A Abdubachaeva, K Vavrik, K Ayvazyan, M Mkrtchyan & Y Nosik 'Sustaining human rights in the era of new technologies: Case studies of Armenia, Belarus and the Kyrgyz Republic' (2019) 3 *Global Campus Human Rights Journal* 286-311
http://dx.doi.org/10.25330/477

Sustaining human rights in the era of new technologies: Case studies of Armenia, Belarus and the Kyrgyz Republic

Aisuluu Abdubachaeva,* Kristina Vavrik,** Karen Ayvazyan, Mariam Mkrtchyan**** and Yuriy Nosik********

Abstract: *The development of new technologies and innovation is meant to enhance accessibility and make life easier. Due to the fast pace of development, the response of countries to new technologies is crucial to ensure their reasonable use. However, along with the development of new technologies different implications have emerged as some developing countries appear not to be capable of effectively responding to these developments. Despite the positive impact of new technologies on various aspects of life, their misuse has negative implications for the enjoyment of human rights. This article aims to explore regional challenges to human rights caused by new technologies at the national and regional levels. It also aims to identify long-term structural challenges to human rights in Armenia, Belarus and the Kyrgyz Republic with a focus on cyber security, freedom of expression, freedom of speech, access to information and data protection policies. It further aims to make recommendations to stakeholders so as to improve the situation and minimise the negative impact of new technologies on human rights. On the one hand, the study reveals that the development of new technologies increased the accessibility of people to information in terms of e-governance programmes. Moreover, it shows that political mobilisation and participation, and freedom of expression have been enhanced due to social media developments. On the other hand, it identifies the current challenges to human rights in Armenia, Belarus, and the Kyrgyz Republic in terms of increasing hate speech online, media manipulation, the spreading of disinformation, data leakage and cyber security. The study shows that despite the positive impact of the new technologies on the enjoyment of human rights, the inability of these states to effectively respond to the developments and eliminate the misuse of new technologies, and the insufficiency of strategies, legislation and policies, are negatively impacting on human rights.*

* This article is based on a paper prepared for and presented at the Global Classroom, a project of the Global Campus of Human Rights, Buenos Aires, Argentina, in May 2019. MA in Human Rights and Democratisation, Centre for European Studies, Yerevan State University; aisuluu.abdubachaeva87@gmail.com

** MA in Human Rights and Democratisation, Centre for European Studies, Yerevan State University; k.vauryk@gmail.com

*** MA in Human Rights and Democratisation, Center for European Studies, Yerevan State University; ayvazyan.karen@gmail.com

**** MA in Human Rights and Democratisation, Center for European Studies, Yerevan State University; mkrtchyanm27@gmail.com

***** PhD (Law); Associate professor of law, Taras Shevchenko National University of Kyiv; yuriy.nosik@gmail.com

Key words: *human rights; digitalisation; cyber security; new technologies; e-governance; freedom of speech; free flow of information; digital rights*

1 Introduction

Scientific and technical progress has led to the emergence of new information and communication technologies (ICT), which have both a positive and a negative impact on individuals' lives and on society. On the one hand, ICT have simplified access to information and significantly improved the communication landscape. People have become able to freely overcome geographic, political, and social barriers in order to build social interaction in a fairly short period of time. Moreover, the progress of ICT enhanced the concepts of e-democracy and the role of media as a facilitator of political mobilisation. In addition, the development of new technologies has contributed to the increased transparency and openness of the activities of the authorities. Of equal importance is the fact that the development of ICT has influenced the implementation and protection of a number of fundamental human rights. However, at the same time it became evident that these new technologies have become tools of manipulation, the spreading of disinformation, hate speech and data interception.

The use of social media networks, especially Facebook, Twitter, Telegram and Instagram has significantly increased over the past ten years. In this sense, online space is being actively used by different civil society organisations (CSOs) to reach a wider audience. For example, Facebook groups or pages are being created to serve as an effective tool for communication with the public to ensure timely responses in decisive situations. In addition, enhanced coverage of events by both local and international media (especially intensive live streaming) has constrained the radical actions of the government in relation to the public. However, the enhanced use of new technologies may lead to several human rights violations. What is at issue is the dissemination of hate speech, the use of individuals' personal data for unjustified purposes, and so forth. In addition, a strong relation between the rapid integration of information technology and cyber security was found, which raises questions about a number of security problems and their solutions, ranging from technical to legislative. The cyber security problem is one of the most pressing issues in the region, especially given its historical-political context. The latter refers to territorial conflicts and the geopolitical interest of major superpowers in the region.

Despite the relevance and importance of this topic, there is no comprehensive research in the field that addresses the challenges of new technologies to human rights in the region. The present research for the first time explores the impact of new technologies on the enjoyment of human rights in Armenia, Belarus and the Kyrgyz Republic. It explores possible mechanisms to prevent the violation of human rights with regard to the new technological developments.

The article aims to explore regional challenges to human rights caused by new technologies. It also aims to identify long-term structural challenges to human rights in Armenia, Belarus and the Kyrgyz Republic with a focus on cyber security, freedom of expression, freedom of speech, access to information and data protection policies, and to make

recommendations to the stakeholders to improve the situation and minimise the negative impact of new technologies on human rights.

The methodological approach adopted in the study is a mixed methodology based on the comparative and contrast analysis of the previous research on the topic, case studies and legal analysis of current legislation and regulations of Armenia, Belarus and the Kyrgyz Republic.

The main body of the report consists of three parts. Part 2 presents the Armenian case study of the topic; part 3 introduces the overall impact of new technologies on freedom of expression and freedom of speech in Belarus; and part 4 provides detailed information on the impact of new technologies on human rights in the Kyrgyz Republic.

2 Positive and negative impact of new technologies on the enjoyment of human rights: A case study of Armenia

This chapter presents how the rapid integration of ICT in the era of globalisation has affected the implementation of a number of fundamental human rights in Armenia and proceeds to describe the role of digital activism in providing even greater scope for democratic participation and decision making during the Armenia's Velvet Revolution. At the end of the section, the negative impact of the new technologies on individuals' lives and society is discussed, taking into account the historical-political context of the country.

2.1 The role of social media in political mobilisation: Armenian Velvet Revolution

The advancement of information and communication technologies in the era of globalisation has turned media into one of the most powerful factors in influencing the processes occurring in the world. This specifically refers to the fact that by means of social media it has become possible to promote a number of fundamental human rights, in particular the rights of peaceful assembly (article 21 of the International Covenant on Civil and Political Rights (ICCPR)), association (article 22 of ICCPR), freedom of opinion and expression (article 19 of ICCPR) and so forth. In this regard, social media has become a means of encouragement of a two-way political communication between the public and the authorities.

Digital activism or cyber-activism is a good example of how traditional notions of human rights have been complemented by a new phenomenon that provides an even greater scope for democratic participation and decision making. Digital activism, characterised by the substantial use of social networks as the main platforms to set up information campaigns and mobilise the masses, was the key factor of success of the Velvet Revolution in Armenia (2018).

In general, cyber-activism in Armenia touches upon many aspects of life: from controversial social principles to dissatisfaction with government policies. Activists deliberately choose social networks such as Facebook for the promotion of common ideas because of its worldwide targeting and transparency. The latter coincides with the principles for which these persons of influence are engaged in the political struggle. At the same time, Facebook is attracting the attention of political and economic elites as

many of them are active users thereof. By using Facebook, activists appeal to their multi-million diaspora. Members of the diaspora, especially those in the United States and Russia, are prominently participating in the political and financial life of Armenia. For this reason, the bulk of user-generated content is written in Armenian, English and Russian.

Over the past 10 years, numerous mass protests were staged in Armenia to express dissatisfaction with the government policies. However, the entire population did not seek to mobilise, but left the steering wheel in the hands of the youth. The case of the Velvet Revolution was somewhat different. When the protest action Take A Step was launched by the leader of the opposition, Nikol Pashinyan, both the youth and adults contributed to the common goal. The reason why in this case the majority of the population sought to take part in the country's political life was conditioned by the impact of digital activism that was causing a snowball effect.

Since the oppositionists mostly appealed to the youth, the first snowball was transmitted to them, thereby inspiring the latter to actively engage in the promotion of an online campaign on Facebook, called *Dasadul* (or 'class strike').[1] The campaign was aimed at encouraging students to skip lessons in order to participate in anti-government protests. On Facebook, special events were created almost daily to provide the interested citizens with all the necessary information as to when and where they needed to gather to start the march.

Another social network actively used during the Velvet Revolution to promote the idea of customer boycott was Telegram. By means of a special channel named Baghramyan 26, information was disseminated among its subscribers as to which supermarkets they needed to avoid using since the latter were the property of political and economic elites (for instance, Yerevan City and SAS supermarkets). The same information was shared by different groups on Facebook, mainly run by the youth.

Another form of the manifestation of discontent was the creation of a number of digital products that reflected the peaceful nature of the revolution, namely, songs (for instance 'Dukhov' ('Risk bravely'), 'Nikol Pashinyan'),[2] short documentary films, and so forth. These were necessary not only to convey key messages to authorities in a peaceful manner but also in order to gain the attention of third parties (that is, of the international community) towards domestic affairs.

The adult population did not yield to the youth. In their turn, professionals in the field of education were running online petition campaigns on their social networks, which were directed at supporting youth activists who had been arrested as a result of their participation in the protests, as this would undermine the value of a number of

1 These were the founders of the 'Restart Student Initiative', key drivers of the Velvet Revolution in Armenia, who coordinated the whole process and created on Facebook special events for the promotion of *Dasadul*, available at https://www.facebook.com/events/369494443572566/ (last visited 10 March 2019).

2 It is interesting to note that the word *dukhov* – a slogan that was very popular in social media and which was depicted on the hats and T-shirts of the protesters – became a real trend even after the revolution had ended.

fundamental human rights, including the right of peaceful assembly, association, and so forth.

Hence, the case of the Velvet Revolution serves as a good example of how new information technologies can help to exercise a number of fundamental civil and political rights and to create various digital products, capable of awakening people's politicised identity and mobilising them.

2.2 Open digital space: Fertile ground for hate speech, manipulation and the spreading of disinformation

With the development of new technologies the accessibility to information has also increased during recent years and the use of social media facilitates the spreading of this information. However; in countries where media literacy is not highly developed and where most social media users lack certain competences to differentiate real news from fake news, they easily obtain 'trapped' disinformation. As is mentioned in the Media Sustainability Index 2018 report, online media provides more varied viewpoints than the television outlets, but another problem arises here, namely, that '[t]he news feed, and the flow of fake news is so abundant that a public with quite low media literacy levels becomes ripe for manipulation' (IREX 2018: 5). Social media manipulations have escalated in Armenia, especially over the past year, when the opposition tried to bring up false agendas to discredit the previous government, which managed to win the sympathy of the vast majority in the country. Thus, the problem of media literacy, which arises with the development of new technologies and the manipulative use of social media, on the one hand, and a lack of literacy, on the other, has a negative impact on the wider public. Additionally, the manipulation leads to the hate speech towards certain groups, politicians or the government itself.

Another trend that has been very popular in Armenia, especially before the parliamentary elections in 2018, is online campaigning through fake accounts. Certain politicians or political parties make use of new technologies and social media and freedom of social media in Armenia to create fake accounts in order to manipulate the public with their false agendas. The fake accounts usually spread false information on behalf of the Prime Minister or the leading party in order to create mistrust towards the government and discredit the Prime Minister as well as to create an impression of enjoying popularity among the public. According to the investigations of the Union of Informed Citizens, a non-profit organisation, one of the major political parties (Prosperous Armenia) used 390 fake accounts on social media during its election campaign to create an impression of having a high level of support online (Fact Investigation Platform 2018).

In the post-election period more fake pages on Facebook were created on behalf of the Prime Minister and with the slogans of Velvet Revolution in order to attract more attention and get more followers who would be the target of the manipulation and disinformation. Based on the reactions of the public, who mostly believed in the disinformation provided to them as well as hate speech online and online extremisms, the Prime Minister had to ask the national security service to investigate and trace the people behind these fake accounts. Following the order, one of the fake account

users was arrested for spreading racial and ethnic hatred and discrimination online.

The extensive use of social media for political purposes could often entail negative consequences such as the spread of hate speech. In Armenia, by virtue of its strong conservative values, the representatives of the lesbian, gay, bisexual and transgender (LGBT) community often become the targets of hate speech. The social media is being 'served' for people to express their opinions about different topics and mostly the reaction of the public to the posts about LGBT activities and opposition thereto. A content review of the posts on social media about the above-mentioned targets by the most popular online newspaper shows that 82 per cent of the comments observed contained hate speech towards the LGBT community and a transgender woman who has spoken at the National Assembly, whereas 18 per cent were either neutral or combating comments without hatred. Moreover, another post on the LGBT community received 67 per cent hatred comments, and 33 per cent of combating or neutral comments without hate speech. In another case, a post about a member of the opposition, Armen Ashotyan, received hatred comments from 75 per cent of the commentators, while 25 per cent expressed neutral views on the topic and the politician itself (Table 1). Thus, the content analysis reveals that the social media is used to spread hatred towards the vulnerable groups and the opposition.

Table 1: Hate speech in the comments on social media

Facebook post content	**Total number of comments**	**Sample**	**Percentage comments containing hate speech**	**Percentage of neutral comments**
A transgender woman has spoken at the National Assembly https://bit.ly/2ULKmOb (Azatutyun TV)	1944	First 50 comments	82% (41)	18% (9)
An opposition leader, Armen Ashotyan, about the 2nd President, Robert Kocharyan, being a political prisoner https://bit.ly/2XBE9Bn (Aravot Online Newspaper)	216	First 20 comments	75% (15)	25% (5)
Article about LGBT community becoming more active in Armenia after the Velvet Revolution (Blognews.am) https://bit.ly/2Ve2xev	97	First 15 comments	67% (10)	33% (5)

It is worth noting that, in general, the regulations of hate speech in Armenia are rather limited. Article 226 of the RA Criminal Code (2003) covers only national, racial or religious hatred. The first part of the article claims that 'actions aimed at incitement of national, racial or religious

hatred, at racial superiority of humiliation of national dignity are punished' (chapter 26). However, no protection is guaranteed against incidents 'on the grounds of sexual orientation or gender identity'.

It is interesting to note that in practice, article 226 of the Armenian Criminal Code has hardly ever been applied, thereby provoking an atmosphere of impunity. During the Velvet Revolution most of the members of the national conservative party (Republic Party of Armenia) became the targets of hate speech. The latter was the ruling party of Armenia for 20 years and was often associated as a 'post-Soviet ruling party with catch-all ideology'.

When opposition leaders started their protest action Take A Step, the rhetoric of most of them was inflammatory. They were constantly emphasising the division of society into 'us' (that is, the supporters of the revolution) and 'them' (that is, those who were on the side of the Republican Party), giving rise to more incidents of hate speech and offending posts accompanied by memes.

2.3 Rapid integration of information technology in governance: Cyber security in Armenia

Considering the above-mentioned, it becomes clear that everyday society is becoming more dependent on information and communication technologies. Even more crucial is the protection of these technologies for the sake of the national interest.

The development of new technologies makes people's lives easier especially when it comes to accessing or requesting information online. However, it also presents some vulnerability in terms of cyber security. The Armenian government adopted e-governance several years ago, which gives people easier access to information. However, open access to certain information leads to the violation of human rights in terms of data protection. The latest example is Armenia's online voters' register elections.am, the aim of which is to provide citizens with information on locations of district electoral commissions (DECs). The website is developed in such a way that once a citizen (voter) enters some personally identifiable information in special columns, the voter finds information according to the residential address. At first glance this seems to be a good thing, but the problem is that any citizen of the Republic of Armenia who has the minimum information about another citizen – such as a name, surname and/or date of birth – can find the same information on his/her residential address, the DEC as well as information on that person's family members who are registered at the same address. The former in turn questions the right to privacy of this person and his/her family members (article 17 of ICCPR).

Chapter 2, article 4.2 of the Law of the Republic of Armenia on Protection of Personal Data (2015) states that '[p]ersonal data shall be processed for legitimate and specified purposes and may not be used for other purposes without the data subject's consent' (Law of the Republic of Armenia on Protection of Personal Data 2015). However, in case of elections.am, there is a problem as to whether it was justifiable to make personal information of citizens available to the public since this may also serve as a threat to a person's safety and security. In particular, if the purpose of the website is to provide information on district electoral

commissions, then the former can be developed in such a way as to replace columns with the entry of personal information (name, surname, date of birth, and so forth) with the column where the citizens will need to enter special personal codes, available only to them. The latter is of a huge importance since transparency in this case may serve no good but rather will encroach upon citizens' safety and will also serve as a threat to national cyber security as third parties can also access the information.

The development of the information society raises the issue of cyber security, which raises questions about a number of security problems and their solutions, ranging from technical to legislative.

The International Telecommunication Union (ITU) has published the annual Global Cyber Security Index (GCI) study (2017), which assesses the level of cyber security of states according to five main indicators: legal, technical (including child online protection), organisational, capacity building and cooperation. The study was conducted in 2017 in relation to 193 countries around the world. According to Table 2 it is evident that in the CIS region only Georgia and Russia had high GCI scores, and this was conditioned by their good performance in regard to all five indicators. In contrast, the performance of Armenia was unsatisfactory in all spheres except cooperation. This is the reason why Armenia only took the one hundred and eleventh place in the GCI, while neighbouring Georgia was in the eighth and Azerbaijan in the forty-eighth place (International 2017: 54).

Table 2: Global Cyber Security Index (GCI) 2017. CIS region scorecard[3]

	Legal measures	**Technical measures**	**Organi-sational measures**	**Capacity Building**	**Coopera-tion**	**GCI Score**
Armenia	Low	Low	Low	Low	Medium	Low (0,196)
Azerbaijan	Medium	High	Low	Medium	High	Medium (0,559)
Belarus	High	High	Medium	High	Medium	Medium (0,592)
Georgia	High	High	High	High	High	High (0,819)
Kazakhstan	Medium	High	Low	Low	Low	Low (0,352)
Moldova	Low	High	Medium	Low	Medium	Medium (0,418)
Russia	High	High	High	High	High	High (0,788)
Tajikistan	Medium	Low	Medium	Medium	Low	Low (0,292)
Turkmeni-stan	Medium	Low	Low	Low	Low	Low (0,133)

3 Available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

Ukraine	High	Low	Medium	Low	High	Medium (0,501)
Uzbekistan	Medium	Medium	Medium	Low	Low	Low (0,277)

In this study, the ITU also provided information on particular countries' experiences of applying specific solutions in order to advance their cyber security.

For example, with regard to the legal sphere the importance of having cybercrime legislation was highlighted as was the case in Columbia (one of the first countries to enact law targeting cyberspace), as well as Georgia, which established their cybercrime legislation in accordance with the Budapest Convention. Another key factor mentioned was the provision of cyber security training by the government.

Another important sphere was technical (with important dimensions such as the existence of special technical institutions, online protection of children, and so forth). Referring to examples of certain countries, it was shown that the existence of special computer emergency teams (for instance Egypt's G-CERT and Brazil's CERT) is essential to support the information technology sector and to help the latter to cope with cyber security threats. Significant importance was also attached to children's online protection.

Another sphere mentioned was organisational, implying (i) the development of a cyber security strategy (for instance the UK's National Cyber Security Strategy and Russia's adopted National Security Strategy); and (ii) the creation of a special coordinating agency by a government (for instance the Cyber Security Council of Iceland). In addition, special attention was given to specially-designed public awareness campaigns, as was the case in Latvia. A national portal named CERT has been created so that people can be provided with security solutions, for example, anti-viruses, which are free of charge. Moreover, the CERT is organising a bi-annual special campaign during which people can bring their laptops or computers to establish whether they have been infected.

Thus, if the experience of Armenia is evaluated through the prism of the afore-mentioned thought-provoking practices, it would become clear why it took only the one hundred and eleventh place on the list. Armenia has cybercrime legislation which is enacted through the Penal Code and Law on Electronic Communication, and specially-designed computer emergency response team- CERT-AM, but according to the wellness profile created by ITU (2014, 1–3) it lacks (i) an officially-approved cyber security framework necessary for the implementation of cyber security standards (which are internationally recognised); (ii) a national cyber security strategy and accordingly responsible agencies responsible for its implementation; (iii) sector-specific research and development programmes or projects; (iv) educational and/or professional training on cyber security; (v) partnerships that could have contributed to sharing of cyber security assets of either other states or the public sector (it is only the member of a special ITU-IMPACT initiative); and (vi) a special agency that could have provided institutional support on child online protection (even though Armenia has legislation on children's online protection. The latter is enacted through article 263 of the RA Criminal Code.

The aforementioned illustrates most of the major omissions. This should be rectified and a cyber security commitment should be demonstrated, especially given Armenia's historical-political context. What is at issue is the territorial conflict over Nagorno-Karabakh between two former Soviet countries, Armenia and Azerbaijan. This latter was also manifested in the form of an information war, leading to the dissemination of fake news, hate speeches, and even cyber-attacks which occurred in the winter of 2000 (Arminfo 2019). The attacks were from both sides – Azerbaijan hacked 30 Armenian websites and Armenia launched a counter-attack – and the damage was mutual.

Armenian cyber security expert Samvel Martirosyan also claimed that public facilities such as power stations, gas and water supply systems are becoming vulnerable since they can also be hacked. This is of substantial strategic importance especially due to their contribution to military efficiency/capability.

Martirosyan also stressed that in Armenia there is no special agency that can provide institutional support to solve these issues. This is why Armenia needs to create a special national agency – especially for monitoring and awareness-raising purposes – which already exists in neighbouring countries (Martirosyan 2018). Another important issue to be mentioned is that a special control should be established over crucial non-governmental organisation (NGO) structures such as banking (Arminfo 2019), since most of them are in the possession of foreign investors. The latter implies that some problems may arise not only because of a lack of accountability, but also due to of the influence of third countries.

Cyber security issues and the lack of media literacy contribute to the data leakage. People with poor media literacy tend to click on all the links that they receive through email, social media, or advertisements on different unreliable web pages. This leads to the hacking of social media accounts and control over personal user information, including bank account details. This tendency recently became relevant for the applications developed for smartphones. For example, an application called GetContact recently became very popular among Armenians and in the region itself. The application identifies telephone numbers by using the user's contact list, and it emerged that the application uncovers the caller's personal data and photo from its database (Kaspersky 2018).

Hence, referring to what was said above, it becomes extremely important for Armenia to provide institutional support for the development of cyberspace protection mechanisms in conformity with international cyber security and digital regulation practices to avoid threats to the state sovereignty and human rights protection.

3 The impact of new technologies on human rights: A case study of Belarus

This part presents peculiarities of the human rights situation in the Republic of Belarus reasoned by the geopolitical position of the state. It proceeds to explain the importance of new technologies and different sides of its impact on the fulfilment of human rights of Belarusian citizens. Finally, this part emphasises the main challenges and ways to overcome them.

3.1 New technologies and freedom of expression

The Republic of Belarus is a country located between the European Union (EU) and Russia. This geopolitical peculiarity explains many events occurring in the country: on the one hand, Belarus is influenced by Russia and, on the other hand, by the EU. Thus, the impact of Russia on Belarus results in substantially identical legislative provisions regarding the fulfilment of human rights, while the influence from the West is characterised by facilitated development of the new technologies in the country.

New technologies play an important role in the life of Belarusian society in both positive and negative ways. The positive impact consists of accelerating civil engagement, facilitating the communication of the state with civil society and human rights organisations, enhancing monitoring instruments.

Indeed, in recent years engagement of civil society in political life of the state has increased significantly: the Belarusian NGOs engaged in human rights protection regularly organise lectures, seminars and training in an effort to explain how people can protect themselves while using the internet and how to make a difference between a trustworthy information and fake news; a non-commercial platform, Petitions.by, raises awareness and involves millions of Belarusians in a dialog and cooperation with the authorities in a common effort to resolve local, regional and state-level problems. The involvement is carried out through writing, promoting and signing petitions to the relevant authorities with regard to persistent problems bothering citizens of particular districts or regions. At the same time, the Belarusian authorities apply new technologies in the process of governing to facilitate communication with the citizens and make an access to state services easier. Thus, Belarus has made it to the eighteenth position in the rating of countries with the best e-government services (Artezio 2000). Moreover, increased monitoring possibilities have a positive impact on the human rights situation in the state. Now it is possible to get reliable information not just from state entities – the National Statistical Committee of the Republic of Belarus, the National Academy of Science of the Republic of Belarus – but also from civil society as well as national and international human rights organisations that have elaborated their own monitoring systems. The abundance of statistical data allows the situation to be followed and excludes the possibility of even a minute change in the human rights fulfilment going unnoticed. Therefore, it is easy for human rights and civil society organisations to attract the attention of the Belarusian authorities as well as of the international community to problems prevailing in the Belarusian society and, consequently, to accelerate their elimination.

However, enhanced possibilities and easier access to statistical data and monitoring are not the only ways in which new technologies change the human rights status for the better. New technologies applied to the different spheres of society have a very positive impact on the state's economy through the creation of new working places, the increase of incomes via improvement of effectiveness and productivity, and the attraction of investments to the country. Economic growth inevitably leads to better living conditions of society and, consequently, a fuller enjoyment of human rights. A good example of such developments might be presented by the Belarusian Hi-Tech Park, which due to a special IT

environment attracts to Belarus numerous investments in line with dozens of foreign companies, start-ups and initiatives coming to register there every year and creating working places for the Belarusian people, and improving their quality of life.

This is evidence of the positive impact of new technologies on human rights fulfilment. However, reports of international organisations often emphasise overly restrictive legislative provisions on freedom of expression, peaceful assembly and association as well as on freedom of the press. They highlight the resilience of the government to the international pressure and its unwillingness to soften the legislative framework in relation to the freedom of expression and freedom of press/media sources (Human Rights Watch 2019).

Freedom House (2018b) has classified Belarus as 'not free' in both the Freedom of the Press and Freedom on the Net 2018 indexes. Such a low score is justified by facts of massive detention of journalists while fulfilling their professional duties, in particular, covering important, even though unfavoured by the authorities, civic and political events in the country. Even though a number of the detentions has decreased by two-thirds since 2017, it remains high (Table 3).

Table 3: Detentions of journalists in Belarus[4]

Year	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Ranking	20	30	167	60	54	29	19	13	101	31

Moreover, the government has adopted provisions that limit access of independent online media sources to official information and frequently induces them to employ self-censorship. This poses a serious problem for the fulfilment of the free flow of information. State-led media sources' coverage is insufficient and unbalanced, it mostly presents official versions of the events, which is roughly informative and does not provide any critical analysis. Thus, for example, the events of the 101st anniversary of the Belarusian People's Republic (BPR), which took place on 25 March 2019, were at least partly covered by the independent national media sources while state-run media barely mentioned the events of the day and did not present data on detentions of people and reasons of their detention – the use of the Belarusian historical flags and symbols. This means that many people, who do not regularly check online media sources but rather follow television news programmes, are unaware of what is happening in Belarus at the moment and, consequently, cannot make their informed position on the actions of government as well as those of citizens participating in civic and political activities in the country.

At the same time, in 2018 the authorities got arbitrary power to block media sources for a period of three months without a court decision for the alleged violation of restrictions on the press/media (Pravo.by 2003). Ever since there has been a degree of concern among the media, as the

4 Source: https://baj.by/en/analytics/repressions-against-journalists-belarus-2018-chart.

adoption of the Media Bill puts at risk every independent media source critical of the government. The legislative framework for the media enshrines a complicated procedure of registration and often discriminatory policies with regard to the independent resources. This often implies limited access to press briefings, government officials as well as less ability to distribute printed materials and higher costs for it (Pravo.by 2003). Moreover, journalists employed at the independent media or freelancing for international media are being detained while carrying out their duties during civil and political actions. Journalists and freelancers of international media sources face an acute problem, because the government frequently denies them accreditation and editorial certificates, putting them on the front line and leading to temporary imprisonment together with the confiscation of their equipment (Table 4).

Table 4: Fines to journalists under 22.9(2) of the Code of Administrative Violations[5]

Year	2014	2015	2016	2017	2018	04/2019
Ranking	10	28	10	69	118	14

Turning to the issue of digital freedom and security, the Belarusian government has imposed no permanent restrictions on connectivity or access to social media sources as well as communication applications. Nevertheless, the government has the ability to control the speed of internet connection due to the fact that only two entities are permitted to control connections within and outside the country – Beltelecom and National Centre for Traffic Exchange, both of which are controlled by the state. Therefore, the authorities not only control the speed of internet connection throughout the country but also monitor users' activities.

3.2 Regulation of the flow of information, digital security and freedom of speech

To understand the status of freedom of information, expression and digital security properly it is necessary to analyse how this field is being regulated. First, it should be noted that in the last few years the topics of freedom of expression, information and digital security have become very pressing and the authorities are working hard on the development of a legislative framework to regulate all activities in the sphere. Thus, in 2018 the Media Bill was revised (Pravo.by 2003), and drafted a new law on personal data protection (Forumpravo.by 2013), the adoption whereof is planned for the first half of this year. The national concept of information security was also adopted recently (President.gov.by 2019), that is the most important document providing a basis for the development of relevant legislative provisions and defining directions for the state policy.

In December 2018 the amendments to the Media Bill entered into force, raising concern in the Belarusian media sphere (Belarus.by 2009). The revised law stipulates the following:

5 Source: https://baj.by/en/content/article-229-code-administrative-violations.

- the obligation of owners of internet resources – bearing any of the national domains .BY or .БЕЛ – to identify its subscribers;
- compulsory pre-identification of the users to connect to public WiFi;
- the obligation of online media sources to register and obtain the official status of mass media resource in order to have access to the official information;
- the broadening of the list of prohibited information, which now became even more vague and open for interpretation for the authorities. In this light, it includes propaganda of unhealthy lifestyles, drug use, disrespect for different social, national, ethnic and religious groups, xenophobia, extremism, and so forth.

Moreover, the list of prohibited information is not fully presented in the Concept (President.gov.by 2019) or other legislative provisions. Several types of information are provided, but in the end it is always mentioned 'and other kinds of prohibited information stipulated in legislation of the Republic of Belarus'.

These provisions raised broad concerns in society, and particularly among the Belarusian online media sources, when they were first denounced. For the users such provisions inevitably imply a broader collection of users' personal data. This may be regarded as an infringement upon private life and freedom of expression of Belarusian internet subscribers. However, the state has a different perspective on the issue. By the identification and collection of users' data the state seeks to prevent cybercrimes and attacks and, thus, to protect society from prospective risks. It has been said that the state aims at ensuring the safety of collection, processing and storage of the users' data in order to protect their rights.

Turning to the provision on registration of online media, this was met by an even broader public discussion, because basically such provision enshrined the inequality of rights and access between state-led and independent online media sources, which even before faced numerous obstructions while doing their job and made it even easier for the state to prevent critical or objectionable independent media sources from registration by a complicated procedure of registration and a number of obstacles set in the process. Moreover, the broadened list of prohibited information and ability of the Ministry of Information of the Republic of Belarus to block websites for a period of three months without a court order poses a serious threat to all types of online resources. It is provided that one can be prosecuted for sharing false information, which is rather a vague expression and basically gives the authorities an opportunity to act based on their own interests, often not coinciding with the interests of society.

The most crucial document with regard to the information sphere regulation policy is the national concept of information security dated 18 March 2019. The concept (President.gov.by 2019) highlights an important role of IT technologies in the fulfilment of rights and freedoms of the Belarusian citizens and, at the same time, mentions the challenges to national security posed by the transition to the information society. The state reaffirms its commitment to develop effective and transparent system of governance and introduce ICT into the economic and social sectors and admits the digitisation of economy as the crucial aspect of formation of the information society. In line with that, the state emphasises its dedication to retain information sovereignty, which is not contrary to the

international principles of human rights protection, promotion and fulfilment. Information sovereignty is of paramount importance in light of the fulfilment of the strategy of national security in relation to the raising of awareness on issues such as fake news, cyber-terrorism, the imparting of false information aimed at stirring unrest among society and harming national interests and security. From this perspective, the state deems it necessary to promote critical attitudes toward information and activities that are disrespectful to the national customs, traditions, social morals, rights as well as to enhance intolerance to disinformation, information manipulations and attempts of psychological influence by the information means. In this light, the concept (President.gov.by 2019) underlines the necessity of an increase in the range and volume of the national media sources as well as their efficiency in the population. To support this statement the chart of the state budget expenses on the media development is provided in Table 5.

Table 5: State budget support to mass media in Belarus[6]

Year	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Funding	64 mln. EUR	40 mln. EUR	54 mln. EUR	45,5 mln. EUR	60 mln. EUR	52 mln. EUR	60 mln. EUR	45 mln. EUR	47 mln. EUR	48 mln. EUR	62 mln. EUR

From the chart it is clear that the state authorities are taking steps to satisfy the necessity mentioned above and improve the quality of the national media sources functioning. However, in reality the state's increased budgetary expenses do not constitute attempts at liberalising the national information space but rather implies a dedication to enhance control over it.

In addition, the Concept (President.gov.by 2019) underlines the special place of the information and digital security. The state goes to much trouble to prevent imparting untrue information able to harm the national interest and bring unrest to society by tightening control over the information space within the country and more extensive gathering of users' personal data. These measures reaffirm governmental control over media and other information sources and further decrease anonymity on the internet (Pravo.by 2003). However, at the same time the state confirms its efforts in developing effective instruments of digital security in Belarus and ensuring the safety of users' personal data from unsanctioned access.

Eventually, it may be concluded that the national concept of information security (President.gov.by 2019) can be considered as a thorough and balanced document reflecting the reality prevailing within Belarusian society. Nevertheless, the provisions with regard to the media may be considered overly repressive and in need of overhaul. The national as well as international independent media sources should be able to operate freely and with full access to the official information and freelancing journalists must not be prosecuted for acting in their

6 Source: https://baj.by/sites/default/files/analytics/files/smi-01572019-en.pdf.

professional field. This is an essential condition of fulfilment of the freedom of expression, which implies the freedom to receive information from various resources.

Therefore, the following challenges to the full and sustainable implementation of the freedom of expression might be highlighted:

- the extensive intrusion of the government into the functioning of the national media sources;
- the overregulation of the national information space.

In order to overcome these challenges, the government of the Republic of Belarus in cooperation with civil society has to implement the following recommendations:

- to increase activism of the national civil society and human rights NGOs;
- to make the government revise the system of regulation of the information space and media sources;
- to establish the monitoring and self-regulating mechanisms for media in order to identify infringements upon freedom of expression and eliminate them with minimum level of intrusion by the state.

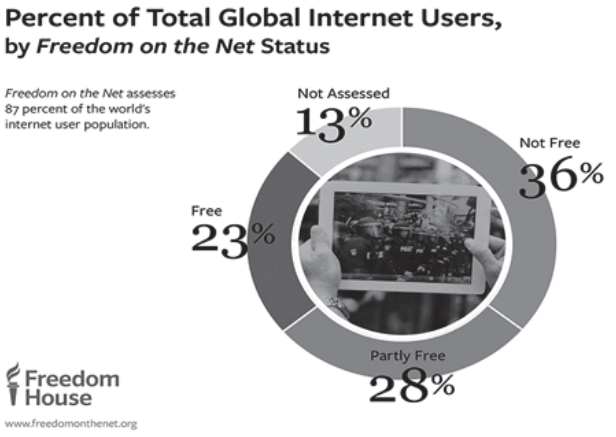
4 New technologies as a tool of protection of human rights: A case study of the Kyrgyz Republic

The case study of the Kyrgyz Republic is an analysis of the legislation, the government electronic services, and the main challenges for the state in the era of global automation. The conclusion of this part recommends the necessary actions to respect, protect and fulfil human rights through new technologies.

4.1 Analysis of national legislation and human rights protection mechanisms in digital space

Kyrgyzstan is a mountainous country in Central Asia with a population of 6 389 500 people as of 1 January 2019. According to the Freedom House Freedom on Net 2018 report Kyrgyzstan is among 28 per cent of countries with partially free internet (Image 1). Kyrgyzstan has 38\100 points in contrast to the neighbouring countries in Central Asia such as Kazakhstan (62\100) and Uzbekistan (75\100), which are among 36 per cent of countries in the category 'Not Free' (Freedom House 2018 (a)).

Image 1: Percentage of total internet users by Freedom on the Net Status



Kyrgyzstan is a developing country. Although digital processes are only beginning to gain momentum, the country aims to move towards becoming a more digital space. To improve the quality of the life of citizens, and to build an open and transparent state, a National Sustainable Development Strategy has been developed, a key component of which is the 'Taza Koom' digital transformation programme. The official launch year was 2016. Since then, it has become clear that the country was not ready for large-scale digital changes. There was no prepared platform and digital infrastructure. Digital infrastructure in Kyrgyzstan is at the medium level. Kyrgyzstan is rapidly increasing the consumption of internet services, especially of international content. However, the quality of telecom-munications and ICT is a major factor in relation to capacity of regional transit bandwidth, independence of national networks, and e-government infrastructure (National 2017).

The legislative level has limited power to regulate the digital environment. The state does not recognise the relations that are exercised in the digital space, making a connection with existing laws and referring to regular and well-known topics and articles in legislation. The Constitution of the Kyrgyz Republic enshrines fundamental rights such as the right to privacy; the protection of honour and dignity; the right to privacy of correspondence (article 29); the right to freedom of thought and opinion (article 31); and the right to freedom of conscience and religion (article 33).

The level of freedom of information is an important criterion in determining the country's compliance with democratic norms. Based on the Constitution the country has various laws related to information. A vivid example of the weak level of regulatory compliance of digital modernisation is the 'Law of the Kyrgyz Republic on guarantees and ways to access information'. This Law regulates the relations that arise in the exercise of the right to freely search, receive, research and produce, transfer and disseminate information, but it is worth noting that this Law

lacks concepts such as internet, digital environment, social networks, and so forth.

Internet resources are not officially recognised media in Kyrgyzstan, but they nevertheless feature in various lawsuits. Jogorku Kenesh (the official name of the country's Parliament) has repeatedly tried to raise the issue of Bills regulating the internet space. It is worth noting that these Bills contain rules that can cause restrictions on freedom of speech on the internet.

The mechanisms for the protection of human rights in the digital environment are not clearly defined. The main elements are written laws and the judicial system. The lack of clear concepts of human rights in the digital environment allows to adjust the letter of the law to the desired meaning. For example, the government agencies by citing anti-extremist law block websites, blogs, and music applications (Freedom House 2018 (A)).

The legislation contains the basics for digitalisation, but remains fragmented and not fully applied. To ensure the protection of rights and freedoms, the Law on the Protection and Use of Personal Data was adopted. Thus, the law equates information on electronic media to paper documents, various electronic transactions to physical transactions, electronic documents and certificates to physical documents, and digital signature to a physical signature.

For the protection of human rights in the digital sphere it is important that the mechanisms could be used. Significant challenges to the implementation of rights are out-dated rules and regulations, gaps in the country's legislation governing the ICT sector, the lack of reliable information and digital infrastructure, as well as weak guarantees in protecting electronic payments, open data and the exchange of personal data.

4.2 The concept of information security in the Kyrgyz Republic: International and regional cooperation

The concept of national security of the Kyrgyz Republic is a system of attitudes, ideas and principles for the protection of individuals, society and the state from external and internal threats to security in all spheres of life. Modern realities prioritise on the concept of security. In this regard information security is one of the most important elements of the concept. According to the Cyber Security Index 2017, Kyrgyzstan ranks 97 out of 180 countries (International 2017).

The Law of the Kyrgyz Republic on Personal Information contains an article on the obligation to provide data transmission via the internet with the necessary means of protection, while maintaining confidentiality of information. Personal data protection should be a priority item in the security concept. At present there is no concept of cybercrime in the law. Government agencies are the main holders of all personal information of citizens. Therefore, they should act as guarantors of the complete protection and security of the personal data. In recent years Kyrgyzstan has witnessed a significant increase in the number of cyber-attacks targeting public and private systems. In 2016 hackers cracked two government agencies: the official website of the State National Security

Committee and the official website of the State Committee on Defense Affairs (Kabar 2016). The hacking of two main bodies that protect personal data indicates weak digital security (Global 2017). The regulatory framework for information security is represented in Kyrgyzstan by documents such as the Constitution of the Kyrgyz Republic, the Civil Code, the Concept of National Security and other laws regulating the security sphere. The country has also developed a Cyber Security Strategy of Kyrgyz Republic 2018-2023. The Cyber Security Strategy was developed with the aim of creating a unified state policy to counter threats in cyberspace and improve the national system of protection of information. The Strategy also confirms the existing gaps in the legislative system and the absence of a cyber security policy.

International cooperation is a significant criterion for the development of states. Joint work aimed at improving human rights and ensuring safe livelihoods has an effect only if there is fruitful work by all states.

As a member country of the Eurasian Economic Union (EAEU), Kyrgyzstan contributes to the improvement of the overall digital space together with neighbouring Kazakhstan, Russia, Armenia and Belarus. The common economic space is not limited to economic relations; the member countries develop their relations in all spheres, one of which is security. Modern challenges render information security in the common space of paramount importance.

EAEU has identified a developmental path related to digital transformation and has developed a Digital Agenda for the implementation period until 2025. To create a durable and secure digital space it is important to develop institutional and legal frameworks. The EAEU Digital Agenda has as its main objective the creation of a safe and independent digital space and the development of the Digital Economy. The transition to a new technical structure taking into account national interests is focused on improving the quality of public services and creating a favourable environment for the development of innovations. While implementing the Digital Agenda, countries may be under a number of security threats, various risks including the loss of digital sovereignty, the emergence of influence and control on national digital space by external players, or the implementation of destructive cyber threats that can be a threat to personal data of states. The cooperation of the participating countries should be based on a coordinated policy of digital transformation. The relationship mechanism should include an open platform for mutual coordination, stimulation and support. The main policy and activity of the EAEU is aimed at the economic component but at the same time the human rights factor is included. The main benefits for human rights in the digital space of the EAEU is that it will serve to improve national digital systems by establishing a common security policy and assist in countering cyber-attacks so as to protect the privacy of citizens and advance economic development.

However, it remains unclear whether participating countries should have a similar legal framework with respect to internet freedom. For example, on 22 March 2019 the President of the Russian Federation introduced the concept of Digital Rights into the Civil Code of the Russian Federation. Does this mean that for equal regulation, member states must have identical laws? Also in the legislation of the Russian Federation there is a Concept for Information Security of Children adopted by a

government decree. On 24 February 2019, the draft law 'On protection of children from information harmful to their health or development' was placed on the official website of the Jogorku Kenesh for public discussion. Public Foundation Legal Clinic 'Adilet' conducted a legal analysis and came to the conclusion that the law contains a number of provisions that carry certain risks to the democratic values of the rule of law including the respect for the observance of the right to freedom of opinion and expression (Public Foundation 2019).

In addition to being a member of the EAEU, the Kyrgyz Republic is also a member of various regional organisations such as the Organisation for Security and Co-operation in Europe (OSCE), the Commonwealth of Independent States (CIS), Shanghai Cooperation Organisation (SCO), and Collective Security Treaty Organisation (CSTO). Each of these structures has developed its own policy aimed at the development of the digital space and the protection of human rights. The main criterion for evaluating the activities of an organisation and unions in this article is the presence of the implementation of the protection of human rights in the digital environment in the activities of the above mentioned organisations.

As the largest security organisation, the OSCE pays special attention to countering cyber threats and ICT security coming from non-state institutions such as organised criminal groups and terrorists, but also provides the basis for preventing states from encroaching on digital sovereignty. Conflicts between states that may arise from the use of ICT can cause a problem. In this regard OSCE member states are working on confidence-building measures.

The confidence-building measures are designed to make cyberspace more predictable and open in this regard to provide important mechanisms, such as: information openness, including discussions of a possible or existing conflict with further escalation, an educational platform, including various educational activities to exchange views, strategies and projects, a security policy that includes collective measures to protect the digital infrastructure, which will contribute to improving the cyber security resilience (Organisation 2016).

There are also other examples of regional cooperation that develop the digital space in different areas:

(1) The activities of the CIS include the provision of digital integration, the development of a digital economy and the provision of cybersecurity. CIS member states are working on a cybersecurity agreement that will facilitate the rapid exchange of information on new types of information technology crimes, also study digital security threats and propose measures to prevent and curb them.

(2) The policy of the SCO is aimed at the benefit of the economic and social development of the participating countries. The SCO also covers the digital agenda and carries out its activities related to the development of cooperation, the exchange of information and the transfer of ICT practices. The SCO also considers issues of digital security, interacting in the fight against the proliferation of various crimes, such as terrorism through the internet.

(3) The CSTO as a military-political bloc carries out its activities directly related to security. The CSTO aims to unite efforts to combat cybercrime, also to create a system of information security and strengthen inter-agency cooperation.

4.3 Development of digital technologies and e-governance in Kyrgyz Republic

Since 2016 Kyrgyzstan has started implementing a Sustainable Development Strategy. Since the beginning of 2018 Kyrgyzstan began to officially launch programmes for the digitalisation of public services. The cardinal change of the state system was met with great optimism of citizens. E-government projects are aimed at increasing state efficiency and counteracting the development of corruption. Examples of different implemented projects include various portals of state agencies, e-visa, e-trading platform, automated border control system e-gates, electronic notaries, and electronic patents.

A bright and successful project that improves the livelihoods of citizens is the system Tunduk. Tunduk is a system of electronic interaction in which ministries, departments, state enterprises, municipal authorities and other organisations (legal entities and individuals) exchange information with each other directly at the machine level. It is important to note its legal value:

- Any transaction passing through the Tunduk platform is automatically signed and becomes a document (certificate, report, information).
- Each state body has its transaction history.
- The transaction is officially signed and it can be used in court as a legal document.
- Any government agency is always aware about a transaction.
- It is impossible to create a fake document as it is automatically created.

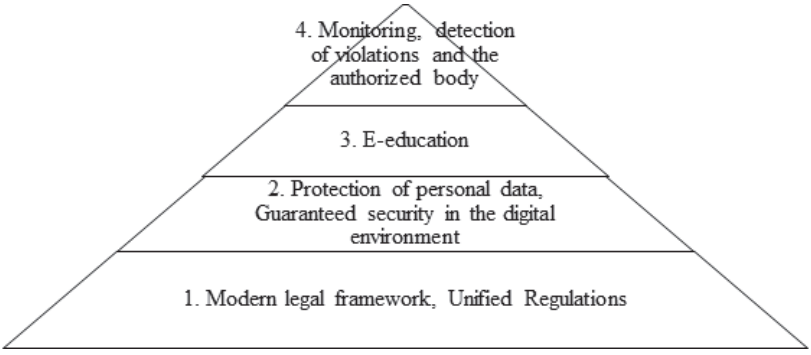
The Tunduk system is based on world practice, namely, the Estonian X-road system. According to specialists the Estonian system allows to save up to €1 billion per year. According to international experts Tunduk will allow the budget to save up to $300 million per year.

The Tunduk system has as its goal the coverage of a large number of state bodies. At this stage it is possible to identify positive changes in the implementation of E-Gov systems, such as improving the work of state bodies, making public administration more efficient, exchanging information directly, which will reduce the number of illegal documents, and reducing corruption.

4.4 Development of new technologies and protection of human rights: What is next?

To ensure the sustainable presence of human rights in new technologies states are obliged to develop a unified standard for the gradual introduction of the protective mechanism of human rights in the digital environment (Image 3).

Image 2: The pyramid of necessary actions to achieve the sustainability of the presence of human rights in the new technologies



1 Modern legal framework, Unified Regulations

Laws that clearly regulate the protection of human rights in the digital environment are required to guarantee the recognition of human rights in the digital environment. Legislation needs to conduct a timely analysis of new digital space challenges. Laws should have the same rules in relation to online and offline rights. Laws should not be duplicated, thereby creating fields for legal gaps helping to avoid legal liability for human rights violations in the digital environment. It is also important to create a sustainable regulatory system from cyber threats. The legal framework should include NGOs, civil society organisations, citizens, and so forth. By involving society forces it can be ensured that the framework does not limit freedom but instead protects human rights.

2 Protection of personal data, guaranteed security in the digital environment

Security is an important component in ensuring the protection of human rights in the digital environment. The state must guarantee the enjoyment of human rights in the digital space. The state should provide guaranteed protection of personal data. Need to develop international and regional relations to develop ways to protect cyberspace and improve cyber security.

3 E-education

Education is one of the main key components of digital processes. Standards for educational activities and educational regulations should include disciplines that teach important skills, such as digital literacy and digital skills, cyber security, human rights in the digital environment, lessons on the right use of E-Gov services, computer hygiene and other items that will contribute to the safe and proper use of digital services. It is important to introduce important principles through digital processes, highlight human rights and freedoms, contribute to the achievement of the UN SDGs, and so forth.

The example of Estonian digital revolution started in 1996 with the state programme Tiger Leap. This programme was focused on implementing technology education and technology infrastructure at schools.

E-education is an essential part of state development. The educational component of digitalisation must necessarily include projects and research in the field of digital development, information campaigns to reduce digital inequality among citizens and the development of digital censorship and etiquette. An example of a working education mechanism is the Digital Rights School in Kyrgyzstan, which includes in its activities new technologies and digital human rights. E-skills become mandatory selection criteria when applying for a job. Lack of technological skills contributes to increasing the inequality gap (The World Bank Group 2016).

4 Monitoring, detection of violations and the authorised body

A component of creating a regulatory framework focused on the digital environment is the creation of a working mechanism, the body authorised to monitor and detect human rights violations in the digital environment. A competent authority is necessary to conduct surveys, focus groups and monitoring in order to identify the causes of inequality, improve access for all categories of citizens, improve the regulatory framework, and identify weaknesses.

5 Conclusions and recommendations

This article explores the dualistic nature of ICT in a way they affect the processes occurring in the world. Based on the case studies of three former CIS countries, it was found that new technologies can significantly contribute to the fulfilment of human rights, and in this process, one of the key roles is assigned to civil society that can properly use those technologies for the achievement of democratic goals. The vivid example of the latter is the digital activism in Armenia that helped different civil society organisations to reach a wider audience and awaken the politicised identity of the major part of the population. Digital activism played a decisive role in mobilising masses and making them exercise their civil and political rights during the Armenian Velvet Revolution. However, in this case one of the challenges that CSOs may encounter on their way is the abuse of state power. Both in Belarus and Kyrgyzstan the states act as opponents for the civil society in the implementation of various activities, thereby infringing on many crucial human rights that citizens should enjoy. Therefore, what has to be done in this case is bringing the authorities and civil society to a dialogue in order to overcome the problem of extensive regulation of all the spheres of society and ensuring the best conditions for the development of a scientifically-progressive digital state.

Another major finding in this article was that the transition towards technologies may have negative impacts such as a lack of control on the content shared online, risk of being subjected to cyberbullying and so forth. Despite the fact that the social media platforms have security measures, a gap remains that allows disinformation to be spread

throughout the world. Another factor leading to the indirect negative impact of new technologies is the lack of media literacy of the wider public. Indeed, it is not the fault of new technologies, rather of the low media literacy level, that the media are being used to manipulate people through new technologies.

Thus, it can be said that as any coin new technologies have two sides: *Tails*, for example, may show how new technologies contribute to the freedom of expression and freedom of speech of people; and *heads* may show how the former may also contribute to the spreading of hatred, discrimination, and cyber bullying.

However, relying on the case studies of Armenia, Belarus, and the Kyrgyz Republic it may said that the overall sustainable and effective implementation of human rights in the context of rapid integration of new technologies requires the combination of the efforts and responsible approaches of individuals, commercial organisations, civil society, states and international organisations. Comprehensive programmes and individual decisions in the field of the protection and implementation of human rights can provide for the inclusion of a complex mechanism, the key components of which are the political will, a strong legal framework, the presence of relevant institutions, infrastructure and technical environment.

References

Arminfo (2019) *Samvel Martirosyan: Cyber security of Armenia and Azerbaijan is vulnerable,* available at https://arminfo.info/full_news.php?id=39061&lang=3 (last visited 1 April 2019)

Artezio 2000 'Belarus among top 20 countries with the best e-government services' 7 February 2018, available at https://www.artezio.com/pressroom/blog/belarus-among-top-20-countries-best-e-government-services (last visited 27 February 2019)

BAJ 2008 'Repressions against journalists in Belarus, 2018 (chart) 5 September 2018, Belarusian Association of Journalists, available at https://baj.by/en/analytics/repressions-against-journalists-belarus-2018-chart (last visited 3 March 2019)

Belarus.by 2009 'Changes to the law about media sources came into force 1 December 2018', available at https://www.belarus.by/ru/government/documents/osnovnye-izmenenija-v-zakon-o-smi-vstupili-v-silu_i_0000092147.html (last visited 19 March 2019)

Eurasian Economic Union EAEU, World Bank 2017, *EAEU Digital Agenda 2025: prospects and recommendations*, available at http://www.eurasiancommission.org/ru/act/dmi/SiteAssets/2017.10.04%20%E2%80%93%20EAES_A3fold_ENG_PRINT.pdf (last visited 21 March 2019)

European Forum for Democracy and Solidarity *Armenia's portfolio* 2018, available at https://www.europeanforum.net/uploads/countries/pdf/armenia.pdf (last visited 14 February 2019)

Fact Investigation Platform 2018 'Vahe Enfiajyan and the army of fake Facebook users from the Prosperous Armenia Party', available at https://fip.am/en/5378 (last visited 8 April 2019)

Forumpravo.by 2013 'The Law of the Republic of Belarus about personal data' nd, available at http://forumpravo.by/files/proekt_zakona_o_personalnih_dannih.pdf (last visited 3 March 2019)

Freedom House 2018(a) 'Freedom on net 2018 nd, available at https://freedomhouse.org/report/freedom-net/2018/kyrgyzstan (last visited 28 April 2019)

Freedom House 2018(b) 'Freedom on the Net 2018' nd, available at https://freedomhouse.org/report/freedom-net/2018/belarus (last visited 25 March 2019)

Freedom House 2018(c) 'Freedom on the Net 2018' nd, available at https://freedomhouse.org/report/freedom-net/2018/armenia (last visited 15 June 2019)

Global Cyber Security Capacity Centre 2017 'Cyber Security Capacity Review – Kyrgyz Republic', available at https://www.sbs.ox.ac.uk/cybersecuritycapacity/system/files/CMM_Kyrgyzstan%20Report%20final_execsummary_1701030.pdf (last visited 20 February2019)

Human Rights Watch 2019 "Belarus. Events of 2018' nd, available at https://www.hrw.org/world-report/2019/country-chapters/belarus (last visited 5 March 2019)

International Telecommunication Union 2017 'Global Cybersecurity Index', available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (last visited 1 April 2019)

IREX 2018 'Media Sustainability Index 2018: The development of sustainable independent media in Europe and Eurasia' available at https://www.irex.org/sites/default/files/pdf/media-sustainability-index-europe-eurasia-218-full.pdf (last visited 8 April 2019)

Kabar 2016 'Kyrgyz security service website hacked', available at http://old.kabar.kg/eng/society/full/16534 (last visited 15 April 2019)

Kaspersky Daily 2018 'GetContact: Find a contact or give your contacts away?' available at https://www.kaspersky.com/blog/getcontact-collects-personal-data/21453/ (last visited 8 April 2019)

Freedom of Information Centre of Armenia 2011 'Law of the Republic of Armenia on Protection of Personal Data 2015', available at http://www.foi.am/u_files/file/Personaldataprotectionlaw_ENG.pdf (last visited 8 April 2019)

National Institute for Strategic Studies of the Kyrgyz Republic 2017 'Digital development assessment – Kyrgyzstan, available at http://www.ict.gov.kg/uploads/ckfinder/files/KG_Digital%20Development%20Assessment_Final.pdf (last visited 15 March2019)

Organisation for Security and Co-operation in Europe Permanent Council 2016 *Decision No 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from Use of Information and Communication Technologies*, available at https://www.osce.org/pc/227281?download=true (last visited 25 March 2019)

Pravo.by 2003 'The Law of the Republic of Belarus "About the media sources"' 17 July 2008, available at http://pravo.by/document/?guid=3871&p0=H10800427 (last visited 8 March 2019)

President.gov.by 2019 'Directive of the Security Council of the Republic of Belarus' 18 March 2019, available at http://president.gov.by/uploads/documents/2019/1post.pdf (last visited 18 March 2019)

Public Foundation Legal Clinic "Adilet" 2019, Analysis of the concept of the draft law of the Kyrgyz Republic "On the Protection of Children from Information Harmful to their Health or Development", available at http://www.adilet.kg/ru/news/full/368?fbclid=IwAR1tqz9v4_IqJWX6iwKZxAlSfc6_yKX-DkuNmBtIACoG6jhGDGLtwxOZ7fE (last visited 10 March 2019)

Shubladze R 'Armenian snap elections seen as the final chapter of the Velvet Revolution' 2018, available at https://europeelects.eu/2018/12/04/armenian-snap-elections-seen-as-the-final-chapter-of-he-velvet-revolution/ (last visited 1 April 2019)

The World Bank Group 2016 'Digital Development Report 2016. Digital Dividends', available at http://pubdocs.worldbank.org/en/961361455690144451/Presentation-WDR2016-Overview-Zahid-Hasnain-en.pdf (last visited 23 March 2019)

United Nations Office on Drugs and Crime 2019 'Criminal Code of the Republic of Armenia 2003', available at https://www.unodc.org/res/cld/document/armenia_criminal_code_html/Armenia_Criminal_Code_of_the_Republic_of_Armenia_2009.pdf (last visited 14 March 2019)