UDC 340:659.4.327.88 (477)

Lysenko Serhii Oleksiyovych,
PhD in Law, Associate professor, Associate professor of the Department of Security Management and Law Enforcement and Anti-Corruption Activities, Interregional Academy of Personnel Management, 03039, Kyiv, Str. Frometovskaya, 2, tel.: (044) 490 95 00, e-mail: crimeconsult@ukr.net
ORCID: 0000–0002–7050–5536

Лисенко Сергій Олексійович,
кандидат юридичних наук, доцент, доцент кафедри управління безпекою, правоохоронної та антикорупційної діяльності, Міжрегіональна Академія управління персоналом, 03039, м. Київ, вул. Фрометівська, 2, тел.: (044) 490 95 00, e-mail: crimeconsult@ukr.net
ORCID: 0000–0002–7050–5536

Лысенко Сергей Алексеевич
кандидат юридических наук, доцент, доцент кафедры управления безопасностью, правоохранительной и антикоррупционной деятельности, Межрегиональная Академия управления персоналом, 03039, г. Киев, ул. Фрометовская, 2, тел.: (044) 490 95 00, e-mail: crimeconsult@ukr.net
ORCID: 0000–0002–7050–5536

METHODOLOGICAL APPROACHES TO UNDERSTANDING THE CATEGORY OF "ENTERPRISE INFORMATION SECURITY SYSTEM" FROM THE PERSPECTIVE OF LEGAL HERMENEUTICS

Abstract. The paper deals with issues related to studying and defining the basic methodological approaches to understanding the category of "enterprise information system security" from the perspective of legal hermeneutics. It also examines the basic views on definition of the concept of legal "hermeneutics" and gives a definition the author suggests for this concept.

Keywords: information law, information security, hermeneutics, law, and enterprise information security system.

МЕТОДОЛОГІЧНІ ПІДХОДИ ДО РОЗУМІННЯ КАТЕГОРІЇ “СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ” З ТОЧКИ ЗОРУ ГЕРМЕНЕВТИКИ У ПРАВІ

Анотація. У статті розглядаються питання щодо дослідження та визначення основних методологічних підходів щодо розуміння категорії “система інформаційної безпеки підприємства” з точки зору герменевтики у праві. Досліджуються основні погляди відносно визначення поняття “герменевтика” у праві та надається авторське визначення цього поняття.

Ключові слова: інформаційне право, інформаційна безпека, герменевтика, право, система інформаційної безпеки підприємств.

МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К ПОНИМАНИЮ КАТЕГОРИИ “СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ” С ТОЧКИ ЗРЕНИЯ ГЕРМЕНЕВТИКИ В ПРАВЕ

Аннотация. В статье рассматриваются вопросы исследования и определения основных методологических подходов к пониманию категории “система информационной безопасности предприятия” с точки зрения герменевтики в праве. Исследуются основные взгляды относительно определения понятия “герменевтика” в праве и предоставляется авторское определение данного понятия.

Ключевые слова: информационное право, информационная безопасность, герменевтика, право, система информационной безопасности предприятий.

Target setting. The process of providing enterprise information security is built in accordance with current legislation and corporate regulatory acts. Any similar process is associated with subjective perception and interpretation of legal rules regulating these relations by actors themselves. Primarily the Constitution of Ukraine, Art. 17, regulates relations arising in the area of providing enterprise information security. They are also subject to the Laws of Ukraine “On Information,” “On the National Informatization Program,” and, finally, to the orders and instructions concerning a given organization enshrined in the charter or founders meeting minutes. With such an array of regulatory norms, cases of different interpretations of the same rules are not uncommon. Issues of understanding the processes of providing enterprise information security are best considered from the perspective of hermeneutics in legal science.

Analysis of recent research and publications. The question of the basic methodological approaches to understanding the category of “enterprise information system security” from the perspective of legal hermeneutics in some sense are considered in the works of Gadamer H.-G., Kuznetsov V. G., Plavich V. P., Ricoeur P., Suslov V. V. and others.

The purpose of the article is to study the methodological approaches to understanding the category of "enterprise information system security" from the perspective of legal hermeneutics.

The statement of basic materials. Nowadays, hermeneutics represents a branch of modern philosophy. The subjects of contemporary hermeneutics include issues of social cognition and its methods. The central question of the methodology of hermeneutics is how people should understand the senses of what is and what should be, and what limits there exist on interpretative freedom. H.-G. Gadamer expressed its essence as follows: "Hermeneutics is practice... The fundamental truth of hermeneutics is as follows: no one alone can learn and tell the truth. The soul of hermeneutics is to by all means maintain a dialogue, let a dissident have his say too, and be able to assimilate what he uttered — that's the soul of hermeneutics" [7].

In our time, hermeneutics in law and philosophy is construed as a science dealing with understanding the sense of texts and has different stages of development. The term "hermeneutics" is also used in a theoretical sense: hermeneutics is a theory of understanding, comprehending a sense [8].

Based on the above, we can develop an appropriate definition. Legal hermeneutics is understanding and explaining the sense laid by the legislator into the text of a regulatory legal act. The task of legal hermeneutics is to provide methodologically transition from understanding the sense of a point of law to correctly explaining its essence.

Such kind of transition is the process of cognition, which results in finding the sole and correct version of interpretation of general precepts of law concerning a concrete legal situation.

The specifics of legal hermeneutics is associated with the existence of different legal cultures, including Ukrainian national legal culture, with their own vision of such problems as human rights, law-governed state, partition of power, local government etc., and our legal customs.

Whatever fields of law we consider they consist of a totality of various interpretive calculations. In this sense, law is inherently a purely hermeneutic phenomenon.

Italian philosopher and jurist E. Betti worked out the most interesting methodology of hermeneutic analysis of legal texts. He was saying that there is the world of objective spirit, facts and human events, acts, gestures, thoughts and projects, traces and evidences of ideas, ideals and realizations. This entire world belongs to interpretation. A comment appears as the process the aim and identical result of which is comprehension. A commentator must retrospectively reproduce the real process of creation of the text by dint of reconstruction of the message and objectivization of intention of the author of the text [9].

Betti formulated four hermeneutic canons actively used in jurisprudence:

1) Canon of immanence of hermeneutic scale. Reconstruction of the text must conform to the author's point of view. The commentator does not have to bring anything from the outside; he has to look for the sense of the text, respecting dissimilarity and hermeneutic autonomy of the object.

2) Canon of totality of hermeneutic consideration. Its essence is in the idea that unity of the whole is explained through separate parts, but the sense of separate parts becomes clear through the unity of the whole (hermeneutic circle).

3) Canon of relevance of awareness. The commentator cannot withdraw his subjectivity until the end. To reconstruct other people's thoughts and works of the past, to return to genuine vital reality other people's emotions, it is necessary to correlate them with own "moral horizon".

4) Canon of the semantic adequacy of understanding represents a requirements to the commentator of the text. It the author and commentator are congenial and are on the same level, they can comprehend each other. This is also the commentator's ability to understand the purposes of the object of interpretation as his own in the literal sense of the word.

Legal hermeneutics is to simplify the dialogue of legal viewpoints, since legal concepts and categories (such as freedom, democracy, and liability) have different meaning in different legal systems [9].

Contemporary legal science has begun to understand the prospects of the hermeneutic approach to analysis of legislative texts. Application of hermeneutics to interpret rules of information law and information security has become quite logical.

We will try to apply the hermeneutic approach to interpreting the concept of enterprise information security systems. Any rule regulating relations that provide information security represents a result created by its author, the content of which must be established by executors or information security subjects. The literal content of a rule always has behind it a second situational sense without adequate understanding of which correct understanding of the sense of the entire rule is impossible. English lawyers have a saying: "A law contains only one half of the content, the other one is hidden, while ideas are within." Similarly, considering any rules, note that it is necessary to find this hidden idea to apply correctly a law in the course of its interpretation. Hermeneutic interpretation of rules and concepts of information security is just the tool by which the problem of double sense can be solved, in that hermeneutics, in addition to decoding of the literal sense of a text carried out through linguistic interpretation, enables to reveal the content of the legal context.

P. Ricoeur notes in his works that hermeneutic analysis of a legal text includes a number of obligatory procedures. Division into understanding, interpretation, and application is generally recognized [11; 12].

Understanding should be understood to mean an art of comprehension of the signs transmitted by one consciousness and perceived by another via their external expression (primarily linguistic).

The unity of the concepts "to understand" and "to interpret" was revealed. Interpretation is not just some kind of separately occurring process, complementing understanding when opportunity offers; understanding is always an interpretation and hence interpretation is an explicit form of understanding. Understanding always involves

something like application of the text to be understood to the present situation.

Application is as much an integral part of the hermeneutical process as understanding and interpretation are. In legal hermeneutics, there is the essential tension between the text set down... on the one hand and on the other, the sense arrived at by its application in the particular moment of interpretation. A law is not there to be understood historically, but to be made concretely valid through being interpreted [11; 12].

V. V. Suslov notes that legal consciousness is similar to historical one, that is, a lawyer must investigate the background of a fact being interpreted. Admittedly, he emphasizes the special relevance of the above-mentioned approach with respect to the process of proving. However, the content of the said paper and logical deduction following from it give the impression that identification of the legislative will is the ultimate goal of hermeneutic interpretation [14]. V. V. Suslov recognizes polysemy of legal texts and relevance of the situational sense hidden behind the literal one but reduces hermeneutics to its historical method of interpreting [15].

Take the problem of understanding an enterprise information security system by analogy with historical hermeneutics. Let us consider the approaches of a historian and an information security subject to the same legislative act in force.

There are obvious differences. A subject comprehends the sense of an information law rule from the perspective of a specific case and for a particular purpose. A historian does not have a specific case he would consider. He seeks to determine the sense of an information law rule by modeling and embracing with a single view the entire sphere of its application. He concretizes understanding of an information law rule only due to all these cases of its application. A historian may not content himself with initial application of an information law rule to determine its sense. Being a historian, he must take into account historical changes an information law rule underwent; he must define his task in terms of modeling the initial content. At the same time, one cannot present the task of the subject as bringing information law rules in line with the current situation. If someone seeks to bring the sense of information law rules in line with the current situation he must know, first, its initial content, that is, he must think like a historian. And the sense is that historical understanding serves him to achieve a certain goal. We are convinced that the legal content of a given operative information law rule is completely unambiguous and that current legal practice merely follows its original content. If such were the case, the styles of legal and historical thinking would be identical. Then, the purpose of hermeneutics would reduce only to identifying the initial sense of a law and further applying it in this initial sense as a true one. Similar to an uttered thought, understanding itself of regulations of an enterprise information security system must not pose any problem when, according to them, an information security subject has to put himself under the conditions of the initial creator of these regulations

ignoring the contradictions that exist between the original and practical legal content of these rules and regulations. The fact that this is a legal error has recently become apparent.

V. Tsymbaliuk showed in his publication that legal reasons imply a need for reflection regarding historical changes due to which the initial sense of a law and the sense applied in practice get detached from one another. A legal practitioner, alias an information security subject, always means a regulatory act (regulation) itself. However, its content should be determined with account of the case to which it should be applied. Ascertaining with exactitude the content of the regulations of an enterprise information security system requires historical knowledge of their initial content, and only because of the latter, the subject takes into consideration the historical meaning a rule (regulation) itself communicates. The subject may not rely solely on what he knows about the intentions and goals of those who developed these rules and regulations, minutes and charters. On the contrary, he must understand the changes occurred within the information security system of an organization and respecify the function of the rules and regulations [16].

A subject applying regulations of an enterprise information security system, which came to him from the past, to his current needs, seeks to solve a practical problem. It does not mean that he comments on it arbitrarily. To understand and comment means that it is necessary to learn and recognize the current sense of the said rules. The subject seeks to comply with the main body of the information security system regulations translating them in a modern way. He seeks to learn just the legal meaning of the rules and regulations of the entire system rather than their historical meaning for which the entire system was put into operation or, for example, of any case of its application.

The rules and regulations of an enterprise information security system should be interpreted by appealing to their own history of creation by construing them in a modern way. He who understands does not opt for his subjective point of view but finds a sense given beforehand. For self-implementation of legal hermeneutics, it is essential that law is equally binding for all members of an organization. Where this rule is violated, for example, at pathological authoritarian organizations, legal hermeneutics is impossible. A leader has a possibility, disregarding the rules he devised himself, without making any effort to interpret them, to obtain any decision that he will consider as correct. The task of understanding and interpretation is worthwhile only where legislative regulations are regarded as universally binding [11].

Conclusions. The rules of an information security system are applied by a subject covered by these rules as any other organization member. The idea of providing enterprise information security stipulates that a managerial decision must be based on adequate (fair) assessment of the situation rather than on arbitrariness. Each member of an organization who delves specifically into the situation at hand is capable of such fair treatment. This is precisely why the organization with an established and well-run information security system, just as a law-governed state, has a

guarantee of obligatoriness for all subject to perform their duties; everyone knows what he has to do and what he can expect. Any employee has an essential possibility at his workplace to make a correct interpretation, that is, correctly anticipate a legal decision based on the current rules and regulations. Rendering a sound decision in a specific case requires taking account of the previous practice, and not only one's own. Having an opportunity to exchange information and experience with similar information security subjects is sufficient for it. There always is an opportunity to take account of the totality of experience, and this makes it possible to dogmatically handle any situation and make the best managerial decision.

REFERENCES

1. *The Constitution* of Ukraine: the Law of Ukraine of 28.06.1996 № 254к/96-BP // The Official Bulletin of the Verkhovna Rada of Ukraine. — 1996. — № 30. — 141 p.
2. *The Declaration* of State Sovereignty of Ukraine of 16.07.1990 № 55-XII // The Official Bulletin of the Verkhovna Rada of Ukrainian SSR. — 1990. — № 31. — 429 p.
3. *Vynohradova, H. V.* Information Law of Ukraine: a Study Guide. — Kyiv: IAPM, 2006. — 144 p.
4. *On Information*: Law of Ukraine of 02.10.1992 № 2657-XII // The Official Bulletin of the Verkhovna Rada of Ukraine. — 1992. — № 48. — 650 p.
5. *On the* National Informatization Program: Law of Ukraine of 04.02.1998 № 74/98-BP? // The Official Bulletin of the Verkhovna Rada. — 1998. — № 27–28. — 181 p.
6. *On the* Concept of the National Informatization Program: Law of Ukraine of 04.02.1998 № 74/98-BP? // The Official Bulletin of the Verkhovna Rada. — 1998. — № 27–28. — 182 p.
7. *Gadamer, H.-G.* The Relevance of the Beautiful. — Moscow, 1991. — P. 7–8.
8. *Gadamer, H.-G.* Truth and Method: Basics of Philosophical Hermeneutics. — Moscow, 1988.
9. *Kuznetsov, V. G.* Hermeneutics and Humanitarian Cognition. — Moscow, 2005.
10. *Plavich, V. P.* Archetypical Praphenomena of Law and its Structure // State and Law. A collection of scientific papers. Legal and Political Sciences. Issue. 24. — Kyiv, 2004.
11. *Ricoeur, P.* Hermeneutics. Ethics. Politics: Moscow Lectures and Interviews. — Moscow, 1995.
12. *Ricoeur, P.* The Conflict of Interpretations: Essays in Hermeneutics. — Moscow, 1995.
13. *Ricoeur, P.* Triumph of Language over Violence: Hermeneutical Approach to the Philosophy of Law // Philosophy Affairs. — 1995. — № 4. — P. 27–34.
14. *Suslov, V. V.* Hermeneutics and Legal Interpretation // State and Law. — 1997. — № 6. — P. 116.
15. *Suslov, V. V.* The Hermeneutic Aspect of Legislative Interpretation // Jurisprudence. — 1997. — № 1. — P. 88.
16. *Tsymbaliuk V.* // legal, Regulatory, and Metrological Support for the Information Security System in Ukraine. — 2004. — № 8. — P. 30–33.