E-ISSN: 2360 – 6754; ISSN-L: 2360 – 6754

European Journal of Law and Public Administration

2018, Volume 5, Issue 2, pp. 128 -136

https://doi.org/10.18662/eljpa/48

THE CRIMINAL LAW PROTECTION OF PUBLIC REPLATIONS IN THE FIELD OF FORMATION OF INDORMATION RESOURCE

Khrystyna VOROBETS

Covered in:

CEEOL, Ideas RePeC, EconPapers, Socionet, HeinOnline

Published by:

Lumen Publishing House

On behalf of:

STEFAN CEL MARE UNIVERSITY FROM SUCEAVA, FACULTY OF LAW AND ADMINISTRATIVE SCIENCES, DEPARTMENT OF LAW AND ADMINISTRATIVE SCIENCES

THE CRIMINAL-LAW PROTECTION OF PUBLIC RELATIONS IN THE FIELD OF FORMATION OF INFORMATION RESOURCE

Khrystyna VOROBETS[1]

Abstract

The article is devoted to analyse the criminal-law protection of public relations in the field of formation of information resource. The important areas of development of Ukraine in the current context of globalization is integration into the global and European information space, development and implementation in all aspects of life information and communication technologies. On the one hand, the rapid development of information and communication technologies at the beginning of XXI century leds to the emergence of a number of new threats to global and national development, which significantly increases the requirements for the national security of Ukraine and leads to new tasks and functions of the Ukrainian state and its legal system. After the proclamation of Ukrainian independence, the conditions of the formation of the information society becomes the state–legal provision of information security. On the other hand, globalization, high dynamics, latency, spontaneity, and growing threats in the information sphere significantly complicate activity and limit the state's ability to provide information security. State-legal information security processes in Ukraine provide transformation of the state, legal and information spheres, including administrative and judicial reform, law enforcement, national security system and so on. Special attention in the article is paid to the fact that informatization as the purposeful activity of the state consists of political, economic, technical and other conditions for information development of subjects, development of the state information resource and optimization of information exchange through wide use of information technologies.

Keywords:

---

[1] PhD student of the Department of public law, Faculty of Law, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine, e-mail: k.vorobets@chnu.edu.ua , phone: +380660923743

Information resource, public relations, informatization, criminal-legal prohibitions, information security.

Introduction

As the data stored in the computer has increased, Information Security has become correspondingly important. In the past, most corporate assets were «hard» or physical: factories, buildings, land, raw materials, etc. Today much more assets are computer-stored information such as customer lists, proprietary formulas, marketing and sales information, and financial data. The main content of the provision of information security in the field of human rights and freedoms is the prevention of the disclosure of information with restricted access, unlawful restriction of freedom of speech and access of citizens to public information and other rights and freedoms that belong to the information sphere [1: 8–11].

The current state, significance and prospects of the development of the information space, unreasonable hopes for the effectiveness of self-regulation of the Internet and other global information networks prove the need for enough public influence in the information sphere at the national and international levels, especially with regard to information security. This need is further enhanced by the latest issues of information security – the protection of state information sovereignty, security in the cybernetic sector, in particular the fight against cybercrime and cyberterrorism and the protection of the state's cybernetic infrastructure.

Theoretical background

Separate issues of criminal legal protection of information public relations were considered by a number of Ukrainian and foreign scientists, in particular: D.Azarov, P. Andrushko, P.Berzin, V. Vyhov, V.D. Gavlovsky, M. Gutsalyuk, S. Dreomov, D.Kalmykov, V. Krylov, O.Krasnenkova, T. Mikhailina, A.Music, A. Nersesyan, S.Orlov, M. Panov, M. Plugatyr, O.Radutny, M. Rudik, N. Savinova, K. Skoronikov.

The scientists, which focused their attention on administrative protection of information security are: I.Aristov, K. Belyakov, B. Kormich, G. Krasnostun, A. Loginov, N. Novitskaya; criminal law protection – D. Azarov, V. Butuzov, N. Rozenfeld; information Law – O. Baranov, I. Bachilo, V. Gavlovsky, M. Gutsalyuk, R. Kalyuzhnyj, A. Maruschak, V.

Tsymbalyuk; Criminologists – A. Belousov, L. Borisov, D. Pashnev; civil law – V. Dmitrishin, A. Kolisnik, M. Selivanov. In special legal studies, information security in the context of national security was interpreted by V. Bilous, V. Gorbulin, O. Danilian, A. Dzoban, I. Ivashchenko, V. Lipkan, N. Nizhnik, G. Novytsky, M. Panov, V. Sidak, G. Sitnik.

Moreover, there are fundamentally new problems, which are appeared nowadays, connecting with the globalization of information processes: protection of the rights of individuals in the automated processing of personal data, state information sovereignty, excessive commercialization of the information space and the danger of manipulation of consciousness, which make the relevance of this study.

Argument of the paper

There is no doubt that information public relations are developing rapidly and their quantitative characteristics are constantly increasing. Informatization and computerization led to an increase in the amount of valuable information that is processed in automated systems. From the quality, reliability and efficiency of this information depends the most important decisions that are taken at different levels – from the head of state to the citizen [2: 3].

It is worth to admit that in the criminal legal discourse the notion of «information security» is predominantly used in an extremely narrow sense: as protection from the leak of information about state secrets.

E.M. Kislyuk and VI Pavlikovsky, during the analysis of the crime of state treason define that threats of the national (including state) security of Ukraine in the information sphere should be understood as the leak of information about state secrets [3: 31]. Similar positions are expressed in the works of other authors.

Obviously, this situation does not correspond to the social tendencies of informatization in the legal regulation and protection of social relations. As L. Schubert correctly notes: «The scientific knowledge of a certain social phenomenon, generalized in the concept, lies in the fact that science tries to clarify the concept in such a way that its content corresponds to this historical situation» [4: 11].

As possible threats in the field of information security are not limited by the leak of information constituting state secrets, criminal law, as a normative framework for the protection of public relations from criminal encroachments, should not consider information security so narrowly.

Quite interesting is the study of how the concept of «information security» in other normative legal acts is understood. Thus, the Law of Ukraine «On the Concept of the National Program of Informatization» of February 4, 1998 states that information security is an integral part of political, economic, defense and other components of national security. This law defines the next objects of information security: information resources, channels of information exchange and telecommunications, mechanisms for ensuring the functioning of telecommunication systems and networks and other elements of the country's information infrastructure. Thus, «information security» in this normative act means as a complex of measures aimed at ensuring the protection of information from unlawful leakage, distortion, destruction, etc.

The most impornant problems of informing are in the next areas: 1) high-quality information provision of state bodies and officials; 2) effective dissemination of legal information as an organizational basis in important areas of social relations, in particular in the field of information security; 3) providing timely, complete, unbiased information about the activities of state bodies; 4) objective and operational coverage of state and world events.

The specifics of the criminal and legal prohibitions are due to the peculiarities of the social significance of information relations and, as a consequence, the peculiarities of the nature of the social danger of encroachments on these relations. Information security is a relationship, where information needs is provided. This appreciation is carried out by obtaining access to the necessary information and based on the use of information technologies, which provided by the formation of an information resource. On the whole, the social significance of the investigated component of information security lies in the fact that the possibility of realizing the information needs is provided through the functioning of the social relations of the formation of information resources [3: 43].

That's why, the specificity of encroachments on information security in the this sphere is that certain socially dangerous consequences come from the fact that the subject receives an information resource that does not allow to solve the tasks effectively. Also it leads to situation, when the subject could committee certain negative actions. For example, the danger of public appeals for the overthrow of the constitutional order (Article 109 of the Criminal Code) is that certain subjects of public life, who need social and political information about the possibilities of the country's development will be misleading as to the appropriateness of the solution urgent social

problems through violence. In turn, the presence of a significant number of such entities will pose a threat to the national security of the country [5].

The determining component of the information sphere is information relations which expess the existing communicative links of society to the implementation of existing information needs. These needs are aimed at obtaining unimpeded access to information resources, obtaining quality information services, and ensuring the proper protection of information.

Information legal relations are kind of legal relations, because they consist on subject, object and content. However, information relations are the special kind of relations that arise, change and cease during the implementation of the regulated norm of the right of information activity. Violation of the procedure of information activity is the basis for the emergence and occurrence of legal liability, including criminal liability [6: 61–64].

The social need for legal protection of these relations is actualized by the presence of such negative social tendencies: 1) excessive capitalization of information space; 2) the danger of anti-democratic development through manipulation of public consciousness in the political sphere; 3) an increase in the level of ideological vulnerability of political systems through the potential of deep social conflicts that can be exploited through the use of information technologies; 4) the danger of systemic violations of the right for private life and total control of personality through the creation of super-powerful personal data bases.

Analysis of the above set of laws on criminal liability by the method of contextual assessment of the public danger of the act suggests that the current Criminal Code of Ukraine contains the consistent assessments of the public danger of criminal encroachment in the formation of information resources. At the same time, it is necessary to pay attention to a number of controversial provisions.

Arguments to support the thesis

The danger of violations in the area of information resource formation is multifaceted and includes different factors. To elucidate the nature of socially dangerous consequences of violations of information security in the investigated sphere is possible by analyzing the threats

provided by the Doctrine of Information Security of Ukraine. Thus, the socially dangerous consequences of encroachments in the sphere of information resource should be attributed: harm to the national interests of Ukraine caused by the dissemination of distorted, inaccurate and prejudiced information and changes in the national public consciousness caused by exogenous negative informational influences through mass media in the global information space.

Dangers for the domestic political sphere are manipulations with social and individual consciousness and manifestations of restrictions on freedom of speech. In the military sphere, the socially dangerous consequences of violations of information security may be manifested in the weakening of the readiness of the Ukrainian population, including image of military service. State security violations in the area of information resource, in accordance with the Doctrine of Information Security of Ukraine threaten to undermine the constitutional order, sovereignty, territorial integrity and inviolability of the borders of Ukraine, as well as the strengthening of separate sentiments in society. The danger of encroachments related to the formation of an information resource is the dissemination of unusual Ukrainian cultural traditions of values and lifestyles, the cult of violence, cruelty, pornography, disdainful attitude to human and national dignity; displacement from the information space Ukrainian artistic works and folk traditions [6: 61–64].

A key feature of modern processes of information formation is the commercialization of information space.

Activities in the field of providing information is considered today is not just a business. It is believed that the media market provides an impartial, invisible mechanism for the free exchange of ideas in society. Market competition here is understood as freedom from state interference and, accordingly, as a way of ensuring the rights of individuals to free information exchange without external interference [7: 9].

Supporters of exclusively market mechanisms consider the function of mass communication as a two-way process. Its essence consists, on the one hand, in the provision of programs for the audience, and on the other hand, to provide the audience with advertisers. The availability of commercial media supports the availability of competition, which creates conditions for the free and independent choice of the individual consumer of information [8: 11-21].

The problem of impossibility of effective self-regulation of the information sphere can be formulated as follows: through the capitalization

of the activities of mass communication entities, the public information resource is usually formed at the expense of information that potentially can increase the range of consumers of specific mass media. Therefore the tendency for monopolization is typical for the modern sphere of mass media.

The consequence of such a restriction is the significant negative changes in the public consciousness. First, the number of cultural and educational programs is decreasing. Secondly, they become mundane. Most of them ignore the norms of morality and human rights. This trend extends even in analytical programs.

Arguments to argue the thesis

It is important to note that Internet-content is filled with different kind of information, but it's doesn't mean that all types of information are the subject of criminal protection. It's connected only with the information about personal data, for example Article 182 «Violation of privacy», Article 159 «Violation of the secrecy of voting», Article 163 «Violation of the secrecy of correspondence, telephone conversations, telegraph or other correspondence, transmitted by means of communication or through a computer, and national security», Article 362 «Unauthorized actions with information that is processed in computers, automated systems, computer networks or stored on the carriers of such information, committed by a person who has the right to access it», Article 363 «Violation of the rules of operation automated electronic computing systems», Part 3, Article 190 («fraud committed by illegal operations using electronic computers») [5].

There is no doubt that cybersecurity has become a national imperative and a government priority. Increased cybersecurity will help protect consumers and businesses, ensure the availability of critical infrastructures on which our economy depends, and strengthen national security. However, cybersecurity efforts must be carefully tailored in order to preserve privacy, liberty and innovation [9: 45].

To design an effective and balanced cybersecurity strategy, each part of the country's critical infrastructure must be considered separately. Solutions that may be appropriate for the power grid or financial networks may not be suitable for securing the public portions of the Internet that constitute the very architecture for free speech essential to our democracy.

Policy toward government systems can be much more prescriptive than policy toward private systems. The characteristics that have made the Internet such a success – its openness, its decentralized and user–controlled nature, and its support for innovation and free expression – may be put at risk if heavy-handed policies are enacted that apply uniformly to any and all infrastructure that may be considered «critical». Some cybersecurity proposals take a «one-size-fits-all» approach that ignores these nuances.

Dismantling the arguments against

The Internet has a significant impact on all areas of human activity and increases the opportunities for communication. Information becomes the social regulator, which ensures the stability of society and forms the direction of its development.

The main objective of legal regulation in the conditions of the formation of an information society is the construction of an effective mechanism for the implementation of information rights and freedoms; provision of such a level of regulation and protection of information relations that would maximally ensure their qualitative functioning [1: 3-5].

That' why, one of the most important components of such a mechanism is the criminal law protection of information security, from which depends the realization of information rights and freedoms.

Conclusions

The Internet has not fundamentally changed the nature of freedom of opinion and expression or the limits of its protection. Freedom of expression is an inalienable catalyst for the implementation of a number of other human rights. However, as the Internet is increasing human rights violations and increasing their potential harm, the legislation and practice of restrictions should be developed accordingly.

This need is further enhanced by the latest information security issues – the protection of state information sovereignty, security in the cybernetic sector, in particular the fight against cybercrime and cyberterrorism, the protection of critical cybernetic infrastructure of the state and others.

The provision of information technology (technology) security includes the creation of opportunities for the secure formation and development of information resources; timely detection of threats of state's security and effective counteraction to them through technical means.

Informatization as the purposeful activity of the state consists of political, economic, technical and other conditions for development of the state information resource and optimization of information exchange through wide use of information technologies.

References

[1]. Karchevs′kyy MV. Kryminal′no-pravova okhorona informatsiynoyi bezpeky Ukrayiny: Monohrafiya. Luhans′k: Ministerstvo vnutrishnikh sprav Ukrayiny, Luhans′kyy derzhavnyy universytet vnutrishnikh sprav im. E. O. Dydorenka; 2012.

[2]. Shubert L. Pro suspil′nu nebezpeku kryminal′noho diyannya. Moskva: MA Gelfer; 1960.

[3]. Bailov AV, Vasiliev OA, Rabbit OO. Kharkiv. Kryminal′ne pravo Ukrayiny. (Osoblyva chastyna). Kharkiv; 2011.

[4]. Yudin OK. Informatsiyna bezpeka derzhavy: navchal′nyy posibnyk. Kharkiv: Konsum; 2005.

[5]. The Criminal Code of Ukraine. Law No. 2341–III fom 2001 Apr. 05 [accessed 2018 May 17]. Available from: http://zakon5.rada.gov.ua/laws/show/2341–14.

[6]. Tuharova O.K. Kryminal′no-pravove zabezpechennya okhorony informatsiynykh vidnosyn. Naukovyy visnyk Khersons′koho derzhavnoho universytetu: zbirnyk naukovykh prats′. Seriya «Yurydychni nauky». 2015; 3 (4): 61-4.

[7]. Shtihve R. To the Genesis of World Society. Innovations and Mechanisms [accessed 2018 May 17]. Available from: http://www.soc.pu.ru:8101/ publications/jssa/1999/3/5stichw.html.

[8]. Nazarov MM. Zasoby masovoyi komunikatsiyi i rosiys′ke suspil′stvo na porozi XXI stolittya. Kyyiv: Sotsial′no-humanitarni znannya; 1999.

[9]. Mel′nyk MI. Naukovo-praktychnyy komentar do Kryminal′noho kodeksu. Kharkiv: Faktor; 2011.