The Role of Information and Communication Technologies in Civil Law Relations: Analysis of the Civil Code of the Republic of Kazakhstan

Submitted: 16 September 2020
Revised: 18 January 2021
Accepted: 21 January 2021

Article submitted to peer blind review

Zhandos K. Zhetibayev*
ORCID: https://orcid.org/0000-0002-7647-9068
Sara K. Idrysheva**

DOI: https://doi.org/10.26512/lstr.v13i2.34142

Abstract

[Purpose] The purpose of the study is to establish using the methods of legal linguistics, synthesis and analysis of information the mechanism of formation of the conceptual sphere of cybersecurity and its representation in the texts of regulations.

[Methodology] The methodological basis of the study was determined by the hermeneutic approach to jurisprudence which is mainly focused on methodology, legal technique, the logical and semantic interpretation of certain provisions of various branches of law. In the process of research, methods of analysis and synthesis of information, the comparative analysis also were used.

[Findings] The authors note that the use of the system of civil law relations affects both the civil sphere directly and the procedural aspects of relations and partially the criminal branch of law. The synergistic nature of informatisation of civil law relations and consider it as a part of the system of general cybersecurity of the state as a whole were emphasized. The use of this concept and its legal construction was revealed.

[Practical Implications] The practical significance of the study is determined by the possibility of forming an integrated system of using the mechanism for predicting the development of information and communication technologies to form an equilibrium environment for ensuring the rule of law.

[Originality] The novelty of the study is determined by the fact that information and communication technologies are understood as components of a larger system of ensuring legal security in a country as a whole.

Keywords: Civil Turnover. Structure. Cybersecurity. Legal Lexicography. Information Law.

*Zhandos K. Zhetibayev – Chairman of the Akkol district court of Akmola region, PhD student at the Higher School of Law, M. Narikbayev KAZGUU University, Nur-Sultan, Republic of Kazakhstan. His scientific interests concentrate on juridical practice and enforcement of law issues. E-mail: zhetibayev5409@uoel.uk.

**Sara K. Idrysheva – Full Doctor in Law, Professor at the Department of Private Law, Higher School of Law, M. Narikbayev KAZGUU University, Nur-Sultan, Republic of Kazakhstan. Her research area includes civil, contract and international law aspects. Address: 010000, 8 Korgalzhyn Highway, Nur-Sultan, Republic of Kazakhstan.

ZHETIBAYEV, Z. K; IDRYSHEVA, S. K. *The Role of Information and Communication Technologies in Civil Law Relations: Analysis of the Civil Code of the Republic of Kazakhstan*. **The Law, State and Telecommunications Review**, v. 13, no. 2, p. 121-138, October 2021.

INTRODUCTION

Cybersecurity is an integral part of national security and then acts as a guarantee of the sovereignty and viability of the state. Therefore, while cybersecurity issues will be resolved segmentally within individual branches of law in different projections and interpretations, it is rather problematic to assert its effectiveness (MACAK, 2016). First of all, the development of conceptual approaches to cybersecurity policy in the conditions of the Republic of Kazakhstan is required, which strategically and tactically unites all aspects of this area of activity. The first steps in this direction have been made, because both the Strategy for Cybersecurity of the Financial Sector of Kazakhstan (Kazakhstan, 2018) and the Doctrine of Information Security (Civil Code, 1994; Message from the President, 19997) were adopted. However, these documents reflect not so much the state of the system in the future, to the construction of which the activities of the national cybersecurity system should be directed, but rather to overcome immediate threats, primarily those associated with the threat from the external environment (AMATO et al, 2020). The complexity and versatility of the problem have led to its research by diverse specialists: lawyers, philosophers and political scientists, information technologies.

Recently, scientific activity in the field of legal linguistics, which is at the intersection of law and applied linguistics, has also significantly intensified (RUTKOWSKI, 2011). In the field of view of scientists, there are various aspects of the formation and functioning of the legal terminology system, the normative nature of the interpretation of linguistic units in legal lexicography, the language of law and speech of laws at the level of the lexical-stylistic and grammatical application of linguistic means in the texts of normative legal acts. Now many new terms need to be studied, for example, the term “electronic transaction”. An electronic transaction is an action of a person aimed at acquiring, changing or terminating civil rights and obligations, carried out using information and telecommunication systems (BAHUGUNA et al., 2018).

Despite significant improvements in related fields of science, the issue of the legal linguistic foundations for the formation of the cybersecurity policy concept sphere practically remained outside the field of vision of scientists, therefore, requires coverage (NAMAZIFARD et al., 2015; WANG, 2017). Using scientific metaphors, a rule of law can be compared to the tip of an iceberg, most of which is underwater. In this invisible part, the conceptual sphere “hides” as a holistically formed idea of a particular concept in its autonomous existence and the paradigm of interaction with other elements of the system (PARMAR and PATEL, 2016). Thus, there is reason to consider the conceptual sphere not only as a conditional abstract but also the materialisation of the ideas of the goal through language. Understanding this mechanism is fundamentally important since that mainly scientists are trying to analyse the texts of acts that are already in force or are proposed as projects (AYALEW TAREKE and DATTA, 2018). Essentially, this is working with results, not with the whole idea model itself. In connection with the above, the problem of methods of working with the metalanguage of various industries is actualised. It should be based on the specifics of each area (WILK, 2016).

Concerning the sphere of cybersecurity, the authors state the fundamentally important influence of the binary nature of key concepts (SEVIŞ and SEKER, 2016). On the one hand, the globalisation of the world is becoming more and more, which has been largely facilitated by the emergence of cyberspace, which breaks traditional boundaries, localisation of information sources, and introduces a transnational component to illegal actions in the field of information technology (JONES and CHOO, 2014). This creates the basis for understanding the scale of single cyberspace and the responsibility of each state to the world community (SHUSHTARI and AMIRI, 2020). On the other hand, ensuring national security has been and remains an integral function of any state (PITZER and GIRDNER, 2014). Since cybersecurity acts as a component of national security, the development, implementation, continuous improvement of systemic administrative-legal, managerial, socio-economic, scientific technologies is required (VAN NIEKERK and RAMLUCKAN, 2019). It is the unified concept of cybersecurity policy implementation that makes it possible to do this effectively (CHOWDHURY, 2016).

Again, it should be borne in mind that there is a multidirectional multifunctional movement in the formation of the cybersecurity policy concept sphere (PITCHAN and OMAR, 2019). Kazakhstan cannot but take into account the experience accumulated by other states. This becomes important both for the adaptation of national legislation and for the implementation of international cooperation in this area solely based on the compliance of this policy with national interests, protection of the information (including cybernetic) sovereignty of the state. Such a situation significantly complicates the task, since it requires a clearly defined conceptual approach to finding harmony between the national and the international.

MATERIALS AND METHODS

The development of a scientific basis for cybersecurity policy is both a theoretical and an applied issue (VON HEINEGG, 2013). Any concept is realised through its materialisation in a category-conceptual apparatus. Consequently, in the framework of the implementation of scientific research tasks on the development of methodological foundations for the formation of a theory of cybersecurity policy, it is advisable to be guided by an interdisciplinary approach, as well as modern legal theories that correspond to the current trends in the development of society. In this context, the methods of legal linguistics and legal hermeneutics are justified (SALEEM, 2019).

The use of this group of methods made it possible to formulate two models for the formation of the concept sphere: a hybrid mental space and a semiotic space. Using this method, the possibility of their application was demonstrated and the effectiveness of using such models was proved, however, emphasising that this was not the only possible way (SANDER, 2019). Undoubtedly, this topic is multi-layered and does not claim to cover everything in its consideration, attempting only to define, according to the subject of the study (LOSAVIO et al., 2019). The purpose of the study of these methods was to establish, using the methods of legal linguistics, the mechanism for the formation of the conceptual sphere of cybersecurity and its representation in the texts of regulatory legal acts.

The extra-linguistic factor gives grounds for using the model of a hybrid mental space, developed by cognitive linguistics specialists J. Fokagnier and M. Turner, in the study of the metalanguage of the cybersecurity policy concept. According to the authors, the theory of conceptual integration uses "blend" as a key concept, which, in fact, is a projection of various spaces that do not intersect with each other, but these spaces can merge into a single whole into a common generic unity, which is called "generic". Therefore, in relation to the state aspects of cybersecurity policy, it is advisable to talk about a certain blend, which is mentally limited by the specifics of the national legal system. Although taking into account the integration in the concepts of cybersecurity of legal, political, information technology categories, it is worthwhile, even on the scale of a single country, to apply the concept of hyperblend as a hierarchical multifunctional inter-scientific concept correlated with the realities of a particular state. The development of general concepts on an international scale goes to the generation level, getting rid of national specifics and conglomerating components common to all blends and hyperblends. Thus, the cognitive model of the founders of cybersecurity policy is based on a well-defined imaginary interaction of blends and hyperblends.

Extrapolation of cognitive activity in the development of cybersecurity policy concepts fits well with the theory of semiotic space. According to this theory, the metalanguage functions in a three-dimensional space, which is represented through the categories of semantics, syntactic and pragmatics.

RESULTS AND DISCUSSION

Features of the Interlanguage Aspects of Semantics in the Case of the Application of Internationalisms

Semantics acts as an integral primary component of the metalanguage. Before the drafter of the law, political scientist, lawyer, first of all, the question arises from the sphere of nomination: how exactly to name this or that concept, phenomenon, legal fact; whether to use in this case already existing linguistic units or to introduce neologisms, including by borrowing and lexicalising foreign words; what principles of nomination should be preferred. The linguistic competence of a cybersecurity specialist should cover the concept of polysemy of terms, their etymology, and requirements for the norms of word use. Interlanguage aspects of semantics in the case of application of internationalism (and there are many of them in the field of legal informatics and cybersecurity, and this can become the topic of a separate study) should take into account the differential features of linguistic units in each individual language.

The authors will demonstrate this with the example of the key term "cybersecurity". According to the word-forming structure, this is a complex abbreviated word, the first part of which is internationalism (in Russian), the second is a common word. It can be viewed as a partial tracing of the international term "Cybersecurity". But the semantics of this lexical unit, according to the definitions contained in the normative documents of different countries, differs significantly. For a comparative analysis, the authors will use the materials of the information note "Legislation and strategies in the field of cybersecurity of the countries of the European Union, USA, Canada and others", prepared by the European Information and Research Centre.

According to the help data, the essence of the concept of "cybersecurity" in some states is conveyed through the keyword "events":

- A set of organisational, legal, technical and educational measures aimed at ensuring the continued functioning of cyberspace (Policy for the protection of cyberspace of the Republic of Poland);
- Measures to prevent harm from failures in ICT operation and its elimination (National Cybersecurity Strategy of the Kingdom of the Netherlands).
- Other states in their normative acts build a definition based on the lexeme "state":
- The desired state of information technology security, due to which the risks to cyberspace are reduced to an acceptable minimum (Cybersecurity Strategy of Germany);

– The desired state of the information system, in which it can counteract the challenges of cyberspace that may negatively affect the reliability, integrity and confidentiality of data stored or processed by this system (France's Information Systems Security and Defence Strategy).

For a person who is not sensitive to language, the difference between state and measures is generally incomprehensible, however, in the formation of concepts of cybersecurity policy, it is fundamentally important to distinguish between these concepts, select priorities, and possibly search for their own approaches. In particular, based on the connotation of objects, the concept of cybersecurity can be focused primarily not only on the technical and technological components (as presented in the above definitions), but also contain a significant humanitarian component, which is methodologically subordinate to the principles of anthropocentrism, because in the end, it is not just the smooth functioning of mechanisms and systems that is important, but the safe existence of people who live in this space. Considering the fact that Kazakh legislation now lacks a legally enshrined definition of the concept of "cybersecurity" (it has yet to be formed and adopted), such a provision is fundamental. It is quite consistent with Art. 1 of the Constitution of the Republic of Kazakhstan, according to which "the Republic of Kazakhstan asserts itself as a democratic, secular, legal and social state, the highest values of which are a person, his life, rights and freedoms" (Constitution of The Republic ..., 2001). Only one example is given, but such situations are typical for almost the entire conceptual apparatus of the studied sphere.

The second aspect of the three-dimensional space of metalanguage is syntactic – a section of semiotics that studies the syntax of various sign systems. It can be roughly compared with the alchemy of words, because the combination of linguistic units at the level of word combinations, microtexts and texts create new intentional spaces. In accordance with the laws of the metalanguage functioning, microtexts and texts can be formed only based on the interaction of individual components of this information and communication space. As an illustration, the semantics of the key for the cybersecurity sphere related terminological combinations "policy" and "cybersecurity policy" can be compared. The point is not only in formal grammatical features, according to which one of them is a combination of an attribute with a nominative, and the other is a nominal construction. The main thing is new lexical and semantic meanings, conveyed by a combination of consonant words.

Thus, syntactic constructions created according to the model "nominative plus nominative in the genitive case" (N + N2) are distinguished by their specification of object relations. In contrast to them, constructions like "attributive + nominative" (Ad + N) convey more generalised characteristics that are generally able to abstract and scale the essence of the concept. It is enough to compare the syntactic pairs “civil society” – “society of societies” or “information law” and “right to information” with the analogue of such constructions.

Returning to the terminology of the sphere of cybersecurity, it is worth noting that it is the methods of legal linguistics that make it possible to differentiate the semantics of the terms under study. Therefore, the concept of “cybersecurity policy” is more specific and narrow. It can be used (and, by the way, is used) in the activities of individual institutions, organisations, establishments, commercial structures to designate management requirements for the safe use of computer equipment in compliance with the confidentiality of information, rules of official conduct on the Internet. If it is about “cybersecurity policy”, then it means the systemic activity of the state to counter information threats spread through the cyberspace, the coordination of the activities of all state and non-state structures involved in ensuring cybersecurity, protected from possible illegal actions in this area.

Along the way, it should be noted that the potentials of speech mean to play a significant role in syntactic. So, for example, according to the rules of the Russian language, only a nominative construction is possible (“policy of cybersecurity”). The English-language analogue “security policy”, depending on the context, can be translated into Kazakh in two ways. Syntactics as a component of the legal and linguistic foundations of the formation of the conceptual sphere of cybersecurity policy is an equally important component of the fund of the category and conceptual apparatus of this sphere. In the end, pragmatics in the context of the formation of the concept sphere pursues a solution to the applied aspects of the problem using linguistic means. First of all, it is about defining the goals and priorities of the cybersecurity policy, the range of subjects that act as carriers of such a policy. On the other hand, pragmalinguistics allows effectively solving legal-stylistic and communicative tasks that arise at the stage of creating regulatory legal acts. Thanks to pragmatics, it is possible to integrate cognitive, logical, methodological components of mental meaning at the level of concepts, and this, in turn, allows systematising the picture of the world.

Pragmatics to a certain extent reflects legal discourse since it incorporates not only constant characteristics that are more inherent in semantics and syntax, but is also able to clearly respond to the dynamics of rapid changes in society, the emergence of new realities and modern challenges. Again, if semantics and syntactic are mainly focused on the accuracy of the formulation of information, then pragmatics introduces components of perception (mutual understanding, taking into account the peculiarities of perception of others) and interaction (ways of organising communicative interaction).

The specificity of the interaction of the considered conditional coordinate system, which is the basis of the research model, lies in the fact that each of them, despite its autonomy, manifests itself in interconnection and, during the formation of the concept sphere, is implemented in an integral unity. This can be seen very clearly at the level of reflection of the cybersecurity terminology in the priority lists of the political strategy and tactics of various states.

In the United States, the preference is mainly for the term "cybersecurity," that is, the emphasis is on the security of the Internet architecture. At the same time, China and Russia use the concept of "information security" much more often with an emphasis on restrictions on the information dissemination and texts censoring. Thus, the analysis makes it possible to form a paradigmatic multivector character of interpretation of basic concepts, to identify the direction of cybersecurity policy from the methods of creating conditions for the implementation of national interests to prohibitive and restrictive methods.

Of course, within the framework of the study, it is impossible to demonstrate an analysis of the terminology that forms the entire arsenal of the cybersecurity policy concept sphere by using the semiotic space model. This is just one of the models that is functionally effective when working with ideologemes. Therefore, further it is necessary to consider other approaches. One of the scientific methods of such research can be a hermeneutic approach, in particular, the method of legal hermeneutics, with the help of which it is possible to analyse and compare the cybernetic and information space.

Analysis of the Hermeneutic Approach as a Method of Forming the Correct Conceptual Apparatus

Legal regulation of cybersecurity policy, including legal support of cybersecurity, is based on the category-conceptual apparatus of science. The use of key terms as nominative units is based on a clear understanding of the semantics of each of them. Consequently, within the framework of the formation of the theory of cybersecurity policy, the scientific task of forming a correct conceptual apparatus arises. On this path, one of the necessary methodological techniques, which is adequate for solving this problem, is the use of a hermeneutic approach for the study of terminological combinations, highlighting their integration and differential features. Taking into account the obtained data in the future will serve to form a scientific position regarding the proposal of definitions of certain terms, and will also allow in the future to improve the legal technique of rule-making in this area.

The rapid development of science and technology, which fundamentally changes the living conditions of each person and society as a whole, is mainly focused on the field of information, especially in the collection, analytical processing, storage, processing and formation of new knowledge, norms and dissemination of modern data. In this regard, the interpretation of meanings is of particular importance, which is extremely important for the law. The problems of legal regulation of the information sphere, which is a narrow sense can be attributed to the branch of information law, are in fact syncretic, since in their versatility they correspond with a number of other sciences, in particular: administrative law, cybernetics, management theory, philosophy of law, political science, national security, criminology, applied linguistics. The limitation of only one narrow segment of knowledge in the study of complex objects leads to the number of storeys of scientific conclusions, irrational wandering in search of objective laws that manifest themselves only under the condition of a systematic approach. In this regard, when studying integration issues, it is important to refer to the scientific works of scientists from different industries. On the other hand, one cannot ignore the fact that the foundations of legal hermeneutics are emerging step by step in the domestic field.

The attention of scholars who deal with the hermeneutic aspects of jurisprudence is mainly focused on methodology, legal technique, the logical and semantic interpretation of certain provisions of various branches of law, which is, of course, important for the further advancement of scientific thought and coverage of new theoretical and applied problems. At the same time, this area has significant potential due to the wide field of realities covered by jurisprudence.

Highlighting the previously unresolved parts of the general problem in this context, it can be noted that despite the extreme urgency of information and cybersecurity issues and the corresponding directions of state policy, the constantly growing interest of scientists in legal hermeneutics, the integration sphere of the intersection of the two indicated planes has not yet found its proper reflection in scientific works. This situation, to a certain extent, leads to a disorder of terminological consumption, which, in turn, hinders the development of the concept sphere, and hence the practical implementation of the foundations of the state's information security. The use of the hermeneutic approach will make it possible to analyse the key elements of the categorical and conceptual apparatus of information law and determine the directions for improving civil legal regulation in this area.

Recent high-profile events, in particular the intensification of cyberterrorism – attacks by the so-called “Petya.A” computer virus, have clearly demonstrated the scale of threats not only to the state, but also to individual citizens due to the ineffectiveness of measures taken in the field of cybersecurity. It would be methodologically incorrect to assert that the problem lies only in technology, because understanding the complexity of the anticipatory, proactive nature of counteraction is the only thing that can further protect not only the Kazakh, but also the international community from similar cyber incidents.

Thus, there is a need for scientific support of the processes of fundamental renewal of the cybersecurity strategy, including the improvement of legal norms governing activities in this industry. One of the first steps on this path should be the development of the hermeneutic foundations of rule-making, clear differentiation of the semantics of key concepts. First of all, there is a need to define the essence of the concept of hermeneutics. The etymology of the name is associated with the name of the god Hermes, who in ancient mythology was positioned as a mediator between gods and people, conveying the last essence of the will of the higher ones, explaining God's commands. Therefore, the nomination itself reflects the ancient chronology of the existence of hermeneutics. However, despite a long period of development (from antiquity to the Renaissance and modern times), the range of coverage of various branches of science (from theology, philosophy, linguistics to the law), hermeneutics is only now gaining widespread acceptance and recognition. One of the proofs of this is the absence of a corresponding dictionary entry during the period of Soviet history.

The key concept is presented as art and theory of interpretation of texts, the original meaning of which is not clear due to their antiquity or incompleteness. This interpretation was borrowed from the understanding of hermeneutics within the framework of the Alexandrian and Antiochian schools, in which hermeneutics was interpreted as the doctrine of understanding any texts. Moreover, this art concerned the interpretation of the statements of the priests and oracles. Subsequently, hermeneutics in the Middle Ages was transformed into the doctrine of the interpretation of sacred texts, in particular the Bible (exegesis).

This interpretation cannot meet modern requirements for a number of reasons. First, in the above definition, art precedes. This means that in such a situation, the emphasis is on intuition, inspiration, the ability of a subject, and not on scientific foundations. In advance, the problematic is transferred into an emotional-evaluative sphere, devoid of objectivity, but permeated with the subjective perception of the surrounding reality. Secondly, the concept of “primary meaning” is rather vague. Obviously, it is about the author's creative intention, his vision. However, who, besides the author himself, can know what he meant by creating this text. Another person can only assume something, not assert. Thirdly, pointing to the antiquity or incompleteness of the texts, a compiler of this definition deprives scientists of the right to interpret modern documents, including regulatory legal acts. Even this example clearly demonstrates the non-modern understanding of the key concept, not to mention the derived categories and, accordingly, the formation of the paradigmatic foundations of the study.

Hermeneutics is defined as a separate science aimed at interpreting the deep meaning of texts, their translations by studying the structure and semiotic nature of the language, studying historical, philosophical, religious and other data related to a specific type of literary work. The goal of hermeneutics is to achieve a correct understanding of texts, and its most important tool is the principle of dialogic of humanitarian knowledge, which has an interpretive character, since interpretation is an eternal moment, a form and way of functioning of philosophical knowledge: new philosophical knowledge is always the result of interpretation. Considering that the object of hermeneutics was constantly changing, it was a historical, philosophical, religious, artistic text, the boundaries of hermeneutics remained undefined for a long time. Hermeneutics was viewed as an art and a theory of text interpretation, as a formula of historicism, a methodology of humanitarian knowledge, a methodology of scientific knowledge in general, a philosophical ontology and a way of philosophising, a kind of social therapy.

Hermeneutic procedures are used in legal sciences dealing with the analysis of the objective results of a person's conscious activity. Hermeneutics acquires: the function of ontology, since being, which can be understood as a language; social philosophy, since understanding is a form of social life and criticism of ideology. Actually, this contributed to the branching and further differentiation of the directions of development of hermeneutics and led to the emergence of legal/juridical hermeneutics. The above attributes should be considered as complete synonyms, differing only in their origin, where legal is a Kazakh word, and juridical is Latin. Therefore, both options are used in the literature, while the authors give preference to the first.

It should be noted that until now scientists do not have unanimous views on the interpretation of the key concept. So, quite often cited is the expression according to which hermeneutics is proposed to understand the science and art of interpreting legal terms and concepts, the pinnacle of legal skill, the culmination of legal activity. It seems that this definition is not devoid of emotional pathos. In addition, it limits the scope of legal hermeneutics to the lexico-semantic level of individual nominations, without affecting the level of textology, without going beyond the level of understanding the meaning of texts to the level of comprehending the meaning of the text.

Somewhat broader (and closer to the authors’ understanding of the essence of the term) legal hermeneutics is interpreted as a special method of interpreting a legal norm, including not only literal decoding of the text of the norm that is being interpreted, but also an assessment of the legal situation accompanying the implementation of this norm. It is proposed to understand legal hermeneutics as the scientific direction of thinking in the legal sphere, understanding, interpretation, interpretation of the norms of ordering social relations and the creation of legal norms and texts of normative documents. Generalisation and systematisation of the views of scientists give grounds to assert that the semantic field of the key concept "legal hermeneutics" covers: methodology; science, science and art; scientific direction; direction of jurisprudence; an approach; method; process. This is evidence of the lack of a unanimous understanding of the concept by scientists, which is caused by the polysemy of the term. Therefore, depending on the context, it can be used in different meanings.

When studying legal hermeneutics, one should also understand its binary nature: on the one hand, there are methodological, logical, technological paradigms that act as universals regardless of a country, its state structure; on the other hand, a sign, symbolic nature of each language, the peculiarities of the principles of nomination, logical-semantic structures at the level of vocabulary, morphology, syntax and textology determine the specificity of hermeneutics in its specific localised manifestations. Considering that the branch of information law is at the stage of its formation, there is reason to assert that the formulation of its norms takes place both on the basis of approved methods of legal technique and in the search and interpretation channel. Thus, the semantic analysis of key terms, which is at the centre of this research, should be carried out in the paradigm of the hermeneutic approach, which allows the most objective definition of the essence of concepts. At the same time, such an analysis creates the basis for the differentiation of basic terms, without which their application in legal documents becomes quite problematic.

It is characteristic that the high frequency of the use of the terminological combinations, such as "cyberspace" and "information space", has made them a kind of cliché. However, behind the apparent simplicity and clarity a serious scientific problem of distinguishing between concepts hides. Comparing the specified terminological combinations, to the presence of a common nominal component draws attention. By the way, it acts as internationalism, since in the English-speaking counterparts the element "Space" in the main seme also means "space". Referring to linguistic dictionaries allows establishing the ambiguity of a lexeme, which simultaneously acts as a common word and as a term in a number of sciences, primarily philosophy, economics. In fact, it can be stated that the term was formed precisely through the specialisation of the common word. Therefore, values such as:

- Philos. One of the forms of existence of matter, which is characterised by length and volume.
- Unlimited extent (in all dimensions, directions); three-dimensional extent above the ground.

- Free, great view; spaciousness.
- Paleo. The absence of any restrictions, obstacles in something; will.

Therefore, the question arises: in what meaning is the key term used in legal texts? Since at present there are no standardised definitions of the key terms that are researched in the current regulatory legal acts, the texts of the current legislation of the Republic of Kazakhstan were analysed. Therefore, using the methods of semantic analysis, it has been established that the contextual use of the term is based on the same, which conveys the meaning of multidimensional unlimited extension. At the same time, the national segment of the information and cybernetic space is a priori considered not in isolation, but as part of the corresponding world space.

It is characteristic that, similar to the English-language analogue ("cyberspace"), the Kazakh terminological combination based on the principle of linguistic economy is most often used in the texts of regulations and in scientific works in the form of a complex abbreviated word, while the term "information space" cannot be abbreviated. Therefore, the semantic differentiation of paired nominations occurs on the basis of attributive components. In this regard, it is advisable to consider and compare the semantic fields of related terminological systems.

The legal definition of cyberspace is included in a number of laws and regulations. According to them, cyberspace is understood as an environment that arises as a result of functioning on the basis of uniform principles and according to general rules of information (automated), telecommunication and information-telecommunication systems. In passing, it is worth noting that the term is interpreted based on the word "environment". From the standpoint of the hermeneutic approach, this is very significant, since in its semantics, the "environment", firstly, has more or less clearly defined boundaries, and secondly, it coexists with other spheres. Among other things, the meaning of the word contains an understanding of the filling of this space with certain material objects. Thus, it is advisable to consider cyberspace not just as an environment, but as a systemic, complex environment that functions and develops as a result of the interaction of subjects (persons) with technology using certain technologies with certain (legitimate or illegal) goals.

In the context of strategic cybersecurity, it is regarded as another, the newest environment, along with those that have become traditional, is gradually turning into a field of warfare, in which the corresponding units of the armed forces of the leading states of the world are increasingly active. The latter is very important in view of the fact that some scientists, substantiating the methodological foundations of the concept of cyberspace, argue that it cannot be recognised as a kind of real physical space. It can be interpreted as a kind of perceptual or conceptual space, that is, it can be attributed to the inner world of a subject, a person. Such a position cannot be considered acceptable, since it artificially narrows the sphere of functioning of the phenomenon of cyberspace, leaving out of its technical component, which is essentially the core of the key concept. Thus, the semantics of the concept of cyberspace is reduced to the concept of "virtual space". Despite the presence of related semes in the given terms, such interchangeability contradicts the methodological principle of scientific character. The position is based on the fact that cyberspace is hybrid, combining material and imaginary components, since it cannot exist without its instrumental and technological component, without the real activities of persons, professional or amateur, lawfully or illegally acting in this area. This lays the foundation for the legal regulation of activities in the cyberspace, forms the basis for understanding the development of directions of state cybersecurity policy.

In contrast, the concept of "information space" is more abstract and voluminous. The symbolic nature of information gives grounds to explore the information space, first of all in the context of semiotics, and only then – in cybernetics. When it comes to the application of the concept of "information space" in the legal sphere, in particular, in the texts of laws and bylaws, one should rely primarily on the norms of information law (possibly subsequently, cyber law). Note that, at the same time, the concept of "cyberspace" in the legal paradigm tends more towards the field of information and cybersecurity. In this context, one should separately express an opinion about the need for certain scientific studies of narrative semiotics as methods of text analysis in cyberspace, which will allow reconstructing the narrative structures of the text that form the connection between the surface (the text itself) and the deep structure (the system of values, norms and instructions of the subject of cyber relations – the author). In Kazakhstan, this topic, within the framework of legal regulation of analytical activity, is being developed in the study of the formation of analytical narratology.

CONCLUSIONS

The specificity of the information space lies in the fact that it acts primarily as a social component of the life of society, including political, economic, educational, scientific, legal, cultural, documentary and other components. One should not lose sight of the fact that this space covers and provides for the preservation and transmission of culture, traditions, certain ideologemes to the next generations, that is, it acts as a kind of carrier of "social memory", the legacy of basic meanings and concepts that form the identity of each social system. This makes it possible to consider the semantics of the terminological message not only in the coordinate system of length and volume, but also in time coordinates.

Therefore, in the study of the concept of "information space", both functional and structural, systemic, evolutionary approaches can be applied in their synchronous and diachronous sections. This is due to the specifics of the object itself, which is a multilevel hierarchical structure that includes a set of diverse information systems.

Useful in this perspective is the use of a semantic differential – a method of measuring expert opinions, views and values through a set of bipolar graded evaluation scales, the opposite poles of which are set using verbal antonyms.

Summarising the scientific foundations of the connotation of the concept of "information space", there are three main positions:

- **Territorial:** localisation of information sources, location of databases, place of residence of the population, limits of action of certain legal norms, etc.
- **Geopolitical:** ensuring the information security of the state in the context of globalisation of the world, preserving national information sovereignty.
- **Properly Social:** perception and transformation of information by subjects by filtering and processing information using certain mental models, which allows evaluating various situations and make decisions.

Considering the attempt to systematise the existing approaches to the definition of the concept of "information space" to a certain extent, one should express the opinion that the fourth, unspecified position, the integration one, also has a right to exist. It is due to the fact that in modern conditions the information space is more and more based on information and communication technologies and is increasingly connected with cyberspace. Hence, it becomes necessary to further study the properties of concepts with the transfer of the scientific foundations of cybernetics, information law, information security, legal informatics, applied linguistics to the practice of law-making and law enforcement. That is why a logical continuation of the study is the research of the representation of the terminology of cybersecurity policy in the texts of regulatory legal acts.

REFERENCES

AMATO, F.; CASTIGLIONE, A.; COZZOLINO, G.; NARDUCCI, F. A semantic-based methodology for digital forensics analysis. *Journal of Parallel and Distributed Computing,* v. 138, p. 172-177, 2020. DOI:10.1016/j.jpdc.2019.12.017.

AYALEW TAREKE, T.; DATTA, S. Automated and Cloud Enabling Cyber Security Improvement in Selected Institutions/Organizations. *Proceedings of the 2nd International Conference on Computing Methodologies and Communication*, Erode, India, p. 533-538, 2018. DOI:10.1109/ICCMC.2018.8487245.

BAHUGUNA, A.; BISHT, R. K.; PANDE, J. Roadmap Amid Chaos: Cyber Security Management for Organisations. *Proceedings of the 2018 9th International Conference on Computing, Communication and Networking Technologies,* Bangalore, India, p. 1-6, 2018. DOI:10.1109/ICCCNT.2018.8493977

CHOWDHURY, A. Recent cyber security attacks and their mitigation approaches – An overview. *Communications in Computer and Information Science,* v. 651, p. 54-65, 2016. DOI:10.1007/978-981-10-2741-3_5.

Civil Code of the Republic of Kazakhstan, 1994. Retrived from: https://online.zakon.kz/document/?doc_id=1006061.

Constitution of the Republic of Kazakhstan, 2001. Retrived from: https://www.akorda.kz/ru/official_documents/constitution.

JONES, D.; CHOO, K.-K. R. Should there be a new body of law for cyber space? *Proceedings – 22nd European Conference on Information Systems,* 2014. Retrieved from: https://aisel.aisnet.org/ecis2014/proceedings/track11/4/.

Kazakhstan approves the Cybersecurity Strategy of the financial sector for 2018-2022. 2018. Retrieved from: https://www.zakon.kz/4945077-v-kazahstane-utverzhdena-strategiya.html.

LOSAVIO, M.; HINTON, J.; FRITZ, K.; LAUF, A.; HIEB, J.; IM, G.; BERGMAN, M. STEM for Public Safety in Cyber: Training for Local Law Enforcement and Cyber Security. *Proceedings of the 2019 9th IEEE Integrated STEM Education Conference***,** Princeton, New Jersey, p. 215-221, 2019. DOI:10.1109/ISECon.2019.8881990.

MACAK, K. Is the international law of cyber security in crisis? *Materials of the International Conference on Cyber Conflict,* p. 127-139, 2016. DOI:10.1109/CYCON.2016.7529431.

Message from the President of the country to the people of Kazakhstan "Kazakhstan - 2030: prosperity, security and improving the well-being of all Kazakhstanis", 1997. Retrieved from: https://online.zakon.kz/m/Document/?doc_id=1015368.

NAMAZIFARD, A.; AMIRI, B.; TOUSI, A.; AMINILARI, M.; HOZHABRI, A. A. Literature review of different contention of E-commerce security and the purview of cyber law factors. *Proceedings of the 9th International Conference on e-Commerce in Developing Countries: With Focus on e-*

Business, Isfahan, Iran, p. 1-14, 2015. DOI:10.1109/ECDC.2015.7156333.

PARMAR, A.; PATEL, K. Critical study and analysis of cyber law awareness among the netizens. *Advances in Intelligent Systems and Computing*, v. 409, p. 325-334, 2016. DOI: 10.1007/978-981-10-0135-2_32.

PITCHAN, M. A.; OMAR, S. Z. Cyber security policy: Review on netizen awareness and laws. *Journal Komunikasi: Malaysian Journal of Communication*, v. 35, n. 1, p. 103-119, 2019. DOI:10.17576/JKMJC-2019-3501-08.

PITZER, D. R.; GIRDNER, A. M. Addressing and managing cyber security risks and exposures in process control. *Proceedings of the Society of Petroleum Engineers – SPE Intelligent Energy International 2014***,** Utrecht, The Netherlands, p. 866-882, 2014.

RUTKOWSKI, A. Public international law of the international telecommunication instruments: Cyber security treaty provisions since 1850. *Info***,** v. 13, n. 1, p. 13-31, 2011. DOI:10.1108/14636691111101856.

SALEEM, M. Brexit impact on cyber security of United Kingdom. **Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services, Cyber Security**, Oxford, United Kingdom, pp. 1-6, 2019. doi: 10.1109/CyberSecPODS.2019.8885271.

SANDER, B. The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations. *Materials of the International Conference on Cyber Conflict,* Tallinn, Estonia, p. 1-21, 2019. DOI:10.23919/CYCON.2019.8756882.

SEVIŞ, K. N.; SEKER, E. Cyber warfare: Terms, issues, laws and controversies. *Proceedings of the 2016 International Conference on Cyber Security and Protection of Digital Services, Cyber Securit***y,** London, United Kingdom, p. 1-9, 2016. DOI:10.1109/CyberSecPODS.2016.7502348.

SHUSHTARI, A.; AMIRI, A. P. The position of cyber security in Iranian E-commerce law (Case study: Consequences of cyber-attack on digital signature). *Journal of Critical Reviews*, v. 7, n. 7, p. 120-124, 2020. DOI:10.31838/jcr.07.07.19.

VAN NIEKERK, B.; RAMLUCKAN, T. A legal perspective of the cyber security dilemma. *Materials of the European Conference on Information Warfare and Security,* p. 544-550, 2019.

VON HEINEGG, W. H. Chapter 1: The tallinn manual and international cyber security law. *Yearbook of International Humanitarian Law***,** v. 15, n. 3, p. 3-18, 2013. DOI: 10.1007/978-90-6704-924-5-1.

WANG, C. Analysis of six legal systems on cyber security law. *Nanjing Youdian Daxue Xuebao (Ziran Kexue Ban)/Journal of Nanjing University of Posts and Telecommunications (Natural Science)***,** v. 37, n. 1, p. 1-13, 2017. DOI:10.14132/j.cnki.1673-5439.2017.01.001.

WILK, A. Cyber Security Education and Law. *Proceedings of the 2016 IEEE International Conference on Software Science, Technology and Engineering,* Beer-Sheva, Israel, p. 94-103, 2016. DOI:10.1109/SWSTE.2016.21.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET