Information security problems of communication processes: philosophical analysis

Aydar Kayumov – Nasira Muginova – Yelena Leonova – Vera Sarayeva

DOI: 10.18355/XL.2018.11.01.03

Abstract
In the article, we have analyzed postulates of the main philosophy paradigms – realism and idealism – in the security sphere and demonstrated that existential dilemma of the information security had been determined by such subject matter of information phenomenon as subjectification in the process of the human activity. We state that formation of confidence, mutual understanding, and existence of general values are appeared to be the main problem of communication processes. Treatment of communication as spiritual and moral category enables us to cover problems of information security of communication processes in its human, moral and ethical qualities. In such a context, we have examined an issue of the balance between accessibility of information and information protection as a key option in the process to ensure information security. In the frames of indicated components, we offer potential instruments to tackle the problem of information security of communication processes. Solutions to the mentioned problems and ways of improving the effectiveness of communication processes are of practical interest in the context of further development of information technologies are proposed.
Key words: security philosophy, informational technologies, social communication, realism and idealism paradigms

Introduction

One of the key features of the new society is its specific form of social organization, where the generation, processing, and transmission of information have become the fundamental sources of productivity and power due to the new technological conditions that emerged during the current historical period (Castells, 2003; Grad, Frunza, 2016: 326; Moretti, 2017: 342; Pieters, 2011: 326; Ruby, 2014; Smarandache Vlăduțescu, 2014: 243).

Information technology has dialectically increased individual and social opportunities (Adams, de Moraes, 2016: 161; Crotty, 2017: 147; Palos, Petrovici, 2014: 85); however, these opportunities have also created serious risks in relation to information security (Esposito, 2015: 89; Soomro, Shah, Ahmed, 2016: 215). Although certain methods for ensuring information security were described a long time ago (in the sixth century BCE) by Sun Tzu (McNeilly, 2001), the term 'information security' emerged only in the late twentieth century; nowadays it has many different definitions in both scientific works and regulatory, legal acts (Al Hogail, Mirza, 2014: 1; Peltier, 2016; Von Solms, Van Niekerk, 2013: 97).

Thus, the social and philosophical foundations of information security of communication processes have not been investigated comprehensively. This study aims to solve this problem. The substantial problems of information security were determined based on an in-depth analysis of major scientific theories and a detailed investigation of the distinctive features of modern communication processes, which enabled substantiating the philosophical foundation and setting teleological landmarks for information security management. The research takes a philosophical approach to investigating the essence of information security of communication process.

Security philosophy

It is worth noting that the concept of 'security' is traditionally interpreted within the philosophical paradigm of realism, and, since the mid-twentieth century, within the paradigm of neorealism. According to the classical author of realism, the natural state of an individual, who is a greedy and egoistic creature by nature, is a state of "free-for-all war" (Brown, 1965). In realism and neorealism, power is considered as the main tool for ensuring security, while the balance of power is considered as the main condition that guarantees security. Those who support this paradigm interpret information security mainly as the capability of the state to withstand both internal and external threats in the field of information. Enhancement of state capacities in the field of information and communication technologies, which can be used as an information weapon, information protection through the extension of list of information that is considered classified and confidential, restriction on the spread of information by the channels that are not controlled by the state, and the use of manipulation technologies in the coverage of important political events are considered the main areas of information security assurance. However, in the current conditions, this approach seems too limited.

The philosophical paradigm of idealism is an alternative to realism. The development of this paradigm in Europe is linked with stoicism, the development of Christianity, and the view of I. Kant (1889). This paradigm is based on the notion of moral and political unity of humankind, inherent and natural human rights, and the idea that the interests of a citizen outweigh the interests of the state (Tuck, 1999). The most extensive formulation of the philosophical foundation of security embraced by idealists can be found in the categorical imperative of I. Kant: "Act only according to that maxim whereby you can, at the same time, will that it should become a universal law" (Kant, 1995). One of the central ideas in this paradigm is the idea of cooperation between all elements of the social system, which is based on universal values and common human interests. From this perspective, the participants of social relations, who refuse to cooperate, who breach general moral and legal rules, pose a threat to security.

This research relies on the philosophical foundation of the security theory, which is developed within the abovementioned paradigms. This enabled defining the problem of correlation of power-related and moral stimuli, methods of counteraction and cooperation. Interrelated trends of globalization and informational support prioritize dialog and cooperation as a means of ensuring security, which corresponds with the postulates of idealism.

In terms of the concept of "information security" as part of security in general, it is worth noting that the existential features of information distinguish this element from the other material components of security. 'While the philosophical foundations of information security have been unexamined, there is an implicit philosophy of what protection of information is, - W. Pieters (2015: 326) stresses. - This philosophy is based on the notion of containment, taken from analogies with things that offer physical security (e.g., buildings, safes, fences)'. He argues that this implicit philosophy does not take into account the human nature of information and social aspects of information security problem.

The Phenomenon of Information

Information is regarded as one of the most significant and at the same time mysterious phenomena in the world. Two approaches to this phenomenon – functional and attributive – can be distinguished (Buckland, 2013; Budd, 2011: 56).

Ever since C.E. Shannon and W. Weaver (1949), apologists of the functional approach have focused on the mathematical and technological aspects of information processes (Shannon, 1948: 379). Using this approach, information can be understood

as any useful data, instructions, or meaningful message content. The concept of "information security" is interpreted accordingly by this approach. "Information security is the protection of information and minimises the risk of exposing information to unauthorized parties" (Venter, Eloff, 2003: 299).

The CIA triad is a very important trio in this concept of information security. The CIA stands for Confidentiality (protecting confidentiality deals with keeping things secret), Integrity (integrity deals with making sure things are not changed from their true form), and Availability (the idea here is that nothing is being stolen, and nothing is being modified) (Pilerot, Limberg, 2011: 312). In 2013, based on a thorough analysis of Information Assurance and Security (IAS) literature, the IAS-octave was proposed as an extension of the CIA-triad. The IAS-octave includes Confidentiality, Integrity, Availability, Accountability, Auditability, Authenticity/Trustworthiness, Non-repudiation and Privacy (Cherdantseva & Hilton, 2013).

While criticizing, to a certain extent, the functional approach to investigating the essence of information security, stresses that information security is such a broad discipline that it is easy to get lost in a single area and lose perspective. Each best practice is tied directly to a higher, more philosophical security concept. Therefore, the attributive approach is more effective for the present study. Its supporters begin with the claim that information either constitutes or is closely correlated with what constitutes our existence and the existence of everything around us (Kerschner, 1965: 33). This means that information plays an ontological role in the manner in which the universe operates. According to L. Floridi (2004: 554), information is as fundamental a concept as "life," "knowledge," "good and evil" and is even "more powerful" a concept than the abovementioned ones are. In other words, according to Floridi (Floridi, 2004: 554), these other concepts can be expressed through the concept of information.

However, despite the appeal of ontological "depths" that are offered by the supporters of the attributive approach, this study will rely on the structural and functional concept of the interpretation of "information," since the study focuses on the role of information in the formation and functioning of social structures. In this regard, L. Floridi (2011) emphasizes the key role of the interactions between agents and the environment. Based on the theory that he calls Action-based Semantics (AbS), the philosopher claims that human agents share with other informational agents a reality made of information. He offers to use an informational approach to structural realism, according to which knowledge of the world is knowledge of its structures dynamically interacting with each other.

When considering the category of "information" from the perspective of the activity approach, the assumption is that the phenomenon of information is closely related to the structure of reality and results from the interaction between the material and ideal components that comprise this structure (Kolin, 2010: 29). Thus, the properties of matter, nature, and society are only potential information; they become information only after an individual acquires knowledge thereof (Beni, 2016: 323). It is worth noting that the information as a product of human activity has a dual nature. When obtaining, in the form of information, certain knowledge or data about an object, the subject changes itself and alters the obtained information "as it sees fit," i.e., subjectifies the information. Already at this point, a contradiction emerges between the properties that are actually specific to the object and the information that is perceived by the recipient. Therefore, the investigation of interaction and mutual influence of the information, its cause, its sender, and its recipient is a relevant problem. This problem is of utmost importance for the social and philosophical analysis of information security of communication processes. The objectification of information, as a condition of information security, implies the opportunity of

obtaining information from a variety of diverse sources and the ability to comprehend it critically.

Value communication as a goal and means of information security

This study does not cover the numerous technological models of communication that focus mainly on the technical aspects of media operation and ignore the problems of the social environment and other important factors of interaction between communicators, which are significantly more extensive than the purely technical ones.

From the perspective of social process studies, the model suggested by H. Laswell (1971) is the conceptual model of communication. This model raises five consecutive questions: Who? (Who transfers the information?) Says what? (What is the information?) In which channel? (In which channels is the information transferred?) To whom? (To whom is the information transferred?) With what effect? (What is the effect of this information?) Thus, Laswell's model implies the transfer of information from one actor to another through certain means.

The next step is to present communication as a bilateral process and to investigate the exchange of information. The model of bilateral communication, when the sender and the recipient of information act within their inherent correlation frameworks, the relations established between them, and the social situation they find themselves in was presented as part of the communication concept. This model is based on the fact that communication occurs only in the presence of a zone of intersection of value-conceptual frames of correlation between communicators, i.e., in the presence of a predetermined community and trust in each other, which develops during communication. According to N. Luhmann (1996: 257), meaning-making communication is the essence of the social, since sociality without meaning is impossible a priory. However, N. Luhmann claims that the individual conciseness and the individual him- or herself, as a combination of "mental and organic systems" should be "factored out" of the sociological analysis. This, according to the scientist, is the sociological interpretation of communication.

It is worth noting that such relatively specific questions are more relevant for sociological studies. In terms of social philosophy, which investigates communication as a social phenomenon that covers the entire variety of relationships between people, it is necessary focus on communication as an intercourse, i.e. the implementation of subject-subject relationships and the creation and recreation of community, which was denied by Luhmann (Resaev, Tregubov, 2015: 141). According to A. Kostyrev (2010: 88), communication is not only an exchange of messages but also a process of mutual interpretation of the messages with a view to understanding their cognitive meaning with an obligatory formation of the so-called "feedback loop" in the process. This is important in the context of ensuring information security of communication records since the disruption of the feedback loop actually breaks the communication process. It is also worth noting that according to J. Habermas' (1984) theory of communicative action, the purpose of communication is to establish a consensus – a balance of interests and to distribute the chances symmetrically not only during the discourse but also in all subsequent actions taken by the communicants.

Therefore, this research will hold the view that the effectiveness of communication processes can only be considered from the perspective of changes in the way of thinking and feelings of individuals and the nature of their practical activity. In turn, the comparison of goal and success aspects allows determining the influence factor of the information. If the matter at hand is communication, then it is possible to say that it has been implemented only when the informational process results in the development of mutual understanding and trust required for the interaction of subjects.

In the context of assurance of communication process security, it is important to differentiate information processes by introducing the "goal" indicator into the selection filter. This study emphasizes the fact that the goal of informing is a unilateral transfer of information, the goal of manipulation is a hidden encouragement of the information addressee to take actions that the sender wishes taken and that the goal of communication is mutual understanding. With that, communication is regarded as a process, which is determined by the presence and implies the development of value components, which define communication as a holistic social, spiritual, psychological, and moral phenomenon.

Thus, the value-conceptual and teleological analysis of communication identified a problem of communication process security – the formation of trust and mutual understanding based on common values and goals. In this case, the moral principles of communicators are the "filters" that guarantee "cleanness" of communication channels. Security is a peculiar set of conditions of the subject's existence that he or she is able to control. In turn, information security is a condition when subjects maintain and recreate their values during communication. Thus, the concept of communication is the decisive factor when defining the concept of information security, while the communication process is both the goal and a necessary condition of information security. According to S.A Townley (2005: 163), based on information security philosophy, the organization must provide open communication, allowing any implicit assumptions relating to implementing the policy to be surfaced and discussed. Observing numerous searches, Z.A. Soomro, M.H. Shah and J. Ahmed (2016: 215) make a novel contribution by arguing that a more holistic approach to information security is needed.

Within the framework of such a comprehensive approach, it is expedient to consider information security of communication processes as a set of conditions that provide for unhindered and balanced circulation of information, which is implemented under the value correlation between social actors and the goal of achieving mutual understanding and trust during social interaction.

A standpoint such as this would place communication at the center of concern for social philosophy, and this idea has given rise to the new fields of information security philosophy as human, culture and ethics problems.

Discussions

Holistic value approach makes the human factor a central problem of information security in its wider philosophical definition. This is shown by the study of a number of scientists. E. Metalidou et al. (2014: 424) focus on the relationship of the human factor referred to information security which presents the human weaknesses that may lead to unintentional harm to the organization. Speaking in the same way, S. Mondal (2013) argues that information security is the organizational problem rather than IT problem and social engineering is a major threat. She points out that "human wall is always better than a firewall," and calls "let us build a human wall along with the firewall."

In this context, the development of information security culture becomes a relevant problem. A. Da Veiga and N. Martins (2015: 243) show that a strong information protection culture is necessary to reduce the risk of human behavior to the protection of information as well as to uphold privacy requirements from a regulatory perspective. A. Al Hogail (2015: 567) argues that establishing information security culture in organizations impacts employees' perceptions and security behavior in a way that can guard against many information security threats posed by insiders.

Since the communication process is regarded as the value-oriented informational interaction of social actors; one faces the moral and ethical problem of balance between confidential and public information in the context of information security assurance. According to the Stanford Encyclopedia of Philosophy (2012), the

primary moral values of concern are privacy, ownership, trust and the veracity of the information being communicated. Information security is also an important moral value that impacts the communication and access to user information. H. Tavani and J. Moor (2004) argue that in some cases giving the user more control over the information may actually result in greater loss of privacy. If we grant the control of our information to third parties in exchange for the services they provide, then these entities must also be responsible for restricting the access to that information by others who might use it to harm us (Epstein, 2007; Magnani, 2007; Tavani, 2007).

Internet and social media have forced us to change a simple notion of confidence as a key component of information security into more philosophical dialectic concepts that recognize both the benefits and risks of communication. J. S. Ibucez (2003: 31) reviews the security usage of the Internet focusing on its characteristics: the universality of information, the communicative facilities and the easy access to information; Ibucez (2003: 31) believes that these characteristics are key to information security. H. Nissenbaum (2009) and P. Broderick, (2004: 1) observe that, where previously, physical barriers and inconvenience might have discouraged all but the most tenacious from ferreting out information, technology makes this available at the click of a button or for a few dollars.

Thus, it seems that information technology has a strong dissonance created in the competing values of security and openness based on the competing values of the people designing the technologies themselves. Therefore, social actors who secure their own information and take care of content communication will be increasingly valued as responsible influencers and trusted sources. “If you interact with the Internet - the typical methods of communication today - betray you silently, quietly, invisibly, at every click, - advice E. Snowden. -At every page that you land on, information is being stolen. It is being collected, intercepted, analyzed, and stored by governments, foreign and domestic, and by companies. Sometimes you can’t always keep something secret, but you can plan your response” (Lee, 2015).

Information disclosed by Snowden confirms that the development of the Internet and online networks make relevant the problem of moral responsibility not so much of users as of the social actors that can monitor communication processes (providers) and establish the agenda for public discourse (bloggers). Since the very design capabilities of information technology influence the lives of their users, the moral commitments of the designers of these technologies may dictate the course society will take and our commitments to certain moral values (Brey, 2010; Bynum, 2008; Ess, 2009; Johnson, Powers, 2008; Magnani, 2007; Moor, 2008: 111; Spinello, 2002; Sullins, 2010).

Lies are the enemy of communication. Having told a lie once, the communicator loses the trust and therefore drops out of the communication interaction zone. Developing this aspect, O. I. R. Orduca (2003: 21) asserts that the image is one of the most important aspects of information security. Despite the common but erroneous opinion, truthfulness is one of the main conditions of information security of communication processes.

Ethics conflict in values has been debated by philosophers in the context of hacker’s activism. This problem in the context of Snowden’s case was investigated by *A. Chadwick and S. Collister* (2014: 2420). Investigators introduce the concept of *boundary-drawing power*. They demonstrate that *on the one hand,* the leak’s mediation reveals professional news organizations’ evolving power in an increasingly congested, complex, and polycentric hybrid media system where the number of news actors has radically increased. But on another hand state power and surveillance involved exercising a form of strategic, if still contingent, control over the information and communication environments within which the Snowden story developed.

A very similar value split plays out in other areas as well, particularly in intellectual property rights and pornography and censorship. R. Rivera, D. S. Velasco and V. C. Garcia (2016: 55) show that one unintended consequence of mass media consumption increase is the proliferation of risky consumption, including online and offline pornography. When talking about social networks as a new stage of ICTs development and an important phenomenon of mass cooperation, J. Vivar (2009: 21) also stressed that social networks were not a panacea, furthermore they posed a threat, especially to young users, who often get caught in the toils of child abusers or pornography.

However, attempts to censor the Internet are also counterproductive. At the same time, when investigating the correlation between security and openness of information, C. Hart, D. Y. Jin and A. Feenberg (2014: 2860) agree that the Internet could be more secure, but they stress the importance of cyberspace as an open, global commons of information that has allowed innovation and rapid technological growth. Scientists, therefore, discuss how the cybersecurity issue can be reframed to take into account the importance of this openness instead of viewing it as a vulnerability and seek solutions that do not unduly or disproportionately impact civil liberties. Therefore, it seems that information technology has a strong dissonance created in the competing values of security and openness based on the competing values of the people designing the technologies themselves. However, as A.S. Duff (2004: 69) shows, if freedom of information (FOI) issues are at the core of information policy, so privacy and area of data protection are the other sides of the FOI coin, and official secrecy policy, too, can be seen as a logical extension of FOI.

When considering the problems of information security from the perspective of social philosophy, the assumption is that freedom and security are closely related phenomena, which form the fundamental aspects of social existence, the most important characteristics of social actors. Security assurance as a process of mastering the conditions of existence is also a process of realizing the freedom of the subject. The principle of information openness is regarded in the society as the foundation of democracy; it is a specific (informational) variant of the freedom principle. At the same time, individual freedom implies the integrity of his or her private life and personal information.

The ICTs development makes relevant the problem of information overload, which may obstruct communication channels and even can cause them to burst. For instance, mobile first is the default for 2015 with 4G, optimized websites, apps and device integration each contributing to an ‘always on’ communications environment. With the online world perpetually to hand, the demand is for smart personalization of communications to deliver what people want, when, where and how they want it, without compromise. It takes people to understand people and gain sufficient insight to guide decision-making. However, the promise that ‘big data’ could automate organizational communications has proved a fallacy.

‘Big data’ also raises philosophical problems. As J. Copeland (2014) says, once you have a huge quantity of data, errors in the data will be practically inevitable. It is often not appreciated that it's a theorem of standard deductive logic that if you have a contradiction in your data, then anything and everything can be deduced. Typically today's computers are programmed in accordance with standard deductive logic. So suppose, for example, that a big European surveillance database receives a couple of contradictory weather reports from different sources, and then someone from the military queries the database: “Has Russia launched a nuclear missile?” The database would answer “Yes.” It would answer “Yes” to any question, simply because it contains a contradiction. Just one little contradiction is enough. This phenomenon is called «explosion under contradiction.» At this point, the filters that absorb information according to the value-amount ratio may assist the information filters of critical thinking and moral principles.

The ICTs development raises such social and philosophical problems that we had no idea of even ten years ago. However, even if it is impossible to predict all the possible dangers that modern ICTs bring, it is important to try to anticipate the changes that are likely to emerge soon in the field of information security by investigating current trends from the perspective of social philosophy. J. Moor (2008: 111) argues that moral philosophers need to pay particular attention to emerging technologies and help influence the design of these technologies early on before they adversely affect moral change.

Conclusions

This research is based on the philosophical foundation of the security theory, which is developed in within the framework of the realism and idealism paradigms, which allows defining the problem of correlation of power and moral stimuli, methods of opposition and cooperation. The interrelated trends of globalization and informatization prioritize dialog and cooperation as ways of ensuring security. This concept of security is regarded not as derived from the concept of the individual, group or national interest, but as a result of the development of trust between the actors during effective communication.

The comparison of the functional and attributive approaches to understanding the phenomenon of information found that information as a product of human activity has a dual nature. This means that when obtaining, in the form of information, certain knowledge or data about an object, the subject changes itself and alters the obtained information "as it sees fit," i.e., objectifies the information. Already at this point, a contradiction emerges between the properties that are actually specific to the object and the information that is perceived by the recipient. Therefore, the investigation of interaction and mutual influence of the information, its cause, its sender, and its recipient is a relevant problem. This problem is of utmost importance for the social and philosophical analysis of information security of communication processes. The objectification of information, as a condition of information security, implies the opportunity of obtaining information from a variety of diverse sources and the ability to comprehend it critically.

Thus, information security implies free access to various sources of information from the information environment, but also the protection of personal information databases from unauthorized access. This dilemma of information security brings one to a natural, from the philosophical perspective, conclusion: information protection and information accessibility are in dialectical interaction. In other words, each communication system should have its own level of openness and closeness in order to ensure the security of personal information.

The value-conceptual and teleological analysis of communication as social and philosophical category identified a problem of communication process security – the formation of trust and mutual understanding based on common values and goals. The results of this study are based on the value approach to the security problems in general, and information security in particular, which enabled distinguishing their humanitarian, cultural, moral and ethical aspects. This value approach makes the human factor a central problem of information security in its wider philosophical definition.

Since the communication process is regarded as the value-oriented informational interaction of social actors; one faces the moral and ethical problem of balance between confidential and public information in the context of information security assurance. The primary moral values of concern are privacy, ownership, trust and the veracity of the information being communicated. We argue that information security issue can be reframed to take into account the importance of this openness

instead of viewing it as vulnerability and seek solutions that do not unduly or disproportionately impact civil liberties.

The ICTs development makes relevant the problem of information overload, which may obstruct communication channels and even can cause them to burst. Hence, information security can be figuratively depicted in the form of a valve (nipple). In order to ensure a balanced functioning of the social system under informational overload, this valve should be equipped with a set of filters in the form of critical thinking, moral and ethical attitudes, and an indicator of the value to amount ratio for information.

The scientific and theoretical value of this study is determined by its in-depth social and philosophical analysis of current problems of information security of communication processes. The herein offered solutions to the mentioned problems and ways of improving the effectiveness of communication processes are of practical interest in the context of further development of information technologies.

Bibliographic references

ADAMS, F. – DE MORAES, J. A. 2016. Is There a Philosophy of Information? In: Topoi, vol. 35, n. 1, pp. 161-171.

AL HOGAIL, A. 2015. Design and validation of information security culture framework. In: Computers in Human Behavior, vol. 49, pp. 567-575.

AL HOGAIL, A. – MIRZA, A. 2014. Information security culture: a definition and a literature review. In 2014 World Congress on Computer Applications and Information Systems, pp. 1-7.

BENI, M. D. 2016. Epistemic Informational Structural Realism. In: Minds and Machines, vol. 26, n. 4, pp. 323-339.

BREY, P. 2010. Values in Technology and Disclosive Computer Ethics. In The Cambridge Handbook of Information and Computer Ethics. Cambridge: Cambridge University Press.

BRODERICK, P. B. 2004. On communication and computation. In: Minds and Machines, vol. 14, n. 1, pp. 1-19.

BROWN, K. C. 1965. Hobbes studies. Cambridge: Harvard University Press.

BUCKLAND, M. K. 2013. The philosophy of information. In: Journal of Documentation.

BUDD, J. M. 2011. Meaning, truth, and information: Prolegomena to a theory. In: Journal of Documentation, vol. 67, n. 1, pp. 56-74.

BYNUM, T. 2008. Norbert Wiener and the Rise of Information Ethics. In Information Technology and Moral Philosophy. Cambridge: Cambridge University Press.

CASTELLS, M. 2003. The Power of Identity: The Information Age: Economy, Society, and Culture Volume II. Wiley-Blackwell.

CHADWICK, A. – COLLISTER, S. 2014. Boundary-Drawing Power and the Renewal of Professional News Organizations: The Case of the Guardian and the Edward Snowden NSA Leak. In: International Journal of Communication, vol. 8, pp. 2420-2441.

CHERDANTSEVA, Y. – HILTON, J. 2013. A Reference Model of Information Assurance & Security. Availability, Reliability, and Security (ARES). In Proceeding of the 18th International Conference.

COPELAND, J. 2014. The Philosophy of Information. The Information science Academy.

CROTTY, B. H. 2017. Considerations and Challenges in Information and Communication Technology. In Ethical Considerations and Challenges in Geriatrics. Springer International Publishing, pp. 147-156.

DA VEIGA, A. – MARTINS, N. 2015. Information security culture and information protection culture: A validated assessment instrument. In: Computer Law & Security Review, vol. 31, pp. 243-256.

DUFF, A. S. 2004. The Past, Present, and Future of Information Policy. In: Information, Communication & Society, vol. 7, n. 1, pp. 69-87.
EPSTEIN, R. 2007. The Impact of Computer Security Concerns on Software Development. Internet Security, Hacking, Counterhacking, and Society. Canada: Jones & Bartlett Publisher.
ESPOSITO, E. 2015. Beyond the promise of security: uncertainty as resource. In: Telos, n. 170, pp. 89-107.
ESS, C. 2009. Digital Media Ethics. Massachusetts: Polity Press.
FLORIDI, L. 2004. Open problems in the philosophy of information. In: Metaphilosophy, vol. 35, n. 4, pp. 554-582.
FLORIDI, L. 2011. The Philosophy of Information. Oxford: Oxford University Press.
GRAD, Y. – FRUNZA, S. 2016. Postmodern Ethics and the Reconstruction of Authenticity in Communication-Based Society. In: Revista de Cercetare Si Interventie Sociala, vol. 53, p. 326.
HABERMAS, J. 1984. The Theory of Communicative Action. Boston: Beacon Press.
HART, C. – JIN, D. Y. – FEENBERG, A. 2014. The Insecurity of Innovation: A Critical Analysis of Cybersecurity in the United States. In: International Journal of Communication, vol. 8, pp. 2860-2878.
IBUCEZ, J. S. 2003. Information and learning in Internet. In: Comunicar, vol. 21, pp. 31–38.
Information Technology and Moral Values. 2012. Stanford Encyclopedia of Philosophy. Available online: http://plato.stanford.edu/entries/it-moral-values/
JOHNSON, D. G. – POWERS, T. 2008. Computers and Surrogate Agents. In Information Technology and Moral Philosophy. Cambridge: Cambridge University Press.
KANT, I. 1889. Kant's critique of practical reason and other works on the theory of ethics. Dublin: Fellow and Tutor of Trinity College, Dublin.
KANT, I. 1995. Criticisms of practical mind, wits. St. Petersburg: Science.
KERSCHNER, L. R. 1965. Cybernetics: key of the future? In: Problems of Communism, vol. 14, n. 6, pp. 33-46.
KOLIN, K. K. 2010. Philosophy of information and fundamental problems of modern informatics. In: Alma Mater Herald of Higher School, vol. 1, pp. 29-35.
KOSTYREV, A. G. 2010. Political communication as a way of national consolidation. International conference on Ethno-cultural Diversity and the Problem of Tolerance in the Globalizing World. St. Petersburg, pp. 88-95.
LASWELL, H. 1971. Policy Problems of Data Rich Society. Cambrige: Cambrige University Press.
LEE, M. 2015. Edward Snowden Explains How To Reclaim Your Privacy. In: The Intercept.
LUHMANN, N. 1996. On the Scientific Concept of Communication. In: Social Science Information, vol. 35, n. 2, pp. 257-267.
MAGNANI, L. 2007. Morality in a Technological World: Knowledge as Duty. Cambrige: Cambridge University Press.
MCNEILLY, M. R. 2001. Sun Tzu and the Art of Modern Warfare. New York: Oxford University Press.
METALIDOU, E. – MARINAGI, C. – TRIVELLAS, P. – EBERHAGEN, N. – SKOURLAS, C. – GIANNAKOPOULOS, G. 2014. The Human Factor of Information security: Unintentional Damage Perspective. In: Procedia - Social and Behavioral Sciences, vol. 147, pp. 424-437.
MONDAL, S. 2013. Information security: importance of having defined policy & process. Braindigit 9th National ICT Conference 2013. Technology.
MOOR, J. H. 2008. Why We Need Better Ethics for Emerging Technologies. Ethics and Information Technology, 7(3), 111-119.

MORETTI, G. 2017. Social Organization, Social Tools: Social Media and Organizations in the Context of a Hybrid Culture. Evolution of the Post-Bureaucratic Organization, p. 342.
NISSENBAUM, H. 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press.
ORDUCA, O. I. R. 2003. Communication in crisis times. In: Comunicar, vol. 11, pp. 21-30.
PALOS, R. – PETROVICI, M. C. 2014. Perceived Importance of Communication Skills and their Predictive Value for Academic Performance. In: Revista de Cercetare Şi Intervenţie Socială, n. 46, pp. 85-98.
PELTIER, T. R. 2016. Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC Press.
PIETERS, W. 2011. The (social) construction of information security. In: The Information Society, vol. 27, n. 5, pp. 326-335.
PIETERSE, J. N. 2015. Globalization and culture: Global mélange. Rowman & Littlefield.
PILEROT, O. – LIMBERG, L. 2011. Information sharing as a means to reach a collective understanding: A study of design scholars' information practices. In: Journal of Documentation, vol. 67, n. 2, pp. 312-333.
RESAEV, A. B. – TREGUBOV, N. D. 2015. Communication and intercourse in the system theory of Nicklas Luhmann. In: Sociological Research, vol. 11, pp. 141–152.
RIVERA, R. – VELASCO, D. S. – GARCIA, V. C. 2016. Online and Offline Pornography: Consumption in Colombian Adolescents. In: Comunicar 46: The Internet of the Future, vol. 26, n. 46, pp. 55-68.
RUBY, C. 2014. Social Media and Democratic Revolution. The Impact of New Forms of Communication Democracy.
SHANNON, C. E. 1948. A Mathematical Theory of Communication. In: Bell System Technical Journal, vol. 27, pp. 379-423.
SHANNON, C. E. – WEAVER, W. 1949. The Mathematical Theory of Communication. Illinois: University of Illinois Press.
SMARANDACHE, F. – VLADUŢESCU, Ş. 2014. Towards a Practical Communication Intervention. In: Revista de Cercetare Şi Intervenţie Socială, n. 46, pp. 243-254.
SOOMRO, Z. A. – SHAH, M. H. – AHMED, J. 2016. Information security management needs more holistic approach: A literature review. In: International Journal of Information Management, vol. 36, n. 2, pp. 215-225.
SPINELLO, R. A. 2002. Case Studies in Information Technology Ethics. New York: Prentice Hall.
SULLINS, J. P. 2010. Rights and Computer Ethics. In The Cambridge Handbook of Information and Computer Ethics. Cambridge: Cambridge University Press.
TAVANI, H. – MOOR, J. 2004. Privacy Protection, Control of Information, and Privacy-Enhancing Technologies. Sudsbury: Jones & Bartlett Publishers.
TAVANI, H. T. 2007. The Conceptual and Moral Landscape of Computer Security. In K. E. Himma (Ed.), Internet Security, Hacking, Counterhacking, and Society. Sudbury Massachusetts: Jones and Bartlett Publishers.
TOWNLEY, S. A. 2005. The Philosophy of Enterprise Information Security. In: Information Security Buletin, vol. 10, pp. 163-178.
TUCK, R. 1999. The Rights of War and Peace. In Political Thought and International Order from Grotius to Kant. New York: Oxford University Press.
VENTER, H. S. – ELOFF, J. H. P. 2003. A taxonomy for information security technologies. In: Computers & Security, vol. 22, n. 4, pp. 299-307.
VIVAR, J. M. F. 2009. New Models of Communication, Profiles and Trends in Social Networks. In: Communicar, vol. 17, n. 33, pp. 21-34.
VON SOLMS, R. – VAN NIEKERK, J. 2013. From information security to cyber

security. In: Computers & Security, vol. 38, pp. 97-102.

Words: 6237
Characters: 41 720 (23,72 standard page)

Aydar Kayumov
Head of Socio - Humanities Department
Kazan Federal University
Naberezhniye Chelny
Bulvar Yamasheva Str., 12/5
Russia
ayd.kayumov@gmail.com

Nasira Muginova
Associate Professor of Socio-Humanities Department
Law and Humanities Department
University of Management "TISBI"
Naberezhniye Chelny
Lazurnaya Str., 13
Russia
mhnazira@mail.ru

Yelena Leonova
Associate Professor of Socio-Humanities Department
Law and Humanities Department
University of Management "TISBI"
Naberezhniye Chelny
Syuumbike Ave., 68/367
Russia
zapad29@rambler.ru

Vera Sarayeva
Associate Professor of Socio-Humanities Department
Law and Humanities Department
University of Management "TISBI"
Naberezhniye Chelny
Moscovsky Ave., 98/240
Russia
vsaraeva@mail.ru