Studia Sieci Uniwersytetów Pogranicza | 2019 | 3
DOI: 10.15290/sup.2019.03.13

Rimma Klyuchko
- e-mail: klrn.grodno@tut.by
- Yanka Kupala State University of Grodno
- ORCID: 0000-0002-1838-5995

PUBLIC DANGER AS A SIGN OF A CRIMINAL INFORMATIONAL ACT

Abstract

- *Goal* – to reveal the signs of public danger during informational actions and inactions.
- *Research methodology* – during the research process, methods of system-legal and formal-legal analysis were used. These methods allowed us to provide an analysis of the existing criminal legislation of the Republic of Belarus and develop proposals for its improvement.
- *Score/results* – the public danger signs of a criminal information act are stated. A criminal informational act is defined as a socially dangerous action or inaction related to the search, receipt, transmission, collection, processing, accumulation, storage, distribution, provision, or use of information, prohibited under threat of criminal punishment.
- *Originality/value* – for the first time, an informational act (action or inaction) is considered a type of criminal encroachment and the criteria for its criminalization are determined.

Key words: criminal informational act, public danger, informational danger, informational security, information, criminal law prohibition, criminalization of informational acts.

1. Introduction

The article examines the signs of social danger of informational acts (actions or inactions), which ultimately lead to its criminalization. A criminal

informational act is defined as a socially dangerous act, or its omission, that is prohibited under threat of criminal punishment. These acts can be related to the search, receipt, transmission, collection, processing, accumulation, storage, distribution, provision, and use of information. Proposals are formulated to supplement the concept of "risk-challenge-threat" in informational legislation with the category "danger" to determine the scope of criminal law protection. To distinguish the signs of public danger in an informational act, it is important to understand the danger of harming the interests of informational relations subjects through the commission of an informational act. Establishing a link between the information characteristics and the public danger of its use is important for determining the boundaries of informational act criminalization. It is concluded that under the threat of criminal punishment, an informational act related to the circulation of information is prohibited, but the information itself cannot be characterized as dangerous, harmful (malicious), illegal, or prohibited. A certain act can only be considered dangerous, harmful, illegal, or prohibited if it uses that information.

2. Criminal informational act

The transformation of our society into an informational society creates new risks, challenges, and threats that directly affect the issues of ensuring national security, informational space security, informational infrastructure, as well as informational systems and resources [Postanovlenie Soveta…]. Russian scholars T.A. Polyakova, A.V. Minbaleev, and I.S. Bojchenko indicate that in an era of transformation of law, the formed triad of subjects (which are the most important subjects in the field of informational security) – individuals, society, and the state – are experiencing the consequences of digitalization processes that require solving problems in the informational security field using multidisciplinary approaches [Polyakova, Minbaleev, Bojchenko, 2019: 66]. Every branch of law has its depth of penetration into the types of social relations [Bachilo, Lopatin, Fedotov, 2005: 18].

Informational law is a regulator of the state policy in the informational security field, however, a special "depth" of penetration into informational relations, regarding its protection from socially dangerous encroachments, is provided by criminal legal means that establish criminality and punishability of informational acts.

A criminal informational act is a socially dangerous action or inaction related to the search, receipt, transfer, collection, processing, accumulation, storage, dissemination, provision, or use of information prohibited under threat of criminal punishment. The emergence of risks and challenges in the informational sphere can be prevented through the use of administrative and legal regulatory mechanisms that avoid or minimize them; threats must be neutralized by legal means, including criminally legal means.

Causing or threatening to cause substantial harm to the interests of an individual, society, or the state is an objective property of a criminal assault and is considered public danger. The addition of the category "danger" to the conceptual series "risk–challenge–threat" in informational legislation is aimed at creating a system of legal mechanisms to counteract these phenomena by taking into account the harmfulness of the informational act or its public danger. It is the presence of public danger that is a material sign of any crime. A crime against informational security is characterized as a public danger because of informational impact, interaction of informational relations subjects or their impact on information, and also crime against informational security is characterized by special target of crime – informational resources. In our opinion, in the structure of the sign of public danger it is possible to single out the information danger as a special sign of the public danger of the informational act. As danger of information we can understand the danger of harming the interests of informational relations subjects by committing an informational act. Informational danger can be considered the legal antipode of informational security.

Commission of a crime against informational security significantly violate the order of interaction between the subjects of informational relations, which leads to socially dangerous consequences (or the threat of them) in the form of significant harm to the interests of the individual or the state or public interests. O.S. Makarov and A.L. Bankovsky defined a number of prohibitions that require an assessment of the public danger and included a criteria for their criminalization, taking into account the general grounds for establishing criminal law prohibitions. Scholars note that "a lot of norms regarding responsibility for committing acts in the informational sphere are not provided with positive norms that determine the rules of behavior, including prohibitions … so far, counteraction to destructive informational impact has not received normative legal fixation".

In order to protect the interests of informational relations subjects, it is necessary to ensure the criminalization of socially dangerous informational acts, which should not entail a violation of the logical order and system of criminal

law. They should also not infringe on criminal legal norms by using norms of regulatory branches of law. The determination or revision of socially dangerous acts that cause significant harm or pose a threat of causing substantial harm to the rights, freedoms, and interests of informational relations subjects is of paramount importance for addressing the criminalization of informational acts, as well as improving existing criminal legislation

.

Crimes against informational security significantly violate the order of interaction between the subjects of informational relations, which leads to socially dangerous consequences (or the threat of them) in the form of significant harm to the interests of the individual or the state or public interests. O.S. Makarov and A.L. Bankovsky defined a number of prohibitions that require an assessment of the public danger and included a criteria for their criminalization, taking into account the general grounds for establishing criminal law prohibitions. Scholars note that "a lot of norms regarding responsibility for committing acts in the informational sphere are not provided with positive norms that determine the rules of behaviour, including prohibitions… so far, counteraction to destructive informational impact has not received normative legal fixation" [Makarov, Bankovskij, 2020].

In order to protect the interests of informational relations subjects, it is necessary to ensure the criminalization of socially dangerous informational acts, which should not entail a violation of the logical order and system of criminal law. They should also not infringe on criminal legal norms by using norms of regulatory branches of law. The determination or revision of socially dangerous acts that cause significant harm or pose a threat of causing substantial harm to the rights, freedoms, and interests of informational relations subjects is of paramount importance for addressing the criminalization of informational acts, as well as improving existing criminal legislation.

3. Characteristics of information and public danger

From the point of view of criminal law, informational interactions implemented within the framework of informational relations involve an interaction using information as a means of communication between informational relations subjects. Based on the above, it is more appropriate to determine the criminal law category of "information" not through an attributive or objective approach, but through a functional cybernetic definition, where the concept of information is

associated with a person (subject), including his technogenic habitat [see more: Sedyakin, Kornyushko, Filoretova, 2012: 180; Sedyakin, 2009: 25–131]. Norbet Wiener was absolutely right when he defined information as having a content of relations and accordingly related it to relative categories [Wiener, 1983].

Establishing a connection between the characteristics of information and the social danger of an act is important for determining the boundaries of the criminalization of informational acts (actions or inactions). The identification and systematization of the features that characterize information as a legal category are important for constructing a mechanism for legal regulation and legal protection of informational relations. Regulatory acts of various industries are abound with assorted characteristics of information that affect the mode of its use (turnover). Thus, the Concept of Information Security of the Republic of Belarus [Postanovlenie Soveta…] uses the following characteristics of information that affect the mode of its use: prohibited (article 40), prohibited by law (article 56), unreliable (articles 40, 45), falsified (40), and illegal (articles 45, 55). The following characteristics are also used in the Concept with regard to information: timely, complete, reliable, generally available, personal, confidential, containing state secrets, limited distribution, official, secret, documented, protected, and mass. We have listed only adjectives used in relation to the category of "information" in the indicated normative legal act, but this list is not exhaustive (it follows the system of interpretation of the Concept). But even this list makes it possible to talk about the absence of a general system of characteristics, which is important for creating a complete and consistent legal mechanism for regulating and protecting information relations.

A criminal law prohibition protects not only information, but also information relations. Under the threat of criminal punishment, a socially dangerous informational act is prohibited if the information is circulated, however, the information itself cannot be characterized as socially dangerous, harmful (malicious), prohibited, or illegal. Socially dangerous, harmful (malicious), illegal, and prohibited can only describe a certain act that uses the information. For example, information about narcotic drugs used during anesthesia, which may be contained in clinical protocols and provided by clinical personnel, does not constitute a public danger, but disseminating that information for non-medical drug purposes may be a public danger. Inaction in the form of not reporting information that can be a danger to people's lives is socially dangerous (article 308 of the *Criminal Code of the Republic of Belarus*), but reporting the same information about an objectively existing danger is a socially useful act, and a deliberately false message about

the danger is recognized as a crime (article 340 *Criminal Code of the Republic of Belarus*) (see also, for example, article 268 "Concealment or deliberate distortion of information on environmental pollution" and art. 324 "Threat of the dangerous use of radioactive materials" of the *Criminal Code of the Republic of Belarus*). Thus, information about narcotic drugs and information about danger by itself cannot be harmful, injurious, or socially dangerous. Public danger can be represented only by acts committed in relation to particular information or with its use, while the presence or absence of social danger is affected by a combination of signs characterizing the content of the information, the acts committed with its use, and the motives and goals of an individual. The systematization of signs that characterize information are important for determining the range of acts that constitute informational danger, and is a prerequisite for systematizing the norms of legislation regulating and protecting information relations and, in particular, ensuring the informational security of individuals, society, and the state.

4. Conclusions

The subjects of information relations should be protected from socially dangerous attacks and be in a state of informational security. Their safety is ensured through regulation and protection (security) by legal and technical means. A.P. Kuznecov points out that "the real effectiveness of informational relations depends on how much they will be provided with legal protection in general and criminal law protection in particular" [Kuznecov 2007: 168]. Criminal legal remedies for protecting such relations are the last "argument" in the mechanism of its legal protection. The emergence of new opportunities for the use of information in the context of informatization process development entails the need to identify new types of socially dangerous information acts by taking into account the challenges, risks, threats, and dangers in the information sphere. There is also a need to determine the criteria for the criminalization of information acts using the existing conceptual framework of criminal and information law and criminological forecasting capabilities. A comprehensive approach to conducting informational-legal, criminal-legal, and criminological studies of risks, challenges, threats, and dangers in the information sphere is necessary to ensure the systematization and improvement of legislation, and the elimination of gaps in the legislation in order to increase the effectiveness of protecting the interests of information relations subjects.

References

Bachilo I.L., Lopatin V.N., Fedotov M.A., 2005, *Informacionnoe pravo*, Sankt-Peterburg || Бачило И.Л., Лопатин В.Н., Федотов М.А., 2005, *Информационное право*, Санкт-Петербург.

Kuznecov A.P., 2007, *Pravovoe obespechenie informacionnykh otnoshenij v Rossii*, "Biznes v zakone", No. 2, p. 165–168 || Кузнецов А.П., 2007, *Правовое обеспечение информационных отношений в России*, «Бизнес в законе», № 2, с. 165–168.

Makarov O.S., Bankovskij A.L., 2018, *Konceptualnyje napravlenija pravovogo regulirovaniya v sfere informacionnoj bezopasnosti Respubliki Belarus* || Макаров О.С., Баньковский А.Л., 2018, *Концептуальные направления правового регулирования в сфере информационной безопасности Республики Беларусь*, [electronic resource] https://etalonline.by/document/?regnum=u01900734&q_id=1241411 [date of access: 23.02.2020].

Polyakova T.A., Minbaleev A.V., Bojchenko I.S., 2019, *Konceptualnyje podkhody k pravovomu regulirovaniyu informacionnoj bezopasnosti v usloviyakh cifrovizacii i transformacii prava*, "Vestnik UrFO", No. 3 (33), p. 64–68 || Полякова Т.А., Минбалеев А.В., Бойченко И.С., 2019, *Концептуальные подходы к правовому регулированию информационной безопасности в условиях цифровизации и трансформации права*, «Вестник УрФО», № 3 (33), с. 64–68.

Postanovlenie Soveta Bezopasnosti Respubliki Belarus ot 18 marta 2019 g. No. 1 "O Koncepcii informacionnoj bezopasnosti Respubliki Belarus" || Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О концепции информационной безопасности Республики Беларусь», [electronic resource] https://etalonline.by/document/?regnum=p219s0001&q_id=630020 [date of access 5.03.2020].

Sedyakin V.P., 2009, *Informaciya i znaniya*, "Nauchnye vedomosti", No. 8 (63), p. 180–187 || Седякин В.П., 2009, *Информация и знания*, «Научные ведомости», № 8 (63), с. 180–187.

Sedyakin V.P., Kornyushko V.F., Filoretova O.A., 2012, *Problema L. Floridi i klassifikaciya informacionnykh nauk*, "Prikladnaya informatika", No. 3, p. 125–131 || Седякин В.П., Корнюшко В.Ф., Филоретова О.А., 2012, *Проблема Л. Флориди и классификация информационных наук*, «Прикладная иинформатика», № 3, с. 125–131.

Wiener N., 1983, *Kibernetika, ili upravlenie i svyaz v zhivotnom i mashine*, 2nd ed., Moskva || Винер Н., 1983, *Кибернетика, или управление и связь в животном и машине*, 2-е изд., Москва.