and limitation in distribution.

With the development of modern information and communication technologies and their applications in all areas of life, increase of quantity and quality of information, the recognition of the

right to information as one of the fundamental human rights in the information society stipulates the necessity to provide the secrets legal regime transformation that must take into account the gaps and conflicts of legal regulation of secret information not only across a state, but also at the international level, factors of informatization of modern society and the fundamental principles of freedom of access to information.

References:

1. Arkhypov O.Ie, Kasperskyi I.P. Metodychni aspekty formuvannia pereliku informatsii, shcho stanovyt komertsiinu taiemnytsiu okremoho pidpryiemstva. Pravova informatyka. 2011. № 1(29). S. 59–66. [in Ukrainian].
2. Rozvadovskyi O.B. Formuvannia derzhavnoi polityky shchodo zabezpechennia okhorony derzhavnoi taiemnytsi ta sluzhbovoi informatsii v suchasnykh umovakh. Informatsiina bezpeka liudyny, suspilstva, derzhavy. 2013. № 2 (12). S. 36–42. [in Ukrainian].
3. Semeniuk O.H. Teoretyko-pravovyi analiz poniattia derzhavnoi taiemnytsi. Informatsiia i pravo. 2016. 3(18). S. 35–44. [in Ukrainian].
4. Kots D. V. Teoretyko-pravovi zasady informatsii z obmezhenym dostupom. Visnyk NTUU «KPI». Politolohiia. Sotsiolohiia. Pravo. 2019. Vyp. 2 (42). S. 107–119. [in Ukrainian].
5. Article 10 of the European Convention URL: https://www.equalityhumanrights.com/ human-rights/human-rights-act/article-10-freedom-expression (date of access: 01.04.2024).
6. Konstytutsiia Ukrainy. URL: http://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (date of access: 19.09.2023).
7. Pro informatsiiu: Zakon Ukrainy vid 02.10.1992 r. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (date of access: 04.04.2024).
8. Pro dostup do publichnoi informatsii: Zakon Ukrainy vid 13.01.2011 r. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (date of access: 12.07.2023).
9. Principles of freedom of information legislation, ARTICLE 19, London, 1999.

Olena Solodka,
P.h.D. in law, senior researcher, National academy of Security Service of Ukraine
E-mail: sweet2701@ukr.net
ORCID: 0000-0002-1799-0712