 DOI: https://doi.org/10.15388/OS.LAW.2020.12

CAPTAIN AMERICA PROTECTING DIGITAL RIGHTS: "OLD SCHOOL" NATIONAL LAW vs. EMERGING INTERNET COMPLEXITIES IN AZERBAIJAN

Shahin Mammadrzali[1]

Abstract. It is indicated in the article that emerging information technologies influences human rights norms in any democratic society. Especially, the Internet has changed the traditional approach to methods of ensuring human rights, while adding new challenges at the same time, such as regulating cybersecurity, digital data protection, digital freedom of information, privacy, discrimination in the Internet, etc. The traditional flow of information through newspapers, radio and television is currently combined with new means of exchanging digital information, mobile and satellite communications, the Internet and other technological advances. Of course, these innovations make governments to review traditional human rights legislation to stay fit and updated. Yet, some fundamental norms of national human rights legislation should remain unchangeable. Simply put, it looks like Captain America from the movie "Avengers" – a very old guy who develops his abilities to defeat dangers, but also preserves "old school" strength and leadership skills. In the light of these issues, the present article is devoted to the analysis of the conceptual foundations of national legislation in Azerbaijan on the protection of digital rights in the Internet. The article emphasizes that digital rights themselves are one of the factors demonstrating the strong impact of communication technologies on human rights, especially information rights and freedom of expression.
Keywords: information rights, freedom of expression, freedom of information, digital human rights, cybersecurity, data protection, information security, Internet, privacy.

INTRODUCTORY NOTES

Rapid development of information society makes it necessary to improve social and cultural life of country, and to regulate new social relations. In this regard, special attention of legislators is attracted by the Internet and relevant digital human rights, prevention of electronic threats and cybersecurity, which play a crucial role in the management of the information society. Taking into account the emerging interrelation between the Internet and human rights, international and national legislator pay more and more attention to appropriate digital human rights regulations. The primary concern is that traditional human rights standards still comply with the digital use of rights and freedoms, but requires new analysis. Nowadays, we may observe digital rights as the new reflection of traditional landscape, especially freedom of expression and information. Probably all of universal and regional human rights mechanisms acknowledge digital freedom of expression and information as the cornerstone for information society building. Yet, international bodies keep silence in determining the content and scope of digital human rights. In its own turn, different approaches to the range of digital

1 *PhD in Law, Baku State University of Faculty of Law. memmedrzali@gmail.com.*

rights and their protection can be seen in national laws of various countries. We may classify groups of digital human rights based on criteria such as online user rights, digital security, data privacy, etc. But it is not sufficient to formulate ideal system of national digital regulation. In general, digital human rights as well as cybersecurity are the integral part of universal human rights system and there are several reasons to prove their importance. Digital rights as part of information rights are crucial for the enjoyment and realization of different groups of collective and individual rights. Thus, right to participate in political affairs and public life, right to education, other social-cultural rights along with right to life and fair trial are among the most interrelated human rights and freedoms for what information society is a new landscape to benefit from. International regulation of human rights also requires the full conditions for the use of human rights by special people groups such as children, youth, elderly people, migrants, refugees with no any grounds of discrimination. Bearing this in mind, digital rights contribute to strengthening political and social balance of the society taking it to the new step of development of information and knowledge society. On the other hand digital human rights could be derived from international obligations of state and non-state actors. In this regard, respecting, protecting and ensuring human rights entails direct reference to share and dissemination of information about human rights. This consideration raises public awareness about whole human rights system as well as supports human rights education what is impossible without digital human rights.

Azerbaijan, as a member of the CIS, has achieved significant results in the implementation of the requirements of international law, the elimination of cyber threats and the prevention of cybercrime. However, study on digital scale of human rights, information society and digital security is not so popular in Azerbaijan. One may prove that there is a strong need to study digital information security and human rights in civil and criminal law areas, human rights in Internet, digital media freedom, national and international regulations on social media, information rights in business and so on. Besides, although the 2030 Agenda of Sustainable Development together with relevant instruments requires strong engagement in digital human rights regulations and Azerbaijan conducts innovative reforms in this sphere, significant concepts and national laws have not been integrated fully in the country. Since the first years of its independence the Republic of Azerbaijan has made effective efforts on adapting national human rights standards and regulations to European human rights features. In this regard, the constitutionalization of information and media rights along with special provisions of domestic law on information society and information security create new opportunities for reviewing digital human rights standards in the country. Still, particular attention should be paid to problematic aspects in the national legislation, namely gaps of human rights norms related to digital human rights sphere and cybersecurity. There is a significant lack of legal studies and legislative research dedicated to cybersecurity concepts and discussion of relevant legislation. In this regard, the present paper seeks to get appropriate answers to the perspectives of digital rights, information rights and cybersecurity in particular, through the analysis of new legislative reforms and revision of conceptual fundamentals. It should be mentioned that, as it is the case of other post-Soviet countries, digital rights, right to cybersecurity and information society norms have not been the central objects of academic discussions and debates in Azerbaijan for a long time. That is the reason why one cannot

find enough scientific research and academic background in national literature on digital human rights. Of course, international organizations and bodies that Azerbaijan is in strong cooperation with, commends human rights innovations and implementation of international responsibilities by the national government. Nevertheless, the ground to discuss argumentative sides of national human rights legislation as well as legal attempts towards well-developed management of cybersecurity, preventing cyber attack and ensuring digital information space still keep importance what is the main purpose of the present article. Of course, it should be highlighted importantly that the present work does not follow the purpose to criticize negatively all of the legislative activity in the country forgetting the achievements in the field of Internet freedom, digital media rights along with national plans and strategy on information society as such kind of approach may be out of objectivity. In this view, the current work is a summary of governmental work on information legislation and national study of information law with all its negatives and highlighted achievements. Bearing this in mind, one can suppose the current academic work as a suggestion of citizens which is intended to improve the digital rights legislation and theoretical framework too. Without doubts, the principle of reality and objectiveness of academic work put a responsibility on us to overview all of the critical points of fulfilment of international human rights obligations by Azerbaijan that is only aimed to support and contribute of raising the effectiveness. Thus, critique for further development in economic, social, political and cultural fields obliges us to objectively analyze national law on information rights, freedom of press, national subjects of human rights protection and defence. Therefore, we hope and believe that our respected and honored reader would find the full knowledge on digital rights trends and the will of Azerbaijani government to create all of democratic conditions for our nation to live in peace and security that stress respect for human rights. In order to respond to these aims and prospects of the introduced topic, the article is divided to some conceptual parts. It starts with the brief introduction to the topic that is followed by some theoretical implications reflected in domestic legislation on digital human rights and information society. The main part of the article contains analysis of Constitution and important national laws. The final part of article is dedicated to the summaries and recommendations for the improvements of national framework on digital information rights and cybersecurity in Azerbaijan.

DIGITAL CHALLENGES AT A GLANCE

Of course, emerging Information-Communication Technologies (ICT) and computer devices, the creation of the Internet network provide great support for our use of human rights both in public and private life. The technologies make the development and renewal of human rights more efficiently. Nevertheless, it would be far from the truth to say that new technologies and the cyberspace have only positive impact on human rights. Problems introduced by digital human rights regulations such as the legal contradiction, theoretical and practical conflicts of technology in the traditional human rights system, and infinite debates are also enough. The problems created by ICT and computer technology in the field of human rights can be classified differently. In general, ICT creates difficulties for the

full enjoyment of certain rights such the "green rights", i.e. environmental rights. New technologies cause more damage to nature and many global environmental problems. Besides, the adverse effects of new technologies could be noticed on the health and well-being of the people. These problems include excessive radiation, psychological dependence on digital games, programs, mobile phones and so on. ICT and computer network have a negative impact on social rights and labor rights too. By the fact that companies and employers want to apply new technologies, saving their workforce has led to problems with unemployment and social security. Additionally, modern technological discoveries and their application have created threats to living in peace, in a friendly atmosphere and in full security conditions. Application of new types of weapons, digital manipulation, dissemination of various non-realistic information, etc. make our daily lives hazardous. Still, in our opinion, the most significant challenge facing the ICT is the lack of digital environment management, the protection of digital human rights in virtual space, and the lack of direct application practice. The key issues facing the use of digital rights in digital area are influenced by concrete factors. Digital environment, especially Internet technologies, creates new types of conflict between human rights. For example, freedom of information and freedom of expression implies the free circulation of different types of books, articles, publications. In contrast, digital copyright recognizes the author's exclusive rights over scientific creativity patterns and determines that there must not be free circulation without author's permission. Hence, copyright infringement within the digital environment creates a conflict of interest. On the other hand, various kinds of electronic transactions carried out in digital market with regard to artistic works and creative pieces usually contradicts the requirements of intellectual property rights. In another area, information related to daily life of popular people is often shared on the social media. But the extent to which the sharing of this information is appropriate to the privacy and family life of the person is questionable.

Digital environment creates opportunities for new types of human rights threats and offenses. That's why, digital rights are sometimes misused. Communication programs or social media disseminate sensitive information, transmit inaccurate information, and slander or insulting expressions. At the same time, there is a strong need for certain restrictive measures and penalties that still does not give the necessary result. On the other hand, the digital environment implies the use of rights in a safe and secure environment. However, digital theft, damaging information environments, application of certain malicious programs, electronic property infringement, etc. make it impossible. Digital environment regulation also raises the question of "Is there a sharp difference and separation between digital environment and real-life, between electronic legal regulation and traditional legal norms?" In our opinion, we must answer this question negatively. Because the digital environment and the real life are different from the first sight, but the rights regulated in both spheres are interrelated. This relationship is also linked to violations of law in both spheres. For example, it may be that the basis of any human rights violation is real, but the result causes threat in digital space. On the contrary, it is also possible that in the event of a digital violation damage occurs to the real person. For example, virtual identity contains personal information about concrete real human being. When this information is stolen on the Internet, our rights as a real person are violated. The loss of the

software in our e-sale process should, in fact, be regarded as damaging property rights in real life. The application of penalties and punishments also demonstrate the relationship between electronic and real-world. Thus, administrative, criminal and civil penalties mean physical and electronic constraints. For example, if a group of individuals infringe digital safety, present slanderous or insulting comments in digital space, they well be administratively punished. At the same time, digital profiles, technical equipment and malicious software programs used by them also will be confiscated.

It is fact that when you say "digital rights" or "cyberspace", people assume social media such as the Internet and virtual reality programs – "Facebook", "Instagram", etc. However, digital human rights should not be limited only to the Internet and social media, but to the broader sense of digital technology means. Originally, ensuring, protecting and regulating human rights is primarily the responsibility of the state, the key bearer of international human rights duties. Yet, in our view, the huge burden of electronic technology and the regulation of digital environment cannot be put only on the state mechanisms. This may, in any event, lead to the failure of the offender to bear responsibility for the digital offense. Along with state mechanisms, the problem of digital environments involves non-state actors – Internet service providers, digital companies, various internet programs and social media owners, and international organizations, legal entities and individuals dealing with information transmission in digital media, and ultimately, all active and passive participants in the digital environment. All legal entities and individuals who are engaged in entrepreneurial activity for other purposes are referred to as "internet intermediaries". The responsibility of legal entities and individuals acting as Internet intermediaries in digital environment is a matter of concern and sensitivity. It is almost impossible to get a global agreement on the solution of this problem. Thus, responsibility for non-state subjects in the digital environment makes it more secure to use ICT and computer technology. On the other hand, excessively severe penalties and punishments may be viewed as pressure on information rights and freedom of expression in the digital environment. Therefore, while state bodies commit to the regulation of digital rights, they must take account of all the specific conditions in each national legal system and society. One may consider that main difficulties arising with the legal regulation of digital information rights and information society occurs because we are trying to put e-relations or virtual sphere to written law norms. The cyberspace is interpreted in the light of the Internet and simply said, while discussing the security and safety of cyberspace, vast majority of people limit themselves only to the notion of Internet. Notion of cybersecurity involves human rights-based approach to the Internet law. Most of prominent experts also proclaims respect to human rights and freedoms as one of the general principles that should be followed by the Internet regulations (Benedek et al., 2008, p. 47–48). However, in its real face cyberspace is not only about the Internet and it covers other digital information technologies, information databases and collections. Still, it should be confirmed that it is exactly the Internet that covers all of problems and difficulties about the cyberspace. Therefore, while analizing the cyberspace and cybersecurity, we may centralize our attention on the security of the Internet and Internet users. The Internet and the problems that it encounters constitute a research object for many sciences and subjects of technical and applied character. We believe that it is expedient to clarify the technical,

historical problems facing the digital rights and, as a matter of fact, to clarify human rights and legal regulation issues on the Internet.

PECULARITIES IN NATIONAL LAW

Definition of the Internet in Azerbaijan varies as there are plenty of different approaches to the matter from social, informational, political and even ethic angles. The professionals from applied sciences usually try to conceptualize cybernetics and determine technical benefits of the Internet (Consalvo, Ess, 2011, p. 18–19). But one may agree that technological analysis of the Internet must not suffice legislators to establish proper regulations of digital human rights. As human rights are basically the result of social activities, we need to clarify the effects and negatives of the Internet in social terms. Therefore, most of internet researchers study social impact of the Internet as well as online behavior (Amichai-Hamburger, 2013, p. 120–121). We can say that in almost all international and regional documents, the Internet is interpreted from a social perspective. Hence, in order to make an objective appreciation, we should take into account both the technological and social features of the Internet.

Primary gaps exist in national human rights legislation of Azerbaijan in defining digital legal terms. For example, there is not any legal explanation or understanding of cyberspace, Internet, information, etc. in national normative legal acts. One cannot find even the definition of "digital human rights" in national law of Azerbaijan. Thus, we have to refer to the Constitution (1995) in order to find appropriate application of general norms in emerging digital area. Starting from the preamble, the constitutional provisions centralize main attention on international duties and obligations of government in the field of human rights. As so, key concepts for the realization of the digital rights in domestic law are included to the Preamble of the Constitution stressing out fundamental intentions of the Constitutions as an expression of the will of the nation while remaining faithful to universal human values. The general obligation of government to protect human rights and freedoms are proclaimed in Article 12. This idea contains criterias for obligations as the highest priority object of the state including their implementation in accordance with international treaties. Moreover, Chapter III introduces the inviolable and inalienable nature of human rights and freedoms in the territory of Azerbaijan and this declaration can be addressed to digital human rights and freedoms too. More precisely, Article 47 covers essential features of freedom of information and media rights. It establishes everyone's freedom of thought and speech. Going further, Article 50 guarantees free flow of information through any means along with prohibiting unlawful limitation such as censorship regarding media and press. The term "any means" allow us to consider digital flow of information and digital data security as elements of media and press too. Article 51 establishes grounds for creative activity that promulgates freedom of new forms and means of information. Articles 54 and 55 introduce the right of people to participate in political, cultural life of the nation and well as in governing procedure. Article 60 guarantees legal protection of human rights, especially freedom of information. Going further, Article 71 introduces grounds for restrictions of rights at wartime, time

of emergency and mobilization in conformity with the international obligations of Azerbaijan. The Constitution stresses out the principle of publicity for the sessions of Parliament in Article 88 as well as establishes the obligation to publish judgements of the Supreme Court, the Constitutional Court in Articles 130–131 and also the normative legal acts defined in Article 149.

Yet, some critical points put doubts and questions to the maintenance of human rights by the Constitution. We consider that an individual and special provision should be added to the Constitution of Azerbaijan in order to modificate it in compliance with international standards on digital rights and cybersecurity. Of course, general provisions of ensuring any means of information freedom entails digital human rights reference too. But, at least, special commentary or explanatory memorandum should be established to apply these general norms precisely. Moreover, in our view, it would better to clarify the degree of restrictions upon digital human rights, the procedural side of restriction mechanisms, levels of restrictions during time of emergency and wartime and their interrelation with international obligations in the Constitution. However, Article 71 of the Constitution stipulates that restrictions to the human rights could be based on the other provisions and laws of Azerbaijan. We consider that this provision does not strictly stop the misuse of restrictions in digital sphere either. In our view, a full list of restrictions included to the Constitution as well as narrow interpretation of restrictions will be able to solve the problem.

It is without doubts that if the technical support of the Internet is low, it will have an impact on the social aspect too. It is impossible to speak about the normal communication between people and safe use of digital rights in conditions of poor technical level of cybersecurity. Therefore, it is necessary to clarify the principles on which the Internet is created and how the cybersecurity matters are included to these principles. While the guidelines for the Internet regulation are determined for its management, it essentially serves to protect basic human rights and freedoms in the network, including the effectiveness of information security (Weber, Grosz, 2010, p. 207–214). In this regard, the Criminal Code of Azerbaijan dedicates special chapter to information crimes and violations in cyberspace (1999, Chapter 30). After the deep analysis of this chapter, we may conclude that direct norm of punishment for Internet providers and host organizations does not exist. The non-existence of such norms gives freedom to Internet space more than enough what would result in raising number of digital crimes. Therefore, establishing precise penalty or punishment for crimes indirectly supported by Internet providers and IT companies is essential for national legal environment. It would also be commendable to control and manage cyberspace by digital regulations means. Thus, law experts strongly recommend Internet providers to create appropriate filters and restrict illegal circulation of information by digital means (Bayuk, 2012, p. 93–96). It should be noted that the legal sources of information law in Azerbaijan also contains special acts that are the regulations in the field of media, education, culture and etc. As the national legislator considers international agreements of Azerbaijan as an integral part of domestic law, one can include international agreements of Azerbaijan to the system on national framework for information law. For our discussion it means that the relevant international standards on information rights are defined as the part of domestic law in Azerbaijan. In this regard, the implementation of international human rights standards has affected

the Criminal Code too. Articles 155 and 156 of the Code establish criminal penalty for the disclosure of private conversation by phone, email and private life secrets. Respectfully, Article 163 aims to prevent the infringement to the professional journalistic activity by refusing to give or disseminate information or using force. Article 202–203 of the Code contains provisions prohibiting disclosure of commercial and state secrets. The Code of Administrative Offences also includes specific sanctions for violations of legislation on access to information. Taking into account the international recommendations, Articles 39–50 of the Code provide penalties on propaganda materials during election periods, prohibits dissemination of false information about deputies, establishes punishments for the media rights violations during elections, for violation of use of state information system and information collections. Articles 181–192 create a special chapter devoted to the violations against right to information and information protection.

Additionally, cybersecurity preserves its importance for safe digital economy and civil law arrangements too. However, national civil laws in Azerbaijan do not contain any direct provisions regarding digital use of human rights or security matters in cyberspace. This problem involves serious challenges and difficulties as regulation of digital economy and digital market is left by the civil law legislation as an open place for any kind of cyber attacks and illegal use of digital information. Nowadays, the information market develops more rapidly and in some countries labor resources concentrates more in the information sphere than in traditional fields of economy. It is widely recognized that information technologies aiming producing, analysing and importing information change the nature of industrial society towards information society. The establishment of internal information sphere in the country is one of the first conditions for the foundation of information society. However, information society needs international integration and globalization of relevant legal, social and political standards too. These trends add importance to the improvement and innovation of the whole information infrastructure including the digital rights, cybersecurity matters and digital security of Internet users. On the other hand, global information society supports the recognition of digital democratic values and contributes respect to persons and their participation in digital information relations by enjoyment of their personal and collective digital rights and freedoms. For the proper analysis and regulation of information society, we need to know main elements of information relations, at first. It is easy to define that information relations are the relations appearing while receiving, imparting and disseminating information as well as producing and expressing it. The participants of information relations are usually considered legal subjects as they have individual rights and obligations and bear responsibility. Thus, in order to be a subject of information relations you need to participate in the mentioned procedures as well as own rights and relevant duties. Indeed, right to information in its traditional meaning, also other elements of information rights contains the fundamental rights and duties for the subjects of information relations. Therefore, the international and national law on human rights in the information sphere usually addresses information rights and information society together.

In the light of international trends, the lack of national legislation of Azerbaijan on digital human rights and cybersecurity puts some crucial questions for discussion. Of course, the foundation and

development of information society in the Republic of Azerbaijan should be characterized by high rates and the activities in these spheres are realizing incrementally on successful practice. However, when it comes to digital law regulations and cyber law, there is a high demand to set up new binding rule (or normative legal act) that would be ground for the development of soft law principles. In this regard new presidential decrees create priorities for future reforms of digital legal framework (Decree of the President of the Republic of Azerbaijan, 2012). In international human rights law the regulation of information rights and freedoms contains various approaches to the issue. The traditional International Bill of Human Rights together with regional conventions, namely European Convention on Human Rights, Charter of Fundamental Rights, Inter-American Convention on Human Rights introduce the roots and starting points of digital rights. However, specific laws follow these documents that include more clear and precise requirements for the implementation of information rights on domestic level. The same approach could be referred to national information regulations as some of them are the basis for the specific other rules.

Summarizing all the discussed and introduced points, one can say that domestic law of Azerbaijan needs a marked shift in ensuring digital human rights. Significant attention must be paid to cybersecurity as individual human right as well as pre-condition for other human rights that are the building blocks of information law. Taking into account the new forms of cyber attacks and security threats, national norms regulating the Internet need to be improved. From a theoretical point of view, a new right-based approach to cybersecurity should be developed on the basis of international case law and human rights documentary what is supported by European scientists too (Wagner et al., 2019, p. 90). Besides, cybersecurity involves obligations not only for states, but also for Internet providers, civil society organizations and other participants of digital information circulation. Of course, some legislative problems should be resolved in the shortest possible time regarding the content and main elements of information freedoms and digital rights. It should not be forgotten that current protection of cyberspace is considered as one of the basic elements of national security. Therefore, use of Internet, high level of data protection along with digital information rights lay in the cornerstone of social, economic and cultural development. But, in general, our respectful reader can highly appreciate the integration way chosen by the young Republic of Azerbaijan towards common universal values. In this view, one can notice that legal thinking of society and legal ethics lay down on the fundamentals of globalization and integration. It is the same in terms of preventing cyber threats and ensuring safety of digital human rights too.

ARTIFICIAL INTELLIGENCE (AI) WAITING FOR TO BE REGULATED

Artificial Intelligence is a notion of ICT development and not all people understands its meaning. Simply put, there is no special legal norms regulating AI in Azerbaijan. However, experts consider AI is an element of our current daily life being used in all aspects of digital activities (Thomas, 2019, p. 3). At first glance, AI has nothing to do with rights and freedoms, but we need further detailed analysis. AI has a strong impact and AI technologies are entering to each and every corner of our

private as well as public life. Serious challenges for human rights are caused by AI and the difficulty of solving these problems is very high. AI-rooted problems in human rights law are colorful and the very root of this process is lack of knowledge about AI activities. Current AI controls ethics in the Internet, arranges our communication, manages statistics and prepare drafts, legal documents for future improvements. The complex character of AI starts from its definition, since there is no a unified explanation of AI in literature what can define AI from not-AI software (Partridge, 2013, p. 33). One thing is absolutely clear that nowadays it is absolutely impossible to ensure cybersecurity, human rights protection and safety without AI conduct. But AI is not always in friendly attitude to human rights. AI software is capable to violate or restrict our rights and freedoms what may result responsibility. I think that is the very root of the AI-based legal questions on whether or not AI can be fully regulated by traditional law. As it is mentioned before, AI can positively support and infringe human rights at the same time period. Taking into account the last trends in AI application to public and private spheres, I can introduce positive aspects of AI as following:

- Ability to predict: AI technologies have ability to see and inform about future danger. It can be dangers of earthquake or possible illness.
- Ability to sustain the development: Despite all the negative issues, AI is a tool for sustainable development. Thus, it can be examined as a crucial element of UN 2030 Agenda for Sustainable Development.
- Ability to adapt: AI is very sensitive to changes. It makes people's life easier. AI is very helpful in terms of economy, ethics, communication, etc.
- Ability to assist: AI is one of the useful instruments of us in resolving global problems such as climate change or environmental pollution. In this regard, AI function of data mining is of high importance.

AI contains some threats for human rights too. Social media users usually face the problem of AI while building new communication or creating new profiles. The issue is that probably all organizers of digital media platforms arrange software tools to prevent insult, humiliation or hate speech. Sometimes, ordinary words used in usual discussions with no insult purpose are recognized as negative and deleted or banned by the software tools. It means that algorithms that these software programs consist of, have not been set up well and were wrongfully developed. Whatever the reason be, the final act of AI software results violation of freedom of information. The same negative process can be suffered while forming new profile or web-page too. A wrongful design of software may recognize new page as spam or risk to digital safety. The outcome will be stopping or banning new page and violation of right to property in cyberspace. These are some simple examples of how AI can work in negative manner and harm human rights enjoyment. There are some other types of possible AI dangers to human rights what can be grouped as:

- Discrimination;
- Disinformation or false information;
- Violation of privacy;
- Harm to cybersecurity, etc.

In general, to systemize the AI impact on human rights, we need to build up some steps for effective academic research. These steps can be as following:

- Understanding the design and structure of machines or AI software;
- Creating models of AI activities in digital environment;
- Detecting primary challenges and finding solutions.

Understanding of AI technology is relatively difficult for experts from social sciences. In any case, one needs to take into account that AI technologies are built on the basis of simple codes and algorithms (Tyugu, 2007, p. 3). Algorithms and codes are the basic elements of digital language in the Internet space. And it is the same for all kinds of digital programs and software. All of actions of us in digital environments such as sending messages, sharing files, etc. are realized via digital commands. The programs and software understand these commands (orders) in the form of codes and algorithms. In general, algorithms build strategies and directions for codes as well as ensure the stable movements of codes. When it comes to AI, designers strive to establish algorithms and codes as free and independent mechanisms what can make decisions, learn and develop. Simply put, algorithms in AI try to increase their abilities, create new algorithms or change existing ones. Making robots or terminators are based on the same algorithmic strategies. It looks like a human brain able to be sensitive to innovations and changes. However, not every one of algorithmic system means a robot or a digital brain. There can be some simple AI technologies such as programs detecting hate-speech or illegal interference to content. The tough issue is how to differentiate simple programs from well-developed AI technologies. In this respect, legal literature examines different understandings and instruments to classify AI technologies. While building a classification, one should not forget that not all AI are fully independent mechanisms and not all of them are robots. On the other hand, AI is not only a mechanism, it is also a process. That's why AI-based classification is hard, but very important. Classification of AI technologies can be based on different criteria but they comprise of the same lifecycle phases (OECD, 2019, p. 26, 28). In any case, Data Mining and deep learning methods lay down in the cornerstone of AI. AI uses different methodology to collect information and study it. It means that AI should work in close collaboration with information security institutions. In terms of human rights, AI as well as data mining procedure touches privacy rights, cybersecurity and freedom of information. Yet, these connections are sometimes very painful, because data mining machines may easily violate human rights. For example, AI programs can prepare very private but new information via summarizing ordinary data about a person's daily routine, behavior, habits, skin color, etc. Of course, that person will not be very happy to see his / her name and all characteristics of his / her body in AI-based statistics. It would mean violation of private life. Therefore, AI and ML have lot in common with privacy rights. I may claim that sometimes they can impact human rights in such a level that new rights could emerge. E.g., if a person is not glad about AI technology collecting personal information, he / she may ask to stop it. Or he / she can ask for non-disclosure of that information. In order to do this, the person should be aware about the information collection. Simply put, before information collection and analysis, persons must be informed about possible AI activities, in order

to comply with requirements of access to information. However, it is not always possible or allowed. Governments may arrange AI to collect information about dangerous diseases or criminal acts in one region without informing people living there. Thus, previous character of inviolability in terms of privacy can be put under danger what should be properly regulated by national law.

CONCLUDING REMARKS

In order to change the legal behavior and legal ethics understanding of societies, some countries prefer to us the "shock therapy", namely immediate reforms and changes in social, political, cultural life of the country that is usually followed by social conflicts or aggressive public debates. In terms of digital law and digital human rights regulations, it is quite impossible to renew the whole picture in one or two years by hard laws and punishment. Because, Internet ethics, digital legal behaviour and better use of information rights need to be assisted by relevant social, economic reforms in regular and very soft manner. Moreover, it is not only the situation in Azerbaijan, but also in most of European countries that drawing precise scale of legal liability and obligations upon digital information users, Internet providers and digital persons is still an ongoing question that has not been able to find suitable solution (Riordan, 2016, p. 5–8). On the other hand, most of countries follow the way of so-called "soft method" that contains cultural, political and social steps to be done regularly during a certain period of time supported by interrelated educational, scientific and other more technological methods. The second way of changes and integration has been chosen by the government of Azerbaijan that demonstrates evidences in our daily life and activity. Bearing in mind the above-mentioned facts, it is easy for reader to realize the role of human rights education with newly proposed theoretical-ideological grounds in the country. Indeed, human rights education addressing digital rights and standards on information society are the serious attempts to review traditional way of thinking in Azerbaijan that could be detailed by some possible recommendations:

a) Information society is conditioned by public awareness in digital human rights, especially information rights and standards on cybersecurity. Unfortunately, the real facts of Azerbaijan do not let us to prove high level of public knowledge in the sphere of digital information rights and cyberlaw. Although, the national legislation entails enough freedom and chances, public participation in decision-making procedure over information society issues, cybersecurity and digital information regulations in particular, is quite low. In this respect, I suppose the improvement of NGOs activities, organization of special legal courses as well as legal education in digital human rights, cyberlaw and cybersecurity would be beneficial for the solution to problems.
b) Despite of the fact that relevant national laws and regulations establish all the possible rights and freedoms for press, still, popular digital newspapers, blogs and magazines misuse their position of public watchdog for financial or other business purposes. It's especially essential while sharing unrealistic information without checking the sources or disseminating false information. I consider that the main reasons of the noted problem are rooted in unsatisfactory level of legal understanding and legal behavior by some press offices. In this respect, special code of ethics and soft law norms should be developed.

c) Of course, national courts of Azerbaijan representing judicial branch of the government implement and apply international human rights standards in the decision-making procedure. Yet, in terms of cybersecurity norms and digital rights, the courts seem to be reluctant to refer to the case law of the European Court of Human Rights and the EU Court of Justice. I suppose proper commentary and interpretation made by the Supreme Court or the Constitutional Court of Azerbaijan would be suitable for solutions to problems. Simply put, a well-developed case law on ensuring digital human rights and application of cybersecurity norms are of paramount importance for information society.
d) Among others, the dangers caused by Artificial Intelligence contain more negative "gifts" for national law of former Soviet countries including Azerbaijan. AI is a very concept both for academic and legislator in the country. However, the government in Azerbaijan has already established digital programs and items for digital government, electronic citizenship and e-democracy. Thus, AI technologies are also applied in these frameworks what should be studied and regulated in a more detailed manner.

While analyzing the introduced problems and concerns, one can prove that digital illiteracy and lack of relevant highly-educated professionals is a special topic of individual discussion. Indeed, new generations of young lawyers with European or, at least, foreign education, change usual landscape of human rights experts in Azerbaijan. Regarding to this, both private and state educational institutions of Azerbaijan are widely engaged in human rights education and training of open-minded lawyers especially in the fields of information law, Internet law and information rights. On one hand, the Human Rights Institute of the National Academy of Sciences together with the Ombudsman Office strongly commits in human rights research and academic work. Moreover, law schools and faculties in the country have already included relevant subjects on information society, information law and information rights to their official study programs. A very good example in this field is demonstrated by the Law Faculty of Baku State University that introduces several master and PhD programmes in the specializations of human rights, information law, intellectual property law, medical law and etc. Courses as international human rights law, information law, human rights, intellectual property law and bioethics are among the compulsory subjects aiming to deepen knowledge of students in mentioned areas.

It is also remarkable that the government of Azerbaijan demonstrates its strong attitude to its obligations to respect, protect and fulfil human rights as well as digital rights and freedoms in the Internet. New ways of human rights education, research, academic study are noted in advisory regulations addressed to public bodies. With this aim, relevant orders and decrees of the government contain new chances and possibilities of the implementation of information rights and freedoms in a safer national cyberspace. These examples and facts themselves, together with state strategies and policy activities in the field of digital rights give us hope to effectively comply with relevant international obligations in close cooperation with democratic civil society institutions.

Bibliography

Legal acts

1. The Constitution of the Republic of Azerbaijan (1995). Available at: https://en.president.az/azerbaijan/constitution [Accessed 26 January 2020].

2. The Criminal Code of the Republic of Azerbaijan (1999). Available at: https://www.wipo.int/edocs/lexdocs/laws/en/az/az017en.pdf [Accessed 26 January 2020].

3. Decree of the President of the Republic of Azerbaijan of 2012, No. 708 "On the Improvement of Activities in Information Security Field" [online]. Available at: http://www.e-qanun.az/framework/24353 [Accessed 26 January 2020].

Specialized sources

4. Amichai-Hamburger, Y. (2013). *The social net: Understanding our online behavior*. Oxford: Oxford University Press.

5. Bayuk, J. L. (2012). *Cyber security policy guidebook*. Hoboken: Wiley.

6. Benedek, W., Bauer, V. and Kettemann, M. C. (2008). *Internet governance and the information society: Global perspectives and European dimensions*. Utrecht: Eleven International Publishing.

7. Consalvo, M. and Ess, C. (2011). *The handbook of Internet studies*. New York: John Wiley & Sons.

8. Organisation for Economic Co-operation and Development (2019). *Artificial Intelligence in Society* [online]. Paris: OECD Publishing. Available at: https://ec.europa.eu/jrc/communities/sites/jrccties/files/eedfee77-en.pdf [Accessed 26 January 2020].

9. Partridge, D. (2013). *Artificial Intelligence and Software Engineering*. 1st edition. New York: Taylor and Francis Group, Routledge.

10. Riordan, J. (2016). *The liability of internet intermediaries*. Oxford: Oxford University Press.

11. Thomas, R. W. (2019). *Regulating Artificial Intelligence*. Cham: Springer International Publishing.

12. Tyugu, E. (2007). *Algorithms and architectures of Artificial Intelligence*. Amsterdam: IOS Press.

13. Wagner, B., Kettemann, M. C. and Vieth, K. (2019). *Research handbook on human rights and digital technology: Global politics, law and international relations*. Cheltenham: Edward Elgar Publishing.

14. Weber, R. H. and Grosz, M. (2010). *Shaping Internet governance: Regulatory challenges*. Berlin: Springer.