Security At Information Culture: Wouldn't We Lose Humanity?

Olena Prudnikova

Doctor of Philosophical Sciences, Assistant Professor,
Yaroslav Mudryi National Law University
(Kharkiv, Ukraine)
E-mail: elenvikprud@ukr.net
ORCID: 0000-0003-4610-908X

Oleksii Kuznietsov

PhD student, National Pedagogical Dragomanov University
(Kyiv, Ukraine)
E-mail: helendereka@ukr.net
ORCID: 0000-0001-9242-0835

The question of informational culture as a semiotic space of functioning and interaction with the information and ethics and communication complex regulating this activity is an urgent need in modern humanities and other related branches of knowledge and socioculture. The study of information security at the psycho-motivational, functional and value level gives a relatively complete spectrum of the mentioned problem in view of its cultural influence. Without such an integrated approach to understanding the essence of information culture, mankind faces a catastrophe in the form of loss of democracy, sociality and humanity. The proposed research actualizes the need for a socio-philosophical reflection of the problems of the boundary between information freedom and information security as one of the key issues of the civilization progress of modern civilization.

Keywords: informational culture, information security, operability, functionality, humanity

Received: February 13, 2018; accepted: April 12, 2018

Philosophy and Cosmology, Volume 21, 2018: 107-115
DOI: 10.29202/phil-cosm/21/11

Introduction

Modern information culture radically changes the way human interaction with the environment, which determines the corresponding transformations both in the middle of society, and in the context of personal identification itself. This is about the formation of the

so-called informational worldview as a holistic view of information, information resources, relevant technologies and the principles of knowledge and activities they make. It is clear that a qualitatively new level of information activity gives humanity some freedom to realize activity, but at the same time creates additional threats and dangers at all levels of social and cultural life.

Therefore, the problem of formation of information culture of an individual, society and humanity as a whole becomes more important and relevant. Especially in view of the speed, quality and efficiency of the processing of information. In addition, the information is indifferent, but the possibilities of its use involve a number of contradictions and abuses. Therefore, it is quite natural to question the formation of information culture in view of the need to address security issues. After all, in the global information flows, the person is not just are protected, but in general there is a tendency to fragmentation and compilation of the concept of personality, in contrast to integrity and assemblage. This tendency is dangerous, first of all, as a threat to the loss of the integrity of the individual, of consciously rational activity and humanity as an example and a value regulating freedom of choice.

Information Culture: From Product Activity to Activity Productivity

The democratic ideals of freedom, equality and fraternity find a new imprint in the virtual space of information culture, which is essentially personalized and anonymous. There is an essential contradiction: on the one hand, external barriers and obstacles to freedom are overcome, and on the other hand, absolute freedom reduces responsibility. And a situation arises when the information space has a destructive effect on the person: from psycho-emotional trolling to political manipulation and financial fraud. This space of freedom provokes essential changes in the motivational sphere of a modern person, in particular, creates and reinforces the aspiration for creative self-realization, in contrast to the technical and schematic activities. That is why the notion of an expert in the modern information space is offset: after all, everyone who wants, not just knowledgeable and experienced, strives to share his thoughts. In the chaos of statements and pluralism of evaluations and impressions, the issue of awareness, the reliability of information, its ability to effectively serve is crucial to survival, not only organizations and institutions, but also human beings as biological beings. Numerous armed confrontations in the modern world, accompanied by massive information attacks, are a striking example of this.

The fact is that in the concept of information there is an indication of integrity, the principle of integration and integration (‘information’ consists of two parts ‘in’, that is, ‘in’, and ‘formation’ − formation, that is, ‘something’). That is, the information, in essence, reflects the structural principle of the organization and operation of the system. Logically, any manipulative effect in the information space is associated with disorientation, with the destruction of integrity. So, let us consider the main theoretical and methodological approaches of security policy analytics in different accentuations of socio-cultural life.

Information Security in Dimensions of Mentality and Subjectivity

Information influence on consciousness, society and culture is obvious. Therefore, there is considerable interest in the study of the psycho-mental perception of information threats. Thus, in the course of factor analysis, Ding-Long Huang developed a mental structure that describes the most important factors in perceiving information in terms of its operationality and potential threats, namely knowledge, impact, complexity, manageability, capabilities

and awareness (perspective) [Huang et al., 2010]. The authors established the existence of a regression relationship between the threat assessment and the corresponding activity of the subjects for its verification and neutralization, revealing the relativity and contextuality of the perception of virtual threats, which most often indicates lack of awareness of users: "Significant differences were found in the Knowledge factor and in the Newness and Personal Exposure items. Marginal significant differences were found in the Understanding and Ease of Reduction items. Naturally, experienced computer users knew more about threats to Info. Sec, perceived those threats as not so novel, had better understanding of those threats and felt it would be on people's perception of information security were tested, using the types of loss that respondents selected for each threat as independent variables, and the overall danger as dependent variables. There were six options (multiple choice) for each threat: financial loss, exposure of personal information, inconvenience of computer use, waste of time, loss of reputation and loss of data" [Huang et al., 2010: 230].

Proceeding from this position, the question of formation of information culture as a philosophical principle of ethics of communication requires an appropriate educational work. After all, the fundamental contradiction between information as a realm of freedom and the security strategy as a control and restriction is clearly demonstrated by a lack of awareness of these issues. The exchange of information cannot be controlled, edited, restricted. On the other hand, the availability of information is dangerous for many reasons. For example, Chad Anderson articulates this problem as a contradiction between the exchange of information and the need to protect it, by offering a dynamic model for the contextual solution of this problem [Anderson et al., 2017]. This research is based on the following methodological approach: the definition of the priorities of activity, its main and secondary components, the ability to navigate through chaotic information flows, without losing the effectiveness of realizing their own potentials — a universal one that should be contained in the context of any activity [Anderson et al., 2017].

In general, the problem of verifying information on security/hazard requires a thorough research and analysis. Philip Menard, with a group of authors, analyzes the mental-psychological factors of information security, addressing the internal motivation of people, the authors seek to establish a mechanism for assessing information on safety/security: the authors believe that using data and individual referrals to provide a choice for users, managers can to observe their intentions of hazard verification and appropriate effective response [Menard et al., 2017]. It is argued that motivation for fear of information security is not effective. Perhaps the curiosity inherent in man prevails over the instinct of self-preservation, and vice versa, the appeal to a personal strategy of choice and responsibility significantly increases the indicators of security efficiency. From the analysis of the work, we conclude that solving the issue of information security is possible only through personal awareness, interest and responsibility.

From a methodological point of view, I would like to emphasize that most research on information security either contextually motivated or probabilistically determined. As Jens Braband and Hendrik Schäbe rightly point out, most of the theoretical constructions on information security are monotonous and ineffective before the challenges of modern times [Braband & Schäbe, 2016]. This is explained by the involvement in the theories of the probability factor, which reduces the coherence of the system. The key to solving the problem, according to the authors, is to handle IT security as well as systematic security failures. The authors argue that the introduction of information security levels is similar to SIL, and therefore, information security cannot in principle be fragmentary, selective, or

probabilistic [Braband & Schäbe, 2016]. At the same time, there is a point of view, the lack of modern philosophical discourses on information security due to the lack of clear protocols of the necessary activities.

The productivity of this approach is to substantiate the co-evolution of social and technical mechanisms, which enables to accentuate the source of information security through social constructions, rather than operational-rational schemes. Introducing the concept of causation, the author applies a pragmatic approach to information security, the main content of which is algorithmization and protocol information security tangibly to a specific task and the corresponding functional. The author of this approach offers the notion of causal isolation, or non-interference as an ethical principle: "Based on this research, it can be argued that a notion of causal insulation has already been developed that is specific to information. This notion has been termed non-interference" [Pieters, 2011: 329]. This non-interference strategy is an effective principle of regulation of interpersonal and business relations: "By connecting the technical and policy discourses on information security and privacy, this analysis can form the basis for a better understanding of their relations in current and future developments. This holds not only for electronic voting, as shown in the example, but also for public transport payment systems, road pricing, electronic patient records, and many more. In all of these cases, technical perimeters as such are overrun by the many connections needed, but perimeters in terms of causal insulation, running through computers, organizations, buildings, and people, can provide the necessary understanding of how security is constructed, and in the end enable better judgments on what is more secure than what" [Pieters, 2011: 334]. That is why; the question of the functionality of the system in the security plane requires careful study and study, heuristively applying the approaches of modern social philosophy.

System Functionality in Information Security Strategies

Information security, due to its purpose and application, has been updated in the works of a number of researchers of the philosophical problems of informatization. David C. Li, analyzing information security at various levels of the organization, notes that the authors usually distinguish three groups of factors: the importance of information security, measured by its disclosure; the existence of state regulation; the size of the organization and the complexity of the links [Li, 2015: 26]. Developing the opinion of the authors, we note that only the first two variables, the correctness of their interpretation, and the regulation of mechanisms for working with it, have a prevailing importance and a positive influence on the indicators of online security. Characteristics of the same system on the way of implementing information security do not significantly affect, and therefore there are grounds to offer universal recommendations.

For their effective processing, it is necessary to find out the concept of risk in information security and the parameters of their influence on the work of the system or organization, to understand the significance of the risk parameters that is the basis of the operational response to information danger. As a key factor in the analysis, some authors propose an economic factor, namely, the possibility of investing in technological security solutions, the introduction of organizational procedures, and the training and transfer of risk to the management of the organization [Bojanc & Jerman-Blažič, 2013]. This analysis is necessary in the context of implementation and implementation of the security strategy of subjects of any level. After all, information security is directly related to the general context of the economic life of society: "Trends like globalization, higher productivity, and reducing costs make business organizations increasingly dependent on their information systems and

Internet services. A potential attack on information systems and an eventual crash may cause heavy losses relating to data, services, and business operations. Security risks are present in an organization's information system due to technical failures, system vulnerabilities, human failures, fraud, or external events" [Bojanc & Jerman-Blažič, 2013: 25]. Consequently, the economic indicators in the analysis of information-space risks are sufficiently substantiated and in demand. At the same time, the issue of investment in business is inextricably linked with the problem of risks and threats, and their collisions in the information space are no less fierce and more effective than real conflicts. In other words: "The economic approach to managing security-risk assessment and selecting the optimum measure in information security is typically a large project. It implies a thorough analysis and evaluation of the information assets, an analysis of threats attacking information assets, an analysis of the consequences of information-technology failure, an analysis of the probability of a successful attack, and an assessment of the costs and benefits resulting from an investment in information security" [Bojanc & Jerman-Blažič, 2013: 35]. However, a mere recognition is not enough. Necessary systemic analytical concept of possible risks and threats using modern research tools of social philosophy.

This is the concept proposed by Mary Sumner, who implements a correlative-regressive analysis of information security operations, also offering a substantive empirical research base whose analysis allowed for the following conclusion: "For the information security risks that are high-impact and high-probability, organizations should implement a risk pre-paredness strategy, which enables them to safeguard and to mitigate against these risks. In contrast, for low-impact, less-probable risks, information security pre-paredness may not be as critical" [Sumner, 2009: 11]. However, system work and protocol technology in responding to possible threats in the information sphere can significantly change the quality of the system as a whole. An important factor in this activity is the philosophy of management processes and organization, their focus on information security (IS): "The next step is to have managers actively promote the organizations IS measures in their daily interaction with subordinates. This is where a genuine familiarity with IS matters and how they pertain to the organization writ large (as well as the local subsetting) becomes so important. If presentations of IS matters convey a sense that information security is a separate and only intermittently revisited concern, then that is basically what it will become" [Sumner, 2009: 76]. Therefore, it turns out that the systemic nature of managerial activity provides sufficient potential for monitoring the dynamics and flow of information activity of a system or organization. And the role of managers in providing information security is a key, although public practice demonstrates that information security managers are usually perceived as peripheral entities in the overall management system. However, modernity is changing accents. A striking example is the defeat of Hillary Clinton in the 2016 presidential race as a result of the release of her emails.

However, the logical question is: how to combine systematicy and dynamism, or freedom of expression, word and conscience in a democratic society with the need to implement an effective security strategy in the information sphere? Chad Anderson, together with other authors, formulates this issue as an important ideological orientation in the information culture, and the main pathos of the study is the contradiction between the exchange of information and the need for its protection [Anderson et al., 2017]. Indeed, on the one hand, the exchange of information cannot be controlled, edited, restricted, but, on the other hand, the availability of information is dangerous for many reasons. One of these threats is the reason to consider the inherent information entropy, which is perfectly illustrated by the famous game in the 'broken phone'. In the information risk assessment, entropy is associated with

subjectivity, as detailed in the modern researches [Cheng et al., 2017]. Mentioned research is devoted to the assessment of the probability and risk impact on system functionality. The previously proposed technologies of risk definition are rejected by these authors, since they were determined using a fuzzy integrated evaluation method. The introduction of the entropy coefficient provides an opportunity to overcome subjectivity in the examination of information threats, therefore, to measure the degree of risk of the information system, possibly by finding out its entropy trends. These source data are needed to form an effective security strategy.

In addition, by overcoming entropy it is appropriate to consider raising awareness of functors (users, managers, engineers, etc.). Therefore, educational work in the formation of information culture needs comprehensive support and implementation. Several studies have argued that information security awareness techniques such as web-based training materials, context-based learning and in-built learning are productive ways of developing and disseminating the principles of information culture. The complex of efforts aimed at increasing awareness of information security is extremely in demand and little studied at the same time, therefore, some authors devote considerable attention to determining the method of reliability of the information that is the most successful in ensuring security awareness as well as the identification of the most effective methodology of training Information Security Rules [Abawajy, 2014: 239-240]. Consequently, the lack of awareness in the areas of information culture and security emphasizes the need for detailed elaboration and implementation of practical recommendations for their application to interested parties.

One of the important information security strategies is the problem of its excessive volume and excess content. Daniel-Ioan Curiac and Mihai Pachia raise an extremely important task in the context of the present, namely the problem of utilization of information: they call this process ‘controlled data destruction’ [Curiac & Pachia, 2015]. Its purpose is to protect personal data that is no longer needed for future goals and strategies, but the leakage of which may be threatened. Similarly, in the work of organizations there is no longer relevant information, which is a burden for the internal structure, and a potential risk factor and challenges, so the destruction of such information is both the optimization of the information space and the factor of system organization. The scheme proposed by the authors describes a reconstructed life cycle of information that shows its direct relevance to the information society, information states, and information space in general at various stages of this life cycle [Curiac & Pachia, 2015].

Consequently, not only the theoretical and methodological complex of information security issues is a topical problem of the life of society at all its levels, but the practical introduction of regulation and ordering of the relevant activities requires careful attention of the specialists of the respective branches of knowledge and activities, their legal and political support. It is clear that modern social philosophy has a special place in this process, which consists in the development of strategic, even paradigmatic concepts for ensuring the steady progress of humanity in the information society.

Modern Ethical Dimension of the Problem of Information Security

If in matters of information security, we quite rightly raise the question of the responsibility of the involved individuals and legal entities, then naturally the question of morality of one or another action and relations in the field of information culture. Indeed, modern technology is a powerful human challenge in human beings, and information culture and information security are radically updating our anthropological practices and value horizons, as pointed

out in their works by Vadim Rozin [Rozin, 2017]. The anonymity of the information space outlines the broad field of explication of human freedom and forms a fertile field for numerous manipulative practices. Indeed, a new type of society, often outlined by the 'smart' metaphor, appears to be the socio-cultural space for the implementation of the informational effects of negative nature, which poses a threat to human in humans [Voronkova & Kyvliuk, 2017].

For example, Liisa Myyry, together with other authors, investigates the problem of the moral and psychological measurement of information security: they offer a theoretical model that demonstrates the gap between moral considerations that determine the flow of information activity and general perceptions about the values of human life and society [Myyry et al ., 2009]. Their model combines two well-known psychological theories: Kolberg's theory of cognitive moral development and Schwartz's theory of motivational types of values, and the empirical intelligences presented by them give a meaningful context for the elaboration of practical recommendations for improving information security from the personal to the political levels. However, the greatest value of this study is the analysis of the psycho-motivational dimension of activity in the information space, since the spectrum of determinants in this aspect is very broad: from personal ambition and sublimated aggression to conscientious psychology and international politics [Myyry et al., 2009: 131- 133].

In this regard, it is appropriate to recall the original study of Stilianos Vidalis and Zafar Kazmi focusing on the research inquiry on the reverse side of information security; in particular, the level of deception and manipulation is a problem area of this work [Vidalis & Kazmi, 2007]. It is clear that the conflict of interests is an inalienable companion of public life. Moreover, in today's technological and globalized world, information advantage is both a goal and a means of realizing aspirations and beliefs. Therefore, the authors argue that the art of deception is a reliable and cost-effective technique that can provide the necessary security infrastructure of a system of any level of complexity [Vidalis & Kazmi, 2007: 37-38]. Indeed, according to the principle 'warned, therefore, armed', manipulative techniques should not be left out of the attention of the involved persons, but rather, thoroughly investigated and typologized. A fascinating attempt to analyze neuro-programming technologies, which are widespread at the present stage of the formation of the information society, were carried out by Vasyl Fatkhutdinov and Oleg Bazaluk [Fatkhutdinov & Bazaluk, 2018].

At the same time, modern education should also become an instrument for developing the 'immunity' of the personality in relation to potential threats from manipulative mechanisms of influence on the person, which, as a rule, are of a culturally determined nature and are addressed to young people as the most socially active population. Denys Svyrydenko in this regard notes that involving of personality to the processes of academic mobility can contribute to the adoption of a wide range of cultural experiences that, in our case, will promote the development of individual stability in relation to external influences of a destructive nature [Svyrydenko, 2015]. This same researcher develops the above thesis, analyzing the challenges of globalization to the ideological orientations of modern youth, which are actualized by the processes of the establishment of a global information society [Svyrydenko, 2016].

It is the developed and productive information culture of the individual and society as a whole that allows to successfully overcome various challenges and obstacles, to reduce emerging crashes, noise and obstacles, breakages of communication, etc. Information culture produces 'massification' of communication and communication, which leads to an increase in the stress ratio, which is why its function is precisely the regulation and regulation of activity, a certain universal principle. Consequently, we have reason to assert that information

culture is a certain technology of modern modernized society, and its value and significance constant. In addition, a culture of any type is impossible without the carrier — a separate person, because information in a pure (not internationalized) form is axiologically and hermeneutically neutral. It is known that the real integral of culture is man and humanity. After all, culture is a cult of human being, and no semiotic, political or other factors dominate the value and value of man and humanity.

Conclusion

The information society produces a qualitatively new type of culture whose purpose is to prepare a person for life in the information space. Conceptual content of informational culture is, on the one hand, the theoretical and functional aspect of information operations, and on the other hand, the formation of a new ethics and communication complex, which will fix the basic regulations of information security. The ontological gap between the operational-functional stratum of information culture and the corresponding axiological basis contains the immediate threats of human life and society. An illustration of this situation can be imagined by a train moving in an uncertain direction, with an unintended purpose, and does not take into account the current circumstances: the presence of a railroad trail, possible obstacles in the way and the associated consequences.

It is indicative that the philosophical thought about the contemporary issue of information culture and information security is mainly negative and pessimistic. Numerous authors predict anthropological catastrophe, the main consequence of which may be the loss of human in man, or humanity as a principle of social life. If we remove the principle of humanity from a social life, then we obtain the primitive state of "war of all against all" for survival, synonymous with the concept of de-modernization. Sociality requires explication in personality, and if the infospace is anonymous and infinitely free, then the catastrophe is inevitable. That is why the issues of information security and information culture require the attention of researchers, and the mechanisms for ensuring effective demarcation between information freedom and information security should be in the focus of research optics of modern social philosophy.

🕮 References

Abawajy, Jemal. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), 2014: 237-248. DOI: 10.1080/0144929X.2012.708787

Anderson, Chad, Richard L. Baskerville, and Kaul Mala. Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. *Journal of Management Information Systems*, 34(4), 2017: 1082-1112. DOI: 10.1080/07421222.2017.1394063

Bazaluk, Oleg and Denys Svyrydenko. Philosophy of War and Peace: In Search of New European Security Strategy. *Anthropological Measurements of Philosophical Research*, 12, 2017: 89-99.

Bojanc, Rok and Borka Jerman-Blažič. A Quantitative Model for Information-Security Risk Management. *Engineering Management Journal*, 25(2), 2013: 25-37. DOI: 10.1080/10429247.2013.11431972

Braband, Jens and Hendrik Schäbe. Probability and security — pitfalls and chances. *Safety and Reliability*, 36 (1), 2016: 3-12. DOI: 10.1080/09617353.2016.1148920

Cheng, Yuan-Dong, Ji-Dong He, and Fa-Gang Hu. Quantitative risk analysis method of information security-Combining fuzzy comprehensive analysis with information

entropy. *Journal of Discrete Mathematical Sciences and Cryptography*, 20(1), 2017: 149-165. DOI: 10.1080/09720529.2016.1178913

Curiac, Daniel-Ioan and Mihai Pachia. Controlled information destruction: the final frontier in preserving information security for every organisation. *Enterprise Information Systems*, 9(4), 2015: 384-400. DOI: 10.1080/17517575.2013.792397

Fatkhutdinov, Vasyl H. and Oleg Bazaluk. The Importance of the Brain Neuro-Programming Technologies in National and Regional Security Strategies. *Philosophy and Cosmology*, 20, 2018: 74-82. DOI: 10.29202/phil-cosm/20/6

Holmberg, Robert and Mikael Sundström. Leadership and the Psychology of Awareness: Three Theoretical Approaches to Information Security Management. *Organization Management Journal*, 9 (1), 2012:64-77. DOI: 10.1080/15416518.2012.666952

Huang, Ding-Long, Patrick Rau Pei-Luen, and Gavriel Salvendy. Perception of information security. *Behaviour & Information Technology*, 29(3), 2010: 221-232. DOI: 10.1080/01449290701679361

Li, David C. Online Security Performances and Information Security Disclosures. *Journal of Computer Information Systems*, 55(2), 2015: 20-28. DOI: 10.1080/08874417.2015.11645753

Menard, Philip, Gregory J. Bott, and Robert E.Crossler. User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems*, 34(1), 2017: 1203-1230. DOI: https://doi.org/10.1080/07421222.2017.1394083

Myyry, Liisa, Siponen, Mikko, Pahnila, Seppo, Vartiainen, Tero and Anthony Vance. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, 18(2), 2009: 126-139. DOI: 10.1057/ejis.2009.10

Pieters, Wolter. The (Social) Construction of Information Security. *The Information Society*, 27(5), 2011: 326-325. DOI: 10.1080/01972243.2011.607038

Rozin, Vadim M. Technology as a Time Challenge: Study, Concept and Types of Technology. *Philosophy and Cosmology*, 19, 2017: 133-142.

Sumner, Mary. Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. *Information Systems Management*, 26 (1), 2009: 2-12. DOI: 10.1080/10580530802384639

Svyrydenko, Denys. Globalization as a Factor of Academic Mobility Processes Expanding. *Philosophy and Cosmology*. 14, 2015: 221-234.

Svyrydenko, Denys. Plagiarism Challenges at Ukrainian Science and Education. *Studia Warminskie*. 53, 2016: 67-75.

Vidalis, Stilianos and Zafar Kazmi. Security Through Deception. *Information Systems Security*, 16(1), 2007: 34-41. DOI: 10.1080/10658980601051458

Voronkova, Valentina and Olga Kyvliuk. Philosophical Reflection Smart-Society as a New Model of the Information Society and its Impact on the Education of the 21st Century. *Future Human Image*, 7, 2017: 154-162.