A Jovanović, E Kanlić, D Savić, G Stanić & K Ćendić 'Online assemblies between freedom and order: Practices in South-East Europe' (2019) 3 *Global Campus Human Rights Journal* 210-228
http://dx.doi.org/10.25330/481

Online assemblies between freedom and order: Practices in South-East Europe

Andrea Jovanović, Edo Kanlić,** David Savić,*** Goran Stanić,**** and Kristina Ćendić*****†*

Abstract: *This article approaches the question of whose interests the internet serves through the prism of online assemblies in the South-East Europe (SEE) region. In order to answer this question, the article uses four connected yet different angles. The first part explores opportunities and limitations of international laws, as well as national laws in the SEE region. Furthermore, the article discusses the role of the state in providing and facilitating access to the internet, that is, enabling the space for online assemblies in the SEE region. The article takes into account the variety of actors in the field of freedom of expression and freedom of assembly online, paying special attention to internet service providers. Finally, the article analyses the surveillance of the internet activities and security and its relation with online and offline assemblies. The article uses all four these aspects to explore the situations in the SEE region. The article specifically focuses on four countries, namely, three former Yugoslav republics: Croatia – a European Union member since 2013; Serbia – a candidate country exercising control over the internet the most; Bosnia and Herzegovina – a country aspiring to become a candidate but in which progress is burdened by divisions and legacy of the war; and Turkey, which has one of the most illustrative examples of stifling freedom of expression and assembly, and the influence of which on the Balkans is also visible.*

Key words: *online assemblies; South-East Europe; freedom of assembly; freedom of expression*

1 Introduction

Freedom of expression is one of the pillars of democracy and therefore it is important to emphasise a high level of interplay between this right and other human rights. Freedom of expression not only is a constitutive right, but also an instrumental one, which is why its 'interaction with a number of other rights vouchsafed by international human rights law is notably dynamic' and it 'generates enhanced understandings and applications of the rights in question' (McGonagle 2011). 'The suggested

* 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. BA (Philosophy); aerdna.1112@gmail.com
** MA (Democracy and Human Rights); edo.kanlic@gmail.com
*** MA (Democracy and Human Rights); david.savic@live.com
**** MA (Democracy and Human Rights, Theology and Religion); gost93@gmail.com
***** PhD (Communication Studies); kristina.cendic@gmail.com
† We wish to extend a special acknowledgment to Nina Belyaeva – Professor, Department Head; National Research University "Higher School of Economics" (HSE); nbelyaeva@hse.ru

principle that the government can simply ignore rights to speak when life and property are in question so long as the impact of speech on these other rights remains speculative and marginal it must look elsewhere for levers to pull.' The article explores the interaction between the right to freedom of expression and the right to assembly in South-East Europe and focuses on the online sphere and the exercise of the two rights on the internet.

The article approaches the question of whose interests the internet serves through the prism of online assemblies in the South-East Europe (SEE) region. In order to answer this question, the article uses four connected yet different angles. The first part explores opportunities and limitations of international laws, as well as national laws in the SEE region. Furthermore, the article discusses the role of the state in providing and facilitating access to the internet, that is, enabling the space for online assemblies in the SEE region. The article takes into account the variety of actors in the field of freedom of expression and freedom of assembly online, paying special attention to internet service providers. Finally, the article analyses the surveillance of the internet activities and security and its relation with online and offline assemblies. The article uses all four these aspects to explore the situations in the SEE region. The article specifically focuses on four countries, namely, three former Yugoslav republics: Croatia – a European Union (EU) member since 2013; Serbia – a candidate country exercising control over the internet the most; Bosnia and Herzegovina – a country aspiring to become a candidate but in which progress is burdened by divisions and legacy of the war; and Turkey, which has one of the most illustrative examples of stifling freedom of expression and assembly, and the influence of which on the Balkans is also visible.

2 Theoretical and legal considerations related to online assemblies and freedom of expression

2.1 The level of recognition of 'online rights'

If the policy makers were to define the right to an online assembly under the Universal Declaration of Human Rights (Universal Declaration 1948), they would have to face rigorous precision requirements set by Eleanor Roosevelt (Fazzi 2017). In addition, under article 31 of Vienna Convention on Law of Treaties (VCLT 1980), the context and the meaning of any international treaty has to be understood in a very clear context by the parties, when it comes to the implementation and interpretation of the Treaty (VCLT 1980). As of now, there is no clear definition on what exactly the right to an online assembly is in legal or social context. Therefore, we must ask how we define the right to an online assembly and the position of the citizens towards this right, and what the role played by the state would be in such predicament. In order to answer this question, this article will define the right to an online assembly by combining the already-existing theoretical and legal frameworks. Under such conditions, the hypothesis is that the internet could be approached as a form of a virtual public space, which allows groups of people to freely express their ideas and opinions, and to be able to form an assembly within the virtual public space.

In the book *Negotiating digital citizenship*' the authors define the internet as an epoch which has the potential to create a new form of relation between the citizens and the states (McCosker, Vivienne & Johns 2016). However, this relationship of the internet has to be 'characterised by openness, sharedness and free exchange' (McCosker, Vivienne & Johns 2016). Such characterisation of the internet very closely resembles the guarantee of the right to freedom of opinion and expression, which has been enshrined in article 19 of the Universal Declaration (1948). In order to exercise these rights, the citizens may 'receive and impart information and ideas through any media and regardless of frontiers' (Universal Declaration 1948). The internet may be seen as a platform which disseminates information and ideas, while it disregards obstacles of national borders. The European Convention on Human Rights (European Convention) safeguards freedom of expression in its article 10. In addition, the European Court and European Commission of Human Rights described freedom of expression as 'one of the basic conditions for the progress of democratic societies and for the development of each individual'. The European Court gives a wide interpretation to article 10, and one of the landmark statements is found in the case of *Handyside v United Kingdom*[1] where the Court said that the scope of freedom of expression is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also those that offend, shock or disturb the state or any sector of the population.[2] What is clear from *Handyside v United Kingdom* is that it is expected of states to give the broadest possible interpretation to freedom of expression, in the interests of promoting democratic values. The Court has interpreted freedom of expression to cover all forms of expression and it extends to all forms of opinions and views, approaching the restrictions of freedom of expression given in article 10(2) only in exceptional cases.

In order to engage in the public debate in which the citizens can freely express their ideas and opinions, a form of public space has to be provided. Habermas in his book *The structural transformation of the public sphere* has coined a term 'the public sphere,' by which he defines a zone where free discussion between the citizens and the state may take place (Habermas 1991). The setting of the public sphere is crucial for a modern and democratic society, as such practice serves the citizens to publicly criticise the state and, by doing so, to shape a narrative which is closely related to the citizens (Habermas 1991). Additionally, an open discussion within the public sphere 'refers to an attitude toward social cooperation, that of openness to persuasion by reasons referring to the claims of others as well as one's own' (Habermas 2003). Following the Habermasian line of thought, the internet may be seen as a form of the virtual public sphere, as social media, blogs and other types of forums allowed the citizens to freely and publicly express their views online, where their voices can be seen. The United Nations (UN) 2030 Agenda for Sustainable Development also recognises that the 'spread of information and communications technology and global interconnectedness has great potential to accelerate human progress' (Sustainable Development 2018). Therefore, through the internet

1 *Handyside v United Kingdom* App 5493/72 ECHR, 7 December 1976 para 49.
2 Freedom of Expression Under the European Convention on Human Rights article 10, Interights manual for lawyers, current as at October 2009.

citizens and states can collaborate together and benefit from open discussion, which should create modern democratic societies.

The crucial element to an open discussion are the citizens. Their voices are part of the productive and civil practice, which allows their participation that may be exercised online (McCosker, Vivienne & Johns 2016). However, the participation usually coincides with the action of particular groups of citizens. In the real world, the groups of citizens often opt for the creation of assembly, which is their guaranteed right according to article 20 of the Universal Declaration. The assembly may be defined as a 'temporary presence of a number of individuals in a public place for a common expressive purpose' (OSCE/ODIHR 2010). This particular definition of assembly may easily be transferred to an online public sphere. The participation and the expressive purpose of an assembly is far easier to be created online today than it is in the real world. The citizens, at least in the developed parts of the world, have an unprecedented access to a public sphere such as the internet, where they can interconnect extremely fast with other individuals or groups. Such connectivity would allow real-time interventions and innovative forms of collaboration (Soh, Connolly & Nam 2018).

Therefore, we may conclude that the right to online assembly should be finally defined, as a guaranteed right to form an assembly in any form or shape on the internet, which is a form of virtual public space. Such civil practice would allow citizens to freely participate and express their purposes and opinions, with the minimum intervention by the state or any other actor. However, the main aspect of an online assembly has to be focused on the peacefulness and the safety of assemblies, which should be a positive obligation that requires public authorities to take action. What is necessary to discuss further in depth is the role of the state and the role of the private sector, which in this case would be the owners of internet service providers. As the right to online assembly is not defined by the international legal system, there currently is a lot of space for ambiguity and uncertainty. This is especially problematic nowadays, since states and the private sector are starting to exert increasing control over the online spaces, under the excuse that they are obliged to provide peace and safety for internet users, hence the citizens. In the next few chapters we will examine to what extent states and internet service providers are primarily ensuring the safety of their citizens, or whether they are overstepping their boundaries by exerting excessive control, which may be harmful for freedom of expression and democratic values.

2.2 The role of the state to provide/facilitate internet access

Among obligations that nation states have as core actors in international politics, they also play a crucial role in providing and facilitating access to the internet for their nationals. Answers to the question of how much states should be involved in facilitating and regulating internet access vary from Hobbes's controlling monster state to Bakunin's vision of collectivist anarchy (Herold 2008). There are those who see the internet as the last truly free place, while some see it as a lawless sphere. Governments of developed states have been focused largely on creating the conceptualised international settings of the internet. States' obligations regarding the internet were mainly agreed and defined through international organisations, with the UN bodies who were pioneers in that field.

In order to understand the process of states' involvement in providing and facilitating internet access, it is necessary to overview the role that the internet plays regarding the implementation of some human rights. The UN Human Rights Committee (UNHRC) has called on states to ensure access of individuals and to foster the independence of the internet, which is interpreted as a new trend in technologies (General Comment 34 Article 19: Freedoms of opinion and expression 2011) through which freedom of opinion and expression (Universal Declaration 1948) can be implemented without interference. According to the Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, the internet is seen as an 'enabler' or catalyst for individuals to exercise their rights, such as the right to education of the right to take part in cultural life, as well as the rights to freedom of association and assembly (La Rue 2011). According to all relevant documents regarding the internet, all the rights individuals have offline must also be protected online, in particular freedom of expression.

Investing in information and communication technologies is one of the Sustainable Development Goals accepted by the all member states of the UN and the internet is perceived as a booster of economy and development of individuals and states (Blazhevska 2017). However, having well-being as one of the significant factors that determines who can access information communications technologies, the internet is likely to be concentrated among socio-economic elites in countries where internet penetration is low (La Rue 2011). This means that by providing and facilitating internet access, states should have in mind the costs this produces, therefore becoming an obstacle in broader internet consumption.

When examining states' approaches in providing and facilitating internet, before the mid-2000s policy makers were mostly focused on infrastructure, and by that time at least 70 per cent of the world's population lived within the range of a mobile internet signal, which makes that process successful (Internet Access for All 2016). Internet Society, an American non-profit organisation founded to provide an organisational home and financial support for the internet standards process, provides policy principles for expanding access infrastructure. Some of the most important principles are the removal of barriers to investment and competition; the creation of transparent and affordable licensing processes; collaboration with neighbouring governments in order to harmonise and coordinate regional cross-border interconnection and licensing regimes; and avoiding burdensome taxes on end-user services (Internet Access for All 2016).

The role of states in providing and facilitating internet access also includes the usage of their power concerning possible restrictions in that field. In the era of globalised fear and securitisation of politics, nation states use national laws to interpret restrictions on the internet more strictly than is the case with rather vague international norms. Article 19 of the International Covenant on Civil and Political Rights (ICCPR) states that everyone has the right to hold opinions without interference and the right to freedom of expression (OHCHR International Covenant on Civil and Political Rights 1966). Nevertheless, this article recognises certain restrictions regarding freedom of expression, which should be provided by law and are necessary for respect for the rights or reputations of others; for the protection of national security, public order, public health or morals.

These provisions gave an open door to states to interpret given exceptions in different ways through their national laws, including cutting off access to the internet entirely. The UN Special Rapporteur considers this practice disproportionate and a violation of article 19, regardless of the justification provided, including times of political unrest or even war (La Rue 2011). Practice in the states of South-East Europe shows how these states are mostly focused on control of the internet, through various forms of restrictions, rather than on infrastructure that is on a very low level compared to the other regions in Europe. This issue will be discussed more in detail in the next part.

2.3 Online as a 'space for assembly'

From the very beginning the internet was regarded as a free and inclusive space with the intention of becoming available to everyone. The period of the 1960s to the 1980s was marked by a collective spirit shared by computer scientists, professionals and others involved in the internet development. They saw it as a communal space for an 'open and non-hierarchical' culture. On the other hand, the internet also had a very anti-commercial character. This changed during the 1990s when, in the words of McChesney, the internet was transformed from a public to a 'capitalist sector' (McChesney 2013). Formally privatising the internet left it open to mysterious and non-transparent market forces, and its goals and course changed accordingly. While this process was secret and mostly 'behind the curtains',[3] it had a significant impact on the way in which online space has been further conceived as 'public' and 'private'.

Market and commercialisation changed the situation and internet service providers started to influence laws and legislation. One of the most important 'battles' has been over Net neutrality, a principle that causes internet service providers to treat all communications on the internet equally and to 'not discriminate or charge differently based on user, content, website, platform, application, type of equipment, or method of communication' (Gilroy 2011). Profit-driven internet service provider companies have an obvious financial interest in abolishing this principle, but the consequences in many countries can be rather political if 'a small handful of private concerns have a censor's power over what had become the primary marketplace of ideas' (McChesney 2013). The dangers are numerous: the pricing of the services, censorships, privacy issues and, finally, surveillance.[4] The issues regarding internet service providers are mainly assessed on a case-to-case basis. An important case is *Delfi v Estonia* which refers to whether there was an active role of the website when it comes to enabling third-party comments. In this case, the European Court of Human Rights 'acknowledges that important benefits can be derived from the Internet in the exercise of freedom of expression, it is also mindful that liability for defamatory or other types of unlawful speech must, in principle, be retained and constitute an effective remedy for violations of personality rights'. On the other hand, the Grand Chamber stated that 'Delfi cannot be said to have wholly neglected its duty to avoid

3 McChesney asserts that 'the media watch group Project Censored ranked the privatization of the Internet as the fourth most censored story of 1995' (McChesney 2013).

4 These problems so far are much more visible in non-Western parts of the world, such as China and sub-Saharan Africa (Skycoin 2018).

causing harm to third parties, but the automatic word-based filter failed to select and remove odious hate speech and speech inciting violence posted by readers and thus limited its ability to expeditiously remove the offending comments'. Another case before the European Court of Human Rights which referred to intermediary liability is *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary*. The Court stated that the applicants 'could foresee, to a reasonable degree, the consequences of their activities under the domestic laws. In doing so, the Court placed considerable emphasis on the fact that the Applicants were a self-regulatory body and a media publisher running 'a large internet news portal for an economic purpose.'

Overall, what changed in the exercise of the human right to freedom of expression is the number of platforms for this exercise because 'the internet has now become one of the principal means of exercising the right to freedom of expression and information'. Accordingly, the number of actors that may be liable for problematic content also increased. However, it is not necessary to introduce new, stricter provisions related to the internet, but more attention is needed when balancing freedom of expression exercised online and, for example, the rights of others (McChesney 2013).

On the other hand, the idea of transferring 'offline' rights to 'online sphere' described before has become much more vague than in the era of collective internet optimism during the 1960s and 1970s. Since most of the important human rights protection documents were written during the non-internet or early internet phase, its direct transmittance to a very specific internet field became impossible. That is one of the reasons why the Internet Rights and Principles (IRPC) Dynamic Coalition in 2010 developed the IRCP Charter and released it at UN Internet Governance Forum (IGF) in Vilnius, Lithuania. In this document, Article 7 – Freedom of Online Assembly and Association – translates article 20 of the Universal Declaration (Universal Declaration of Human Rights 1948) to online space in the following manner: 'Everyone has the right to form, join, meet or visit the website or network of an assembly, group or association for any reason. Access to assemblies and associations using ICTs must not be blocked or filtered' (IRCP Charter 2018). However, this is only part (a) of the article. The rest is still being drafted and may have a significant impact on how the conception of online space as a space for assembly will develop, especially combined with other rights provided for by this Charter. There are many perspectives to this and when all factors are taken into account, the opportunities and dangers occasioned by online space become more complicated.

2.4 Surveillance and security

After an examination of the providers and the very nature of the internet space itself, it remains critical to focus on the status and examples of protective measures and the possible abuses of the web environment. Surveillance and security on the internet define the relationship between online *freedom* and *order*, comprising both legislative and ethical practices that overlap respectively. Moreover, the relevance of the privacy of web users has become even more focal during the last decades since cyber threats are estimated by world governments and security organisations as global danger number one, thus replacing terrorism as the number one

global threat (Contreras et al 2013). In fact, one might claim that terrorism significantly generated the increase of protective measures that can further be abused for surveillance practices. Perry and Roda (2017) claim that

> with the advent of terrorist attacks worldwide, many governments have pushed through legislation permitting online surveillance policies that may violate international treaty commitments and domestic law, particularly with respect to due process and legal consent. Electronic surveillance is a controversial form of data compilation because it is by nature virtual, leaving no physical trace to the untrained eye.

The ambiguity of online security described can most clearly be seen in the fact that the guarantees of privacy protection can never be clearly defined. Web security and privacy depend both on the fragile technological factors and on the users' online habits. It follows that 'a digital system that is not secured cannot be regarded as private, while having secured privacy of the system does not guarantee it is fully secured' (SHARE Foundation 2015).

Hence, it remains crucial to explore the question of how surveillance of our internet-based activities and the security thereof relate to freedom of expression characteristic to assemblies based both offline and online. Related to the topic of providers of internet access, a legitimate question to be asked is that if someone is to ensure protection and security, whether that does not cause the internet to be supervised by someone. Finally, is surveillance a *modus operandi* of online security?

The Guidelines on Freedom of Peaceful Assemblies drafted by the Organisation for Security and Co-operation in Europe (OSCE) state that '[a]ll types of peaceful assembly – both static and moving assemblies, as well as those that take place on publicly or privately owned premises or in enclosed structures – deserve protection' (Belyaeva et al 2010). Since the official instruction to protect online assemblies is still in the drafting process (also by the OSCE panel of experts) the presumption is that online assemblies deserve the same treatment. Yet, exercising protection does not exclude the possibility of interference in the private life, guaranteed by article 8 of the European Convention of Human Rights on privacy, if the actions of an individual or a group threaten national security or the freedom of others (Council of Europe 1953).

The experiences show that surveillance, under the guise of providing protection, not only interferes with privacy, but indeed can lead to severe censorship practices. This is evident from the fact that

> electronic surveillance as currently practised by most states encroaches upon an individual's sacrosanct right to privacy, a fundamental right enshrined in Article 17 of the International Covenant on Civil and Political Rights. In many instances, electronic surveillance is a prelude to censorship. State censorship which involves the suppression of proscribed content and eventual sanctions against the user, is the next step in the digital surveillance chain (Perry and Roda 2017).

3 Online assemblies and freedom of expression in South-East Europe

When the internet arrived in Yugoslavia in 1991, it only connected three faculties of Belgrade University: the Faculties of Mathematics, Electro-

Technics and Political Science (RCUB). The network has spread further to other universities in Zagreb, Ljubljana and Novi Sad. Later on, the war in Yugoslavia slowed down the development and access to internet services. However, in 1992, in the midst of the war in Croatia, a group of human rights activists and students from Belgrade and Zagreb (and later also from Sarajevo) managed to go online, thanks to Open Society Funds and several other anti-war activists from Germany and The Netherlands. Together, they formed a platform called Zamir.net (in Serbo-Croatian at the time 'For Peace'), which was a platform that promoted anti-war efforts and other progressive ideas such as Lesbian, Gay, Bisexual, Transgender, Intersex and Questioning (LGBTIQ) rights and environmentalism. Zamir.net mainly assisted people to connect with their families in other countries, and to make sure that their family members survived attacks or were able to escape the war zones (Gessen 1995). This historic example in South-East Europe illustrates that the online assembly was formed out of the necessity for peace.

3.1 Bosnia and Herzegovina

Due to a very complex constitutional and administrative order in Bosnia and Herzegovina[5] (BiH) it is very difficult to obtain unified data about internet penetration. The most recent data is from the Communications Regulatory Agency (RAK). This agency has published its report of the annual survey of users allowed to provide internet services in BiH in 2018. According to the report, by the end of 2018 there were 67 internet providers in the territory of BiH, with a total internet usage rate of 90,49 per cent (RAK 2019). The data provided in the report shows that the use of the internet in Bosnia and Herzegovina is on a steady pace and the agency expects that further liberalisation of the telecommunications market and the introduction of new technologies will enable the presence of quality services (RAK 2019).

On the other hand, state regulations regarding the internet are not as positive as the usage rate. When the Entity of Republika Srpska (RS) passed the Law on Public Peace and Order in 2015, it caused much controversy among the public. The president of the Entity stated that no limitations were placed on freedom of speech in this Entity but neither should any form of communication be misused (Halilović 2015). Among the public in BiH it is indisputable that hate speech, paedophilia and similar criminal activities are condemned, but with this law there are no restrictions on the ability of the state to regulate social networks and regular citizens expressing themselves. This is why the general impression among the Bosnian public is that the law was passed in order to keep an eye on all those who criticise the government (Halilović 2015). These obstacles are reflected first in the very adoption of necessary legislation that is affected by political pressures, just as it is the case with the content

5 The current political system in Bosnia and Herzegovina is the product of the Dayton Peace Agreement (1995). This Agreement stopped the brutal war which occurred after this state had proclaimed independence from the Socialist Federative Republic of Yugoslavia. According to Annex 4 (the Constitution of Bosnia and Herzegovina) of the Peace Agreement, Bosnia and Herzegovina has two entities and one district: Entity of the Federation of Bosnia and Herzegovina (mostly populated by Bosniaks and Croats) and Entity of Republika Srpska (mostly populated by Serbs) and District of Brčko.

of most media outlets (even public service programming), as they cannot be said to be independent to a great extent.

Specifically, when it comes to the RS's Law on Public Peace and Order, it is particularly worrying to include social media within the definition of a 'public space'. While such legislation is familiar to Western states, such as the United Kingdom, the interpretation of this legal trend is deeply concerning: It gives power to the police and magistrates and judges to interpret the law and sanction any social media action as they see fit. This is problematic, as the law does not include concrete standards for the definition of social media, nor does it explain what constitutes 'offensive' or 'indecent' material, nor denies that citizens can be prosecuted outside of RS. Democratic societies should be void of such arbitrary provisions as they violate the freedom of expression of internet users, which has been commonly recognised under international law (European Convention on Human Rights 1950; OHCHR International Covenant on Civil and Political Rights 1966; Universal Declaration of Human Rights 1948).

The government must be able to 'establish that the expression poses a serious threat to national security' and the restriction constitutes the 'least restrictive means' available. 'Once information has been made generally available, by whatever means, whether or not lawful, any justification for trying to stop further publication will be overridden by the public's right to know' (Johannesburg Principles on National Security 1996).

The government does not state any explicit reason for detaining the users of social networks. Furthermore, there is no proven causal link between any incidence of violence and posts on social networks. Such a link must be established first in order for the aim of protecting the public order to be viable (Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights 1984).

The contents of the posts on social networks because of which the authors were detained do not intend or seem likely to incite riot or any threat to national security, and there is no proof, only a speculative link between the posts and possible threats to public order. One of the most important cases in this connection was that of a journalist, Danijel Senkic, also a representative of an NGO 'front'. On his Facebook wall, Senkic spoke about the authorities in BiH when they arrested Bosniak returnees in RS, and called their activities acts of terror, and described some police officers as 'criminals' and Bosniak politicians as 'mute observers' (Senkić 2015). Interesting is the fact that Senkić was detained despite the fact that he lives in a part of BiH that is out of the reach of the disputable law mentioned above (Dodikova diktatura i u FBiH 2015). At the same time, the authorities did not focus on the verification of information regarding war crimes, but on prosecuting a person who speaks on their Facebook wall. Experts agree that the only way in which it would have been possible for Danijel Senkic to come before court would be for defamation, and only if he would be the person accused of committing the crime (Halilović 2015b).

The most recent case concerning the role of the state and internet restrictions in BiH occurred in April 2019. Good cooperation between the portal Klix.ba, state institutions and internet providers resulted in the arrest of three people in the territory of BiH in only five days, for writing

hate speech in comments on the news portal Klix.ba (Za pet dana u BiH uhapšene tri osobe zbog govora mržnje na internetu 2019). The portal warns about online hate speech as the crucial problem on the internet and calls for citizens/users to report it.

3.2 Serbia

It is a fact that in recent times internet users have succeeded in finding ways to avoid restrictions. However, it is clear that the physical infrastructure in the territory of a particular country cannot, at least legally, exist without the permission and consent of state authorities (Perkov 2017). The most thorough regulation in Serbia is the Electronic Communications Law. Apart from this, electronic surveillance is especially regulated by the Code of Criminal Procedure, the Law on the Military Security Agency and the Military Intelligence Agency, as well as the Law on the Security and Information Agency. All these regulations oblige operators to set up their network infrastructure in a certain way, in order to provide the ability to intercept communications and retain communications data (Perkov 2017).

The field that is the most problematic for Serbian authorities includes social networks. Media and experts close to the Serbian President often use the example of Turkey when justifying control over the internet.Under Erdogan, there is constant control over the messages sent through social networks in Turkey, and one cannot write what one wants or criticise him. In Serbia, an evironment prevails in which insults and defamations are exchanged at will (Kurjački 2017).

This is the example of how an analyst, Vuk Stanković, commented on a situation regarding the programming of the pro-government Pink TV Channel. This channel has a national frequency and has a great influence on public opinion. On the other hand, Nedim Sejdinović from the Independent Journalists Association of Vojvodina sees this statement as an open call for internet regulation, which would open up an enormous space for abuse in terms of 'banning' certain content that does not suit authorities (Kurjački 2017).

If the state intends to punish the owner or author of the platform for violating domestic regulations, such a possibility exists if the head office or representative office is located in its territory (Perkov 2017). Nevertheless, out of the 100 sites most visited, 60 per cent of sites do not have any connection with Serbia, which means that the platforms most commonly used by citizens of Serbia are wholly beyond the reach of the state (Perkov 2017).

When it comes to using the platforms for assembly, an ongoing massive weekend protest in the capital Belgrade, '#1od5miliona', mobilised through online platforms after a murder and violent attacks on politicians from the opposition, can serve as an example. Professor Đorđe Krivokapić claims that the internet is the only media platform in Serbia that can generate significant critique and mobilisation of citizens since other media is controlled by the state (Čilić 2019).

Another danger to the online sphere in Serbia is presented by the recent installation of closed-circuit television in Belgrade. Since video surveillance in public spaces is not regulated in Serbia, it remains

controversial to what degree personal privacy is protected knowing that surveillance cameras have an option of facial recognition (SHARE Foundation 2019). Moreover, similarly to the case of Croatian disclosure of personal data of insolvent persons, the numerous examples of hacking attacks in Serbia display how insecure online platforms of both governmental institutions and NGOs are. Although Serbia has an Emergency Response Team (CERT) that coordinates prevention and protection from security risks in ICT systems on the national level, (Trusted Introducer: Directory: SRB-CERT nd), the hackers' attacks remain frequent. For instance, in 2018 four centres for social work across the country were hacked in order to collect personal data of the victims of violence (FoNet 2018). The Chamber for Public Sales was also hacked, disabling the visibility of more than 20 000 public offers (021 2018). In the same year, the email addresses of the Office for Refugees and Migration were hacked and used to send messages to different recipients (DD 2018).

3.3 Turkey

The examples of Turkey under the current President Erdogan, a country not only with a historical-cultural influence on the SEE region that started with the expansion of the Ottoman empire in the fifteenth century, but also with a strong current political and economic influence on Bosnia and Herzegovina and other countries, are instructive in scrutinising practices of surveillance of the online assemblies. Followed by the 2016 *coup* attempt against the government of Erdogan's AKP (Justice and Development Party), many internet platforms and internet service providers in general faced severe surveillance and controlling strategies exercised by the government. The group of Turkish scholars examined the post-*coup* internet policies in the country and offered their key findings (Yesil et al 2017):

> The AKP's post-*coup* strategies concerning the internet are culminating in a distributed network of government and non-government actors using hard and soft forms of control. While the AKP continues to deploy existing internet law, anti-terror law and press law provisions and further expands its online hegemony by way of decree laws, its post-*coup* internet policy has also come to rely on the opaque activities of users and groups who are affiliated with government officials, party members and partisan media outlets and whose primary objective is to target and harass government critics on social media, and intimidate those who dissent.

As a consequence, in 2018 Freedom House described internet freedom in Turkey as severely manipulated by the government, which was frequently removing or blocking internet content, and because of which it was given 'non-free' internet status (Freedom House 2018).

3.4 Croatia

In Croatia, the youngest EU member and the second of former Yugoslav countries after Slovenia, two phenomena related to online assemblies and democracy dynamics can be observed. The first is the rise of populist parties, notably Živi zid (Human shield), which arose after online-supported anti-government protests. The so-called 'Facebook protests' in 2008 effectively marked the beginning of online-supported protests in Croatia. However, since more than 60 000 people confirmed their attendance, whereas only a few thousand people gathered in the capital

Zagreb, media characterised the Croats as rebels only on the internet and rightly pointed out that protests initiated on Facebook had failed (Werman 2008; Valich 2008). Yet despite the failure, the leader of the protest, Ivan Pernar, and his populist party Živi zid has increasingly become one of the most relevant political actors in the country ten years later. Their main political activity is the fight against foreclosure methods and enforced evictions with which banks deprive indebted individuals and families from their houses. Besides organising resistance towards police officers in front of the confiscated houses, they became popular also because of their strong anti-EU stance and because of the promotion, using their social media profiles, of bizarre conspiracy theories such as urging people not to vaccinate their children since, according to them and other promoters of this theory, this can cause autism and similar conditions (NACIONAL 2017).

A related phenomenon of the SEE region, namely, the foreclosure trend manifested in the myriad of executed bankruptcies, is an example of weak legal protection of personal data. With a population of around four and a half million, Croatia has more than 300 000 people/families in foreclosure status, mostly due to falling into debt using Swiss currency of which the value significantly decreased in the 2010s. Since 2013 people hit with foreclosure measures are gathered in the association Blokirani (Blokirani.hr nd). However, in the beginning of 2019 the courts were allowed to publish personal information of the bankrupted individuals and thus increase their public visibility and consequently personal and financial vulnerability. The personal data of more than 100 000 people was made public, but the Ministry of Justice claims that the right to privacy is not violated since the courts are supposed to work transparently (N1 2019).

4 Conclusion

Our research demonstrated that the internet serves different interests in the SEE region. Although one notices an increase in the online mobilisation of public protests, the interest primarily remains in the hands of the governments to exercise control and in the hands of the state-owned companies to maintain monopoly through providing their services. Further, it is important to underline that the progress in the understanding and use of the internet for civil purposes is still burdened by divisions, the legacy of the war and transition in the countries of the SEE region. Thus, rather than exercising and promoting social rights, online platforms are predominantly used by 'troll armies' to spread hatred speech based on national, ethnic, religious, political and other differences. In the context of the global scene, we noticed that regional legislation does not follow technological progress, resulting in the weakly-developed legal system of protection that is always slow to follow the increasingly fast development of new virtual instruments.

First, the article provided a detailed overview of the theory and international human rights law, in order to offer a setting in which the enjoyment of the two rights occurs. The most relevant for the region in this respect is the European Convention on Human Rights and Fundamental Freedoms (European Convention) and the practice of the European Court of Human Rights. Article 10 of the European Convention

safeguards freedom of expression in its first sub-section, and explains limitations to the exercise of this right in sub-section 2. Article 11 refers to the right to assembly, the restrictions of which are similar to the mentioned restrictions in article 10: the interests of national security or public safety; the prevention of disorder or crime; the protection of health or morals; and the protection of the rights and freedoms of others.

The article further explored the role of the state to provide or facilitate internet access. It has been acknowledged that the internet is not a specific platform which requires more regulation, which is why some actions taken by states in the region have been assessed as rather questionable. This article sifts through various examples of advantages and disadvantages regarding internet regulation, but emphasises that the UN Human Rights Committee urged states to ensure internet access to individuals, maintain its independence and its possibilities of providing more space for exercising human rights. Moreover, the fact that the internet is gaining momentum also brought numerous new actors into play, which is why the article is specifically directed at explaining the role of internet service providers, drawing the line between active and passive actors and highlighting the level of editorial liability in this respect.

The article acknowledges the dehumanisation, internationalisation and privatisation of the internet by pointing to the fact that internet service providers have a substantial influence on all aspects of the online sphere and indirectly also on new regulations. The question of net neutrality has attracted specific attention as it causes internet service providers to treat all communications on the internet in the same manner regardless of the type of communication used. The article agrees that profit-driven internet service provider companies have a certain financial interest which may present problems in terms of censorship, privacy issues, the price of the service as well as fake news. Platforms, advertising agencies, advertising networks and the networks and service providers that provide internet access to consumers benefit because they depend on consumers spending more time with a certain type of content and they track profiles of consumers, thus providing them with the content they identified as relevant for certain users.

As far as the interdependent nature of freedom of expression and freedom of assembly is concerned, the article introduces the topic of surveillance and security. The article perceives surveillance mainly as a tool of states to exercise control over the internet and explores the interplay between the two rights, in addition to the right to privacy enshrined in article 8 of the European Convention. The relevance of privacy of web users is an issue that is gaining momentum as cyber security has in the past few years often been in jeopardy. Web security and privacy depend both on technological factors and on the users' online habits. However, as they are easily tracked down, the article acknowledges that there is no guarantee to provide users with full protection, because their activities online are easily visible to network providers, advertisers and even state authorities, and because users often are unaware of the fact that in addition to their rights to be online, they also have responsibilities.

When it comes to legal restrictions placed on freedom of expression and freedom of assembly in the region of South-East Europe, one of the most recent examples is the Law on Public Peace and Order adopted in Republika Srpska – one of the two entities of Bosnia and Herzegovina. The

most problematic aspect of the law is, the lack of the definition of public space. According to local and international experts, the reason for assessing this law to be restrictive lies in its application, because on several occasions public space included social networks and their users were detained by the police. Just as in most examples referring to Bosnia and Herzegovina, the posts dealt with war and war crimes, but there was no sufficient basis to claim that their posts intended or were likely to incite riot or any threat to national security, that is, to public order. In this manner, the authorities not only exercised their control over the online sphere, but they also caused a chilling effect among social network users and made the scope of the restrictions questionable, by detaining persons who were not based in the territory of Republika Srpska, but in the Federation of Bosnia and Herzegovina, the other entity in BiH.

On the other hand, Serbia has seen a rapid decrease in freedom of expression in the past few years, because the state aims at penetrating the online sphere in terms of restrictions and monopoly over internet service providers. In Serbia only two companies provide internet services, namely, Telekom Serbia and SBB. Of these almost 80 per cent of the population uses the former connection, Telekom Serbia, owned by the state. The article explains that there is a panoply of laws referring to the online sphere: the Electronic Communications Law; the Code of Criminal Procedure; the Law on the Military Security Agency and the Military Intelligence Agency; as well as the Law on the Security and Information Agency. All these regulations oblige operators to have their network infrastructure set in a specific manner. This makes the interception of communications and the tracking down of users easy and thus the users' data are rather susceptible to misuse. Now more than ever, the right to freedom of expression and the right to freedom of assembly go hand in hand in Serbia because social networks and online groups are largely used for protests that have for months been going on in Serbia. The article identified the occasions on which these rights were violated, and acknowledged the dangers of state authorities banning certain content, spreading fake news and directly pointed at the attacks experienced by some journalists and protest organisers. The deteriorating state of freedom of expression, freedom of assembly and right to privacy in Serbia is also illustrated by the recent installation of closed-circuit television in Belgrade and the numerous examples of hacking attacks in Serbia. It is particularly disturbing that surveillance in public spaces is not regulated in Serbia, and as protests are occurring and cameras are installed, it is not known to what extent and for which purpose the facial recognition option with cameras will be used by the authorities.

Furthermore, the article discussed trends in Turkey which exercised substantial control over online assemblies. In 2016 Turkey saw an attempt at a *coup d'état* and many internet platforms, internet service providers and even 150 media experienced shut-downs and extremely strict surveillance and controlling strategies exercised by the government. This event has changed internet policies in Turkey as the government used hard and soft forms of control to a great extent all over the internet. The article also acknowledged the fact that the right to freedom of expression and the right to peaceful assembly have been casualties of internet law, anti-terror law and press law. Academics were detained when mentioning problems in the country on conferences; journalists and activists were detained due to their actions taken against the regime that oppressed basic human liberties;

authorities were denied permission to attend traditional May Day demonstrations in Istanbul; and so forth. The rights to online assembly and freedom of expression were violated with every denial of internet access during security operations, several news and citizen journalism websites were blocked, and even Wikipedia was inaccessible while most users of social networks such as Twitter and Facebook received numerous requests for content removal. The article clearly identified the problems faced by online users and pointed at censorship and a substantial level of control over internet by the authorities, which not only jeopardised their exercise of human rights, but often altogether disabled their exercise in the online sphere.

The article finally explored the current state of online assembly and freedom of expression in Croatia. As a new EU member, Croatia had to make its legislation compliant with the EU accession requirements and it has not seen serious cases of censorship or shut-downs. The activities on social networks in Croatia were, on certain occasions, precisely that – the activities on social networks only. Therefore, even though there were initiatives to mobilise protesters via the online sphere, in the offline sphere not many persons were very active. On the other hand, Croatia has seen a rather serious example of privacy violation and the misuse of data gathered through an online group. After executed bankruptcies performed by the banks, the courts were allowed to publish the personal data of over 100 000 bankrupted individuals gathered around the association Blokirani. In this manner the authorities exploited the members of the group and their data which may have had a chilling effect, because it would mean that people cannot freely join groups and thus share similar problems and work for the same cause either in the online or offline sphere, if their personal information is in jeopardy when they do so.

By analysing the examples of countries in South-East Europe, the article explored the interaction between the right to freedom of expression and the right to peaceful assembly. It showed that in the online sphere, the two rights are tightly connected because the internet opened numerous opportunities of gathering people, mobilising through social networks and provided a new space for debates. This space has become increasingly active and vibrant, much activism in the region shifted from the offline to the online world, and this trend was also recognised by the authorities. Therefore, the internet policies in these countries have undergone vast changes, and legislative frameworks have been amended or interpreted rather broadly in order to be more applicable to the online sphere. It seems that such attempts have not thus far been very successful, because instead of enabling and protecting new ways of freedom of expression and of assembly, the states limited the access, caused chilling effects or censored the online content in order to exercise more control over the internet. 'One of the great paradoxes of democracy is that if it functions well, criticism of it will thrive' (McGonagle 2011). Therefore, if public participation, assembly and expression on the internet are thwarted either by legislation, blocking, filtering or causing a chilling effect, then democracy and the enjoyment of human rights in South-East Europe seem shaky and their future rather uncertain.

References

A policy framework for enabling internet access (2016), available at https://www.internetsociety.org/resources/doc/2016/a-policy-framework-for-enabling-internet-access/ (last visited 4 April 2019)

Belyaeva N 'Organisation für Sicherheit und Zusammenarbeit in Europa' Office for Democratic Institutions and Human Rights, Europarat (eds) 2010. Guidelines on freedom of peaceful assembly. OSCE/ODIHR, Warsaw/Strasbourg

Blazhevska V (2017) 'Sustainable Development Goal 9: Investing in ICT access and quality education to promote lasting peace', available at https://www.un.org/sustainabledevelopment/blog/2017/06/sustainable-development-goal-9-investing-in-ict-access-and-quality-education-to-promote-lasting-peace/ (last visited 4 April 2019)

Blokirani.hr nd Blokirani, available at http://www.blokirani.hr/ (last visited 4 May 2019)

Čilić U (2019) Krivokapić: Građanska pobuna na društvenim mrežama Radio Slobodna Evropa, available at https://www.slobodnaevropa.org/a/srbija-protesti-mreze/29785214.html (last visited 4 May 2019)

Contreras JL, DeNardis L & Teplinsky M 'Mapping today's cybersecurity landscape' (2013) 62 *American University Law Review* 1113

Dodikova diktatura i u FBiH: Tuzlak na saslušanju u policiji zbog statusa na FB (2015) Novinska Agencija Patria, available at https://nap.ba/news/13080 (last visited 4 June 2019)

Fazzi D 'Eleanor Roosevelt's peculiar pacifism: Activism, pragmatism, and political efficacy in interwar America' (2017) 12 *European Journal of American Studies: Special Issue – Eleanor Roosevelt and Diplomacy in the Public Interest*, available at https://journals.openedition.org/ejas/11893 (last visited 28 April 2019)

FoNet P (2018) Poverenik: Pokrenuti prekršajni postupci protiv nekoliko centara za socijalni rad Dnevni list Danas, available at https://www.danas.rs/drustvo/poverenik-pokrenuti-prekrsajni-postupci-protiv-nekoliko-centara-za-socijalni-rad/ (last visited 28 April 2019)

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

Gessen M (1995) Balkans Online *Wired*, available at https://www.wired.com/1995/11/zamir/ (last visited 28 April 2019)

Habermas J (1991) *The structural transformation of the public sphere: An inquiry into a category of bourgeois society* trans Burger T & Lawrence F Cambridge and Massachusetts: The MIT Press

Habermas J (2003) *On the pragmatics of communication* Oxford: Blackwell Publishing Ltd

Halilović M (2015) Veliki brat u vašoj kući. Analiziraj.ba., available at https://analiziraj.ba/2015/02/11/veliki-brat-u-vasoj-kuci/ (last visited 4 April 2019)

Halilović M (2015) PROGON GLASNIKA LOŠIH VIJESTI. Analiziraj.ba., available at https://analiziraj.ba/2015/07/02/progon-glasnika-losih-vijesti/ (last visited 4 June 2019)

Herold DK 'Development of a civic society online? Internet vigilantism and state control in Chinese cyberspace' (2008) 2 *Asia Journal of Global Studies* 26

Kurjački N (2017) Da li bi moglo da dođe do cenzure društvenih mreža u Srbiji? N1 Srbija available at http://rs.n1info.com/Vesti/a333532/Da-li-bi-moglo-da-dodje-do-cenzure-drustvenih-mreza-u-Srbiji.html (last visited 4 April 2019)

La Rue F (2011) 'Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development', available at https://doi.org/10.1163/2210-7975_HRD-9970-2016149 (last visited 4 April 2019)

McCosker A, Vivienne S & Johns V (2016) *Negotiating digital citizenship: Control, contest and culture*. London and New York: Rowman & Littlefield International Ltd

N1 (2019) Koliko su nam zaštićeni osobni podaci?, available at http://hr.n1info.com/Vijesti/a369370/Koliko-su-nam-zasticeni-osobni-podaci.html (last visited 4 May 2019)

NACIONAL (2017) PERNAR 'U cjepivo su stavili nešto da nas trajno obilježi, žigoše ko stoku', available at https://www.nacional.hr/pernar-u-cjepivo-su-stavili-nesto-da-nas-trajno-obiljezi-zigose-ko-stoku/ (last visited 28 April 2019)

OHCHR International Covenant on Civil and Political Rights 1966, available at https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (last visited 4 May 2019)

OSCE and ODIHR (2010) *Guidelines on Freedom of Peaceful Assembly* Warsaw and Strasbourg: Organisation for Security and Co-operation and Office for Democratic Institutions and Human Rights (ODIHR), available at https://www.osce.org/odihr/73405?download=true (last visited 28 April 2019)

Perkov B (2017) Nadležnost Srbije na internetu, available at https://labs.rs/sr/nadleznost-srbije-na-internetu/ (last visited 4 April 2019)

Perry S & Roda C (2017) *Human rights and digital technology: Digital tightrope* London: Palgrave MacMillan

RCUB Istorijat (trans Serbian: The History) *Računarski Centar Univerziteta u Beogradu* (trans Serbian: IT Centre at the University of Belgrade), available at https://www.rcub.bg.ac.rs/o-rcubu/istorijat.html (last visited 28 April 2019)

Senkić D (2015) Facebook.com, available at https://www.facebook.com/danijel.senkic.3/posts/10206446620113660?fref=nf (last visited 4 April 2019)

Share Foundation (2019) 'New surveillance cameras in Belgrade: Location and human rights impact analysis – "withheld"' SHARE Foundation, available at https://www.sharefoundation.info/en/new-surveillance-cameras-in-belgrade-location-and-human-rights-impact-analysis-withheld/ (last visited 4 May 2019)

Share Foundation (2015) Vodič: Osnove digitalne bezbednosti. SHARE Foundation, Belgrade

Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights 1984

Soh C, Connolly D & Nam S (2018) 'Time for a fourth generation of human rights?' UN Research Institute for Social Development, available at http://www.unrisd.org/TechAndHumanRights-Soh-et-al (last visited 28 April 2019)

Trusted Introducer : Directory : SRB-CERT nd, available at https://www.trusted-introducer.org/directory/teams/srb-cert.html (last visited 4 May 2019)

UN Sustainable Development 'Transforming our world: The 2030 Agenda for Sustainable Development' UN Sustainable Development Goals, available at https://sustainabledevelopment.un.org/post2015/transformingourworld (last visited 28 April 2019)

UN Human Rights Committee General Comment 34 Article 19: Freedom of opinion and expression, 2011 CCPR/C/GC/34

Universal Declaration of Human Rights 1948, available at https://www.un.org/en/universal-declaration-human-rights/ (last visited 4 April 2019)

Valich T (2008) 'Croatian Facebookers protest: 4 000 people in Zagreb, police/political disruption in smaller cities', available at http://vrworld.com/2008/12/06/croatian-facebookers-protest-4000-people-in-zagreb-policepolitical-disruption-in-smaller-cities/ (last visited 28 April 2019)

Werman M (2008) 'Facebook protests in Croatia' Public Radio International, available at https://www.pri.org/stories/2008-12-05/facebook-protests-croatia (last visited 4 May 2019)

Yesil B, Sözeri EK & Khazraee E (2017) 'Turkey's internet policy after the coup attempt: The emergence of a distributed network of online suppression and surveillance' Internet Policy Observatory