World Applied Sciences Journal 27 (Education, Law, Economics, Language and Communication): 371-374, 2013
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2013.27.elelc.75

Formation of Cybersafety Policy (Ukranian Experience)

Irina Nikolaevna Sopilko

Law Institute, National Aviation University, Kiev, Ukraine

Abstract: The article treats the features of formation of the modern information society and the threats emerging due to the uncontrolled information relations that bear the multivector nature. Therefore, the development scientific principles of the policy of cybersafety are in general one of the ways of solving the problem by improving the cybersafety policy by adopting the Concept of state information policy and the Information code. The importance of adopting these documents is dictated by the need for legal ordering of the cybersafety matters. The main purpose of the cybersafety policy is to preserve the integrity of nations in the society, states, creation of real and effective mechanisms of assuring information rights and personal freedom in the cyberspace, prevention of public opinion manipulation and state interests. An essential item in the article is exploration of the conceptual principles of cybersafety policy.

Key words: Cybersafety · Cyberthreat · Cyberspace · Information · Legal relations · Policy · Cybersafety policy concept · Information code.

INTRODUCTION

Contemporary globalization state necessitates the rethinking of public needs in all spheres of life, including in science. Now we are on the threshold of the new synthesis era. We witness return to the large-scale thinking in all domains of knowledge, from precise sciences to sociology, psychology and economics, to combining the components into the integrity [1, page 223]. The problem of relation between globalization and information society evolution has been attracting a lot authors over the world. The number of analytical studies keeps growing in which authors investigate the globalization challenges from the system viewpoint and its influence in all public life spheres. Particular foreign authors call the modern society type the information or the net society [2-7]. Hence, the tendency is growing to represent the modern society as mismatch between information relations confronted with new challenges and threats. M. Thatcher has noted tat these challenges are harder overcome by the states with made mistakes in managing people and resources [8, page 16]. Though many researchers refer these threats to purely information with the consequences bearing multivector nature, therefore they affect the entire sphere of public relations.

The nave and concept of the latest society progress proposed by M. Kastels is the most popular and now adopted by the USA the state level as the conceptual idea of the new stage of public relations [9].

That is why it is actual to develop new algorithms of controlling these relations and forming the comprehensive legal instructions. This problem can be solved by implementing a more global challenge of development the cybersafety policy scientific principles. therefore, it is realized more urgent thee new state role as a civil society political ad territorial body pursing its policy expanded from the usual spheres to the home, external, economic, scientific and technological, humanitarian, social and other domains involving the cybersafety policy implementation. A significant variety of threats nowadays leave behind the state abilities to predict them in time, detect and neutralize or effectively prevent. It is exactly the essential scientific comprehensive interdisciplinary challenge necessitating to develop the scientific principles of cybersafety policy.

The urgency of this problem is due rather to the neglect by scientific circles the actuality of its solution correlating with modern tendencies of rapidly progressing digital world, transformation of information society based on its net and other communities.

Corresponding Author: Sopilko, Law Institute, National Aviation University, cosmonaut Komarov prospect, 1, 03058, Kiev, Ukraine.

The aim of the present article is to outline the conceptual scientific principles of forming the cybersafety policy in Ukraine.

To implement this aim the following tasks are formulated: to determine the prerequisites of cybersafety policy evolution and basic structural components of this policy. To this end, the scientific methods are applied of the information law, the state theory and law using the interdisciplinary approach.

Main Part: A significant number of scientific works in Ukraine and abroad deal with the information society safety, it should be emphasized that these studies ignore the modern tendencies of cyberspace evolution; they deal mostly with systematization of information legislation and setting up various information law bodies.

The information society phenomenon is treated on the basis, mainly, of non-axiomatic provisions of information sociological paradigm. Moreover, the information society essence is disclosed through the science domain which the researcher represents.

This situation has led to complete chaos both in the information law and cybersafety studies which are unable at present to provide a satisfactory paradigmal concept of the state information policy, let alone development of new scientific principles of cybersafety policy.

The levels of studies in this domain are quite high in Russia both for efficient legal management and implementation of the tasks of effective state formation set up by the Russian President.

For instance, one of the fundamental works at present remains the manual authored by a number of scientists and edited by V.D. Popov 'Information policy' [10] and the work by V.N. Lopatin which outlines the principles of systematic comprehension of the state policy information component [11].

It can be stated that special publications display only some problems of this policy development without reaching the strategic systematic level.

Moreover, the analysis of fundamental documents in the national security, including the information security sphere, enables to state that there is a significant legal potential: The doctrine of information security in Russia endorsed in 2000году, The strategy of information society development in Russian Federation approved in 2008, the priority problems of scientific research were endorsed in the same year to provide the information security in Russian Federation.

As regards directly the information policy, it is treated as the humanitarian policy component in the context of implementation of other state national interests of Russia, identification of threat sources to the state.

The situation in Ukraine can be characterized differently. For instance, the national institute of strategic research carries out the systematic study of both the information safety and other adjacent problems. This approach enables to promote the state making decisions from the subjective level to that of scientific research and national interests.

The problem of information security and cybercrime is solved now globally. The parliamentary session of the Eurounion adopted resolution No 1565 (of 2007) emphasizing that all the states should be applied measures against application of computer technologies for criminal purposes; it necessitates the development of international protection and retaliation system.

The resolution states specifically that implementation of the Convention of cybercrime by all Eurounion concerned and non-affiliated states are one of the most important tools to put this problem under control.

In our view, a working group should be urgently set up to protect Ukraine from cybercrime in order to complete fully and adopt the Ukrainian Information code which should be a logical step towards adoption of the state information policy concept intended to be leader in solving cybersafety matters. These documents should be permeated with common ideology; their main sense should in modern world be aimed providing Ukraine's information sovereignty a reliable protection from cyberthreats.

The author proposes own vision of the cybersafety policy concept.

Ontological cybersafety policy base is the paradigmal comprehension of the multivector information society development and its alternatives implying that it is impossible to determine beforehand the progress trends and correspondingly to manage a broad spectrum of information legal relations by applying legal norms. The imperative paradigmality dualism regarding the need of clear-cut state control and imminent alternatives in the information society development as a result of transformation of globalization processes is the initial postulate of this concept. It should reflect the principles of state progress vision in the contemporary conditions when it preserves the leading and determining role in public processes, including the account of anthropological ideas, particularly, the achievement of wise balance between egocentrism and state-centrism. These two factors are studied in Ukraine rather profoundly within the scientific schools of the theory of right and state and the philosophy of right.

The gnoseological cybersafety policy concept basis is the possibility of overanalyzing the interdisciplinary methodology of its formation and to apply the relevant

adequate methodological tools to promote the efficient cybersafety policy mechanism with the account of modern tendencies such as the account of new cyberthreats and making the sciences interdisciplinary. In contemporary conditions, scientists should specialize on particular problems rather than particular sciences. In Ukraine, a considerable work is underway to form the science of information right, to set apart an individual specialty and train highly qualified personnel. Meanwhile, this work is conducted just with the account of traditions of legal sciences and, to some extent; the available achievements in the sphere of international relations are ignored, in particular, those of the specialty of international information. It proves that scientific research lacks conceptually the creative potential and motivation of its development so that the initial boundaries between the methodologies of one science are not delineated (jurisprudence, international relations, economy and others). It results in fact that the systematic problem is treated fragmentary due to the limitations of the mythodolological scientific potential used to explore the systematic phenomenon rather than the researcher's narrow mindedness.

One of the solutions to this situation is to develop the information sociology. In our view, the urgent challenges are the scientific novelty of interpretation of information sociology to be solved by developing the following trends:

- Information acmeology;
- Information ethics;
- Information policy;
- Cybersafety policy.

The main attribute of modern information sociology should be systematic vision of information society and the main is the state role in its effective progress, including by applying administrative, legal and other mechanisms.

The axiological basis of the cybersafety policy concept in case of its legitimization should be the value the document proper contributes to this conceptual level. The contemporary world and formation of its digital universe are unfeasible beyond the cybersafety policy context. The effective state policy progress is unfeasible equally beyond the cybersafety policy and information society. Hence, the main value of this policy is its ability to form main values for which this policy should be persecuted. Regarding this concept essence status, it should be noted that it plays a leading role in the formation of tendencies of both the state policy and information law.

CONCLUSIONS

The state cybersafety policy is formed and implemented when the difference between national and global cyberspace is leveled in the contemporary world, the number of attacks by hackers and the scale of illegal actions augment in the cyberspace, a stable tendency is witnessed that new cyberthreats appear and the cyberspace itself is used more to create stable algorithms of modern civilization control and the space is transformed into the future information battlefield.

The information law poor effectiveness presupposes the ineffiveness of international legal mechanism and cooperation in general in implementation of the cybersafety policy in broad sense.

Therefore, the main requirements to the state cybersafety policy should be emphasized. The latter is expected to perform the following:

- Use the requirements of the Ukrainian Constitution, the provisions of the Concept of state information policy, the Strategy of the Ukrainian national security, the theory and experience of information security, the doctrines of the Ukrainian national security information security based on both home and foreign experience;
- Facilitate the demithization of unambiguous positive perception of information society and to learn the right and adequate interpretation by public of the danger of information society uncontrollable evolution;
- Facilitate disclosure of the falsified interpretation of the state policy provisions and teach how to counteract it;
- To lay foundation of advance development of the legal base to adjust the information legal relations;
- To teach the corresponding culture of cybersafety;
- To reinforce the cybersafety levels;
- To assure formation of universal approach to cybersafety policy implementation at all state levels;
- To use this policy and elaborate the aims, functions, principles and methods of teaching and implementing the cybersafety policy;
- To teach the principles of identification of trends of evolution of the general state cybersafety system.

REFERENCES

1. Toffler, E., 2004. Third wave. Moscow, pp 781.
2. Castels, M., 2000. End of Millennium. New York: Wiley-Blackwell, pp: 448.

3. Castels, M., 2003. The Internet Galaxy: Reflections on the Internet, Business and Society. New York: Oxford University Press, USA, pp: 304.
4. Castels, M., 2004. The Power of Identity: The Information Age: Economy, Society and Culture. Dual City: Wiley-Blackwell, pp: 560.
5. Castels, M. and P. Himanen, 2004. The Information Society and the Welfare State: The Finnish Model. New York: Oxford University Press, USA, pp: 216.
6. Castels, M., M. Fernandez-Ardevol, Q.J. Linchuan and A. Sey, 2006. Mobile Communication and Society: A Global Perspective (Information Revolution and Global Politics). New York: The MIT Press, pp: 345.
7. Castels, M. and G. Cardoso, 2006. The Network Society: From Knowledge to Policy. New York: Center for Transatlantic Relations, Jhu-Sais, 434: 8-9.
8. Thatcher, M., 2003. The art of state administration: strategy of changing world. Moscow, pp: 504.
9. Ñlinton, B and A. Gore, 2000. White Paper "Technologies for America's Economic Growth, A New Direction to Build Economic Strength". Pedro Conceicao. Science, Technologie and Innovation Policy: Opportunities and Challenges for the Knowledge Economy. Greenwood Publishing Group, pp: 578.
10. Information policy. Moscow, 2003, pp: 312.
11. Lopatin, V.N., 2000. Information security in Russia: Man. Society. State. Saint-Petersburg, pp: 428.