Advances in Social Science, Education and Humanities Research, volume 420
XVII International Research-to-Practice Conference dedicated to the memory of M.I. Kovalyov (ICK 2020)

On Infringements of Right to Privacy Through Information and Communications Technology: Legal and Identity Aspects

Inkizhekova M.

Ural State Law University of the Ministry of the Interior of the Russian Federation, Yekaterinburg, Russia
Email: masha_ink@mail.ru

ABSTRACT
The rapid move to digital platforms of scientific and technical development of modern civilization has brought with it many different issues. One of them is the issue of preserving human privacy of a person who uses in communicative practices technical devices operating on the "artificial intelligence" technologies, which leads to an increase in the number of criminal attacks on his/her data presented on the Internet, and, as a result, infringement of his/her right to privacy.
This paper analyzes the reasons for the increasing growth of criminal infringements that happen today in the World Wide Web. It also focuses on their complex and diverse nature. The convergence of external (objective) and internal (subjective) factors determines the transformations that occur to the identity of a modern Internet user. As a result, I conclude, in the conditions of the unraveling fight against cybercrime, the fundamental and legal sciences should pay attention to the concept of "identity", which will help determine the specifics of transformations occurring to Internet users.
Keywords: *identity, right to privacy, cybercrime, artificial intelligence technology, Internet*

1. INTRODUCTION

The rapid move to digital platforms of scientific and technical development of modern civilization has brought with it many different issues. One of them is the issue of preserving human privacy of a person who uses in communicative practices technical devices operating on the "artificial intelligence" technologies, which leads to an increase in the number of criminal attacks on his/her data presented on the Internet, and, as a result, infringement of his/her right to privacy.
Questions arise: Is there a connection between the growth of cybercrime and mental, social characteristics of social media users? What are the ways to decrease the risks and threats of invasion on the Internet users' personal space? How should the law regulate various interactions in the digital space? Such questions require a thorough analysis, based on which, it will be possible to develop practical recommendations and answers.

2. THE OTHER SIDE OF THE INTERNET

The active use of "smart" digital communicators for the rapid exchange of information makes life easier for modern people. This makes them mobile and better informed. However, this is only one side of the matter. What can lie beyond direct electronic communication practices, if we analyze them more deeply? We will find a phenomenon related to the operation of material and intellectual resources of people through manipulation of their conscience and behavior. With what can it be connected?
First of all, let me remind you that the World Wide Web is now under thorough attention of DARPA (Defense Advanced Research Projects Agency). It has been working intensely for many years on the new technologies that will integrate and process information from the entire global Internet space [1. P. 127]. As I wrote earlier in one of my articles, effective manipulation of human consciousness becomes possible with the help of projects developed by DARPA. It can have different purposes; for example, managing political processes, including those that lead to color revolutions [4. P. 121]. One of DARPA'S most significant and well-known research projects is Social Media in Strategic Communication (SMISC) [1. P. 132].
Even now, with the help of new technologies, not only some politicians can be controlled but also ordinary people ("Internet of NanoThings", "Internet of things" – both developed in the USA). From many portable devices (smartphones, smartwatches, fitness trackers, etc.) can be collected various personal information. As A. Losev wittily notes, nowadays even smart fridges and TV sets become domestic spies [6. P. 76].
Following the example of the United States, some other countries have also begun to develop tracking and control

Copyright © 2020 The Authors. Published by Atlantis Press SARL.
This is an open access article distributed under the CC BY-NC 4.0 license -http://creativecommons.org/licenses/by-nc/4.0/.

practices. Speaking at the Moscow Conference with a focus on national security issues, Igor Dilevsky, Chairman of The General Staff of the Armed Forces of the Russian Federation, noted that the rampant development of digital technologies leads to the fact that today more than 120 countries are developing information weapons [5. P. 4-5].

Having the possibility over different control tools is a dream not only for politicians but also for business sphere representatives. They invest a lot in developing new targeting technologies that will help track people's actions, manipulate them, and spy on them [9. P. 35]. I. Shnurenko also notes that in addition to the simple fact of total control, it is also possible to program the behavior of millions of people [9. P. 36]. In his opinion, it happens because: “Facebook, Google, Amazon have nowadays monopolized everything that occurs online, starting from things we buy and read, and ending with things that we love” [9. P. 35].

The aforementioned IT giants (Facebook, Google, Amazon, Google, Apple, etc.) are not the only ones who are interested in the users' data. Many terrorists, as well as extremist organizations, use various mechanisms of information influence on an individual, group and public consciousness. The purposes are different. But among the most common are mentioned: “the international and social tension, inciting national and religious hatred, the propaganda of extremist ideology and the attraction of new followers to terrorist activity” [10. P. 12].

After analyzing the present and potential future of digital technologies, Russian scientists conclude that one of the most important risks is the constant information control: “A person is condemned to it and will scarcely succeed to evade” [8. P. 109].

The technologies of political and marketing manipulation presented above are still largely unknown to ordinary Internet users. They experience on an almost daily basis the action of offenses of another kind. They come from criminal elements trenching on their personal information with the purpose to commit crimes against the property. Consequently, this leads to a violation of the constitutional guarantees of the right to privacy.

Criminal practices are explained, first, by objective reasons (technological features of the Internet), which do not allow law enforcement agencies to quickly identify them; secondly, by features of the psyche, which directly reflect the features of consciousness and behavior of modern subjects of virtual interactions. Therefore, scientists who have been studying virtual communications since the beginning of the XXI century are beginning to turn to the category of "identity".

3. THE SUBJECT OF INTERACTIONS IN THE INTERNET AND IDENTITY ISSUES

The information society, computer technologies, the steady growth of passive information consumers, the practices of active consumption; all of this forms a special type of a modern person – a person whose inner motivations are associated with the aspiration for comfort and escapism.

What can lead an ordinary internet user into the world of virtual simulacra and simulations (J. Baudrillard)? For some, it is the difficulties with everyday problems, for others - the search for new pleasures. In both cases, the reign of the game and masquerade in the virtual world give the user the opportunity to escape from the boring daily routine.

Immersing into the world of games, simulations and simulacra, such an individual begins to use the possibilities of the Internet space more and more for his/her virtual expression in the World Wide Web: for example, creating different userpics and avatars - virtual pseudo-identities. This person's creation of numerous "self-copies" gives him the false impression that he remains anonymous and unknown to other Internet users.

The illusiveness of freedom and the feeling of uncontrolled actions in cyberspace encourage some unconscientious users of the network to use the virtual world to commit a delict. In connection with this, the Internet acquires its negative side: the steady growth of cybercrime, which is now under the thorough attention of state institutions and law enforcement authorities.

The above examples of the behavior of users of network communications can be explained using the theory of the American sociologist Erving Goffman, who identified the phenomenon of the “fulfillment of different roles” by an individual in situations of social interaction at the micro-level. Goffman pointed out that when an individual perceives a phenomenon or stream of events at the micro-level, which includes virtual interactions “here and now”, he/she encloses them in semantic “frames”. It is designed as a system of knowledge and experience about typical situations (in this case, taken from the virtual world) that determine the direction of further actions of the subject in the context of emerging situations.

The actions of the subject become a performance/game, which leads to the loss of subjectivity and self-identity. It is a grotesque situation, when the "frames “define issues”, “reveal reasons”, “give moral assessment” and “offer solutions”, as noted by Russian scientists D. Plisetskaya and K. V. Filimonov [7. P. 161]. The plurality of micro-level communications creates the scenic plural "I", which is a consequence of "role-playing" and wearing a "mask". As a result, such a subject is not critical in the perception of reality, easily reacts to manipulations and has no principles. It is extremely easy for such a subject to commit a crime.

4. THE CLASSIFICATION OF PRIVACY-INVADING CYBERCRIMES

The increase in the number of cybercrimes committed and the appearance of organized cybercrime groups are directly related to the issue of privacy. Namely: violation of such rights guaranteed to a person and a citizen by the state, such as the restriction for collection, storage, use and

distribution of information about the person's private life without his/her consent; right for personal data protection; right of honor and reputation defense, and other types of confidential information.

The variety of forms and manifestations of cybercrime requires the ordering of concepts about it, including using the classification method. Only with the specialization and differentiation of the crimes committed, it will be possible to achieve criminal and legal regulation of this sphere of social relations.

An analysis of published works by experts working in the field of criminal law and criminology shows that a consensus on this issue has not yet been reached. Some researchers consider the methods of committing crimes as the basis for classification and use the categories "illegal", "unauthorized", etc.; for others that make up the majority, the subject and purpose of criminal infringement become the basis for classification. In this case, crimes are divided into two groups: 1) when the purpose of the attack is computer equipment; 2) when computer equipment acts as a tool for committing a crime against the person.

This approach is quite universal, but requires specification. First of all, I believe that the first group of crimes should be divided into two subgroups, highlighting computer-related crimes and computer-facilitated crimes (they are committed with the “help” of a computer and affect other computers and their equipment).

As the examples of the first subgroup (computer-related crimes) can be named such types of crimes as theft, robbery, banditry and other types of private property stealing, and infliction of harm directly to privately owned technical devices. The second subgroup (computer-facilitated crimes) can include intentional damage, deletion or distortion of personal data, failure or temporary resistance to the stable functioning of computer systems, limiting human activity.

The second group, where computer equipment acts as a tool for committing a crime against the person, can also include cybercrimes of both an aggressive (the first subgroup) and non-aggressive nature (the second subgroup). The first subgroup of crimes, that is, of the aggressive nature and committed "in" the World Wide Web, can include crimes against a person, expressed in forms of aggressive behavior in the online environment. Among them:

- "Cyberterrorism" that threatens the safety of many people;
- "Cyber-Mobbing" – a "chain" of threats, insults, and humiliations from deliberately constructed messages to influence the psych-emotional state of an individual or group;
- "Cyberbullying" is also associated with threats of aggressive treatment through electronic communication, but with intimidation about causing bodily harm, including incitement to suicide;
- "Cyberstalking" – harassment, including of a sexual nature ("Harassment"), in some cases also accompanied by either threats and insults ("Flaming"), or passing into the form of open threats of physical violence and causing particularly serious bodily harm ("Cyber-threats"), including direct or indirect threats of murder ("Cyber-kill threats").

The second subgroup of cybercrime, not of a violent nature, can be attributed to criminal attacks on information about the private life of citizens. Methods of committing crimes are unauthorized interception or substitution of specific personal data to extract compromising or spread false information about a person, including the discrediting his honor, dignity, leading to the loss of a person's reputation, as well as cyber-theft, cyber-fraud, cyber-extortion, etc.

Overall, despite the existing considerable differences, cybercrime has a certain amount of common characteristics. In particular, the following is typical for it:

1. Latency (hidden nature) of actions, user anonymity, which is achieved due to the use of the technical device computer-aided operation mode;
2. High-professional competency of criminal activity subjects in the field of IT technologies;
3. A considerable volume of damage, not only material but also moral, sometimes resulting in catastrophic consequences for the injured person;
4. Transnational scale (where crimes are not subject to the jurisdiction of one specific state, that also leads to scarcely solvable enforcement procedures);
5. Long investigation period. Maria Voronova, the Chief information safety expert of InfoWatch Group of Companies, specializing in information safety in the corporate sector, points out: "Investigation of even the most primitive cybercrime takes months, if not years because large resources are spent on revealing the traces of relations in the Internet space. As a rule, investigators succeed to solve cybercrimes only if people who committed them to let their guard down at some stage and made a mistake" [Quoted after 3. P. 70]. Consequently, only 3-4% of cybercrimes are solved in the world today, according to Russian scientists A. Grammatchikov and O. Vandysheva [3. P. 70].

Scientists warn that the number of crimes in the world of the digital economy will not decrease, and the degree of human society criminalization will not fall. For this reason, the law should be updated regularly, with the inclusion of new standards and regulations in its system, summarizes S. W. Brenner [11. P. 52-61]. As for the situation in the Russian Federation, according to D.V. Vasilyev and A. A. Laskin, "the number of digital crimes has increased by 75% over the last three years" [2. P. 17].

5. CONCLUSION

In the conditions of the unraveling fight against cybercrime, the fundamental and legal sciences should pay attention to the concept of “identity”, which will help determine the specifics of transformations occurring to Internet users. Also, in order to fight the illegal actions of criminals who have become "anonymous" in the digital environment and cause considerable damage to the citizens' legal right to privacy, the law-making and law enforcement state systems should be sensitive and respond

in time. At the same time, there is no doubt that the development of the e-economy, digital production, e-learning and e-medicine will require constant updating of digital technology laws. Moreover, it can be assumed that the legal practices of controlling will become more complicated due to the development of inter-subject ("Internet of people"), inter-object ("Internet of things") and subject-subject (man and machine operating on the "artificial intelligence" technology) interactions in the cyber-physical space.

REFERENCES

[1] A.I. Ageyev, Ye.L. Loginov, Fight for the future: who will be the first in the world to learn noomonitoring and subjective reality cognitive programming? Ekonomicheskiye Strategii, 2 (144) (2017) 124-139.

[2] D.V. Vasilyev, A.A. Laskin, Issues of legal support of preventing crimes in the field of the digital economy and ways of their solution, Zakon i Pravo, No. 3. (2018) 15-20.

[3] A. Grammatchijov, O. Vandysheva, There's a people's cyberwar going on, Ekspert, No. 5 (2017) 65-71.

[4] M.S. Inkizhekova, "Multifaceted self-definition" phenomenon at the age of digital technologies, Artificial intelligence: ethical issues of the "digital society": Materials of Internarional Research-to-Practice Conference, BGTU Publishing House, 2018. pp. 119-123.

[5] Information wars: maximum alert, Ekspert. No. 18-19 (1028) (2017) pp. 4-5.

[6] A. Losev, Age of still waters in global politics, Russia in global politics, No. 1 (2018) 66-78.

[7] A.D. Plisetskaya, K.V. Filimonov, Framing and reframing in speech strategies of American political leaders, Bulletin of Moscow University. Series 21. Management. No. 4 (2015) 160-174.

[8] S.V. Rogachev., S.V. Nekrasov, Digital reality: options, challenges, risks (review according to the "Round Table" materials), Social technologies, research (SOTIS). No. 3 (2018) 107-110.

[9] I. Shnurenko, How technology gives birth to tyranny, and whether they can save democracy, Ekspert, No. 47 (2018) 34-37.

[10] C. Beck, Web of resistance: Deleuzian digital space and hacktivism, Journal for Cultural Research. No. 20 (4) (2016) 1-16.

[11] S.W. Brenner, Fantasy Crime: The Role of Criminal Law in Virtual Worlds, Vanderbilt Journal of Entertainment and Technology Law, 11(1) (2008) 1-98.