Reshaping the electoral run through the usage of social media in Montenegro

- Analytical Paper –

CENTRE FOR MONITORING AND RESEARCH

International Foundation for Electoral Systems

CENTRE FOR MONITORING AND RESEARCH

International Foundation for Electoral Systems

RESHAPING THE ELECTORAL RUN THROUGH THE USAGE OF SOCIAL MEDIA IN MONTENEGRO

- Analytical Paper –

September 2020

RESHAPING THE ELECTORAL RUN THROUGH THE USAGE OF SOCIAL MEDIA IN MONTENEGRO

- Analytical Paper –

Publisher:
Centre for Monitoring and Research (CeMI)
Bul. Joseph Broz 23A
e-mail: info@cemi.org.me
www.cemi.org.me

Editor:
Teodora Gilic

Authors:
Milica Zrnovic
Ivan Vukcevic
Vladimir Simonovic

CeMI
CENTRE FOR MONITORING AND RESEARCH

IFES
International Foundation for Electoral Systems

This Paper was published as part of the Facebook Pilot Project implemented by the Centre for Monitoring and Research (CeMI), in collaboration and with the financial support of the International Foundation for Electoral Systems (IFES).

Content

Introduction

The Internet is often described as one of the greatest modern human achievements, one that has quickly become a vital aspect of our lives. The Internet provides us with access to a vast amount of information and services and it allows us to connect and communicate, not only with the people we know but also with countless strangers across the globe. The Internet continues to evolve at a rapid pace, and its impact on every aspect of our life cannot be understated.

It should not be surprising then, that the evolution of the Internet can also be seen in the political sphere. Over the past few years, significant changes were made in how political candidates, organizations, and parties conduct their electoral campaigns. Campaigns used to take place in public places, with as many people as could fill the halls. They later evolved to include billboards, spots on radio stations, TV commercials, print ads, etc. Today, the use of social media is one of the major driving forces behind political campaigns and elections. Social media has quickly become one of the major tools of some of the most influential political parties and subjects, and it has had a profound impact on how candidates organize and structure their campaigns.

With that in mind, in the past couple of years, there has been increasing concern of harmful content and abusive activities that are being shared on social media in particular during the electoral period. These activities include fake profiles, undesirable content, black PR, fake news, etc. We must be aware that the threats to, not only social media but the overall Information and Communications infrastructure may threaten users' privacy and integrity, and affect other aspects of our everyday life. Thus, reliability and security of networks, information systems, and services are essential to economic and societal activities, in particular for the functioning of the society as a whole.
In Montenegro, National Computer Incident Response Team (CIRT) identified a growing trend in the number of reported online and cyber incidents (e.g. denied access to the system and personal information, various online frauds, etc) , as well as the sophistication of the attacks. The incidents were reported by the public and private sector. In 2013 there were 22 reported incidents, in 2014 – 42, 2015 – 132, 2016 – 163, 2017 - 385. The total number of reported incidents from 2013-2017 was 744, of which 17,2% was related to the abuses of profiles on social networks, and 5,65% to inappropriate content on the Internet.[1]

In light of the 2020 Parliamentary Elections in Montenegro, this analytical paper aims to provide a general overview of the national legal framework regarding social media and cybersecurity, as well as to give an outline of the laws regulating social media in other countries. Final recommendations and conclusions are based on findings of the analysis conducted for the purposes of the preparation and the production of this document.

[1] *Strategy for Cyber Security of Montenegro 2018-2021, December 2017*

1.Social media legal and institutional framework in Montenegro

Legal framework

When it comes to social media and Internet regulatory framework in Montenegro, there is no law exclusively governing this field and addressing issues related to social networks.

Some of the legal acts important to mention here that regulate cyberspace and security, as well as electronic media, communications, and commerce are the following:

1. Law on Ratification of Convention on Cybercrime (Budapest Convention)
2. Constitution of Montenegro
3. Criminal Code
4. Criminal Proceeding Code
5. Law on Information Security
6. Law on Electronic Media
7. Law on Electronic Communications
8. Law on Electronic Commerce

Other legal acts important to mention here are also:

- Cyber Security Strategy for Montenegro 2013 - 2017
- Cyber Security Strategy for Montenegro 2018 – 2021

According to the Montenegrin **Constitution**[2] signed and ratified international documents and contracts, as well as accepted rules and standards of international law, have primacy over national legislation and are implemented directly when regulating differently from national laws. Thus, many international and European conventions dealing with the matter of Cybersecurity, Cybercrime or such, that are signed by Montenegro, are transposed to the national law and are directly applicable via the laws upon their ratification.

Council of Europe **Budapest Convention (Convention on Cybercrime)**[3] entered into force in 2010 for Montenegro. The Convention defines a cybercrime as a wide range of virus spread, unauthorized access to a computer network through piracy to pornography and intrusion into banking systems, misuse of payment cards, and other crimes involving the use of computers. Furthermore, the Convention defines as an offense an act related to the infringement of copyright and similar rights.

Montenegro also ratified the **Additional Protocol to the Budapest Convention**[4] concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems in 2010 and it came into force in Montenegro in the same year.

[2]Constitution of Montenegro (Official Gazette of Montenegro, no. 1/2007 and 38/2013 - Amendmentsi I-XVI)
[3]Convention on Cybercrime (Budapest Convention), Council of Europe, 2001
[4]Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Council of Europe, 2003

In accordance with the Convention and its Protocol, the Montenegrin **Criminal Code**[5] prescribes sanctions for the set of activities, defined as criminal offenses, that are directly or indirectly related to cyberspace and the content created on the Internet. **Article 370** defines criminal offenses causing national, race and religious hatred, and provides that anyone who publicly encourages violence or hatred towards the group or group member related to race, skin color, religion, origin, state or national affiliation will be punished by imprisonment for a period of six months to five years (para. 1). The same sanction is prescribed for anyone who publicly approves, denies the existence or significantly decreases the heaviness of genocide, a crime against humanity and war crimes against group or group member set based on the race, skin color, religion, the origin or state or national affiliation, if it can cause violence or hatred towards a group or group member, if such criminal acts are legally decided by judgment in the effect of either Montenegrin or international criminal court (para. 2). The adverb 'publicly' allows the interpretation including the option of associating those criminal offenses with the Internet and the online world. As well, criminal offenses of associating for unconstitutional activities (Article 372) and preparation of activities against the constitutional order and security of Montenegro (Article 373) allows the interpretation that those criminal offenses can be carried out on the Internet.[6]

Article 443 of the Criminal Code defines criminal offenses of racial and other discrimination providing that anyone who, on grounds of a difference in race, skin color, nationality, ethnical origin, or some other personal characteristic violates fundamental human rights and freedoms guaranteed by generally recognized principles of international law and international treaties ratified by Montenegro shall be punished by imprisonment for a term of six months to five years (para. 1) and anyone who spreads the ideas about the superiority of one race over another, or promotes racial hatred, or instigates racial or other discrimination will be punished by imprisonment for a term of three months to three years (para. 3).

Criminal Procedure Code[7] provides measures for combating child pornography on the Internet. Although these measures are general provisions concerning proceedings in respect of minors, the Code provides for the urgency of the proceedings when it comes to these acts, as well as the exclusion of the public.

Law on Information Security[8] defines the notion and measures of information security, that is physical, data, and information system protection. It also provides that National Montenegrin Computer Incident Response Team (CIRT) is the responsible authority for prevention and protection against computer security incidents on the internet and other information system security risks of authorities, legal entities, and natural persons in Montenegro.

Law on Electronic Media[9] regulates the rights, obligations, and responsibilities of legal and natural persons performing the activity of production and provision of audiovisual media services (AVM services), electronic publication services through electronic communications networks of competencies, status, and sources of funding of the Agency for Electronic Media to prevent unauthorized media concentration, the promotion of media pluralism and other issues of importance for the provision of AVM services, in accordance with international conventions and standards (Art. 1).

[5]Criminal Code of Montenegro (Official Gazette of the Republic Montenegro, no. 70/2003, 13/2004, 47/2006, and Official Gazette of Montenegro, no. 40/2008, 25/2010, 32/2011, 64/2011, 40/2013, 56/2013, 14/2015, 42/2015, 58/2015, 44/2017, and 49/2018)
[6]Council of Europe Report, Montenegro Media Sector Inquiry with Recommendations for Harmonization with the Council of Europe and European Union standards, Council of Europe, 2017
[7]The Criminal Procedure Code (Official Gazette of Montenegro, no. 57/09)
[8]Law on Information Security (Official Gazette of Montenegro, no 014/10 and 040/16)
[9]Law on Electronic Media (Official Gazette of Montenegro no. 046/10, 040/11, 053/11, 006/13, 055/16, 92/2017, 82/2020)

The Law on Electronic Communications[10] regulates the manner of management and use of electronic communications networks, terms and manner of conducting the activities in the area of electronic communications and other matters pertaining to this field (Art. 1). In Section XI, the Law prescribes measures and activities the operator should conduct in order to protect electronic communications and prevent its abuse. Among others, it grants operators the competence to warn or temporarily block the user's account in case there is evidence that the user sent spam or in case of abuse of the e-mail account (Article 179). If the user continues to abuse the electronic mail, the operator can permanently delete the user's e-mail account and revoke the contract. If the electronic mail is abused by the third person, the user is liable only if the user avoids the operator's warnings to use the protection. As well, in case of fraud or misuse from the scope of the Law on Electronic Communications, the operator has the obligation that, upon the request of the Agency for Electronic Communications and Postal Services or on its own initiative – in that case with the Agency's approval – blocks the access to certain numbers and services (Article 145).

The Law on Electronic Commerce[11] defines the notion of "information society service" as a „service provided at a distance, for remuneration, by means of electronic equipment for the processing and storage of data, and at the individual request of a recipient of a service, especially selling goods and services via the Internet, data offering via the Internet, marketing by means of the Internet, web browsers, as well as enabling the search of data and services transmitted by the electronic network, providing access to network or storage of recipient's data" (Art. 3).

The Law stipulates that the providers of the information services are not obliged to monitor information stored, transmitted or made available, nor to examine circumstances that could indicate illegal activity of a recipient. Providers of information services shall notify the competent public authority if determining that there is a reasonable doubt that the receiver undertakes illegal activity by using the service provided, and if there is reasonable doubt that the receiver of the service has provided illegal information. Based on the appropriate court or administrative act, they shall present all information providing a ground to undertake investigation and prosecution of criminal offenses, i.e. protection of third parties (Article 22).

The first **Cyber Security Strategy for Montenegro 2013 -2017**[12] contains seven key strategic objectives aiming to define institutional and organizational structure in the field of cybersecurity in the country, protect critical information infrastructure in Montenegro, strengthen incident response and partnership with the private sector, as well as to raise public awareness and online protection. The Strategy also envisaged the establishment of the Information Security Council, an advisory body of the Government, established in 2017 that monitors the implementation of the Cyber Security Strategy, and local CIRTs, aimed at strengthening cyber infrastructure at the local level.

Cyber Security Strategy for Montenegro 2018 – 2021[13] is a continuation of the previous strategy and it identifies eight objectives for improving the National Cyber Strategy for Montenegro during the period from 2018-2021. Reliance on European and Euro-Atlantic concepts, strengthening inter-institutional, regional, international cooperation, and partnership with the private sector, data protection and cybersecurity education are the focus of the Strategy in the coming years.

[10]Law on Electronic Communications (Official Gazette of Montenegro, no. 40/2013)
[11]Law on Electronic Commerce (Official Gazette of RoM, 80/04)
[12]Cyber Security Strategy for Montenegro 2013-2017, July 2013
[13]Law on Electronic Communications (Official Gazette of Montenegro, no. 40/2013)

Institutional framework

As per the institutional framework, similar to the legal framework, there is no national authority with exclusive competencies in the field of social media regulation.

The following institutions have an essential role when it comes to the information system security and protection of users' rights concerning electronic media, communications, and commerce:

1. Ministry of Public Administration (National CIRT)
2. Ministry of Interior/Police Directorate
3. The Agency for Electronic Media
4. The Agency for Electronic Communications and Postal Services

The National Montenegrin Computer Incident Response Team (CIRT) is a state-level central authority established under the Ministry of Information Society and Telecommunications for reporting on cyber incidents. From the organizational point of view, today the CIRT is part of the Ministry of Public Administration. The team coordinates the activities for lowering the risk of computer incidents as responses to such incidents in case they occur. Furthermore, it is dedicated to awareness-raising and education on how to recognize cyber threats and cybercrime. In the last years, **31 local CIRT** teams were created, in charge of cooperating with members of the national CIRT on the issues of protection against computer security incidents on the Internet. With regard to the private sector, seven CIRTs were created within the companies Montenegrin Telekom, Telenor, M: tel, Wireless Montenegro, Telemach, M-kabl, and Societe Generale Montenegro Bank.[14]

Within the **Ministry of Interior** and its Department for Fighting against Organized Crime and Corruption has been established a High-Tech Crime Group dealing with the issue of high-tech crimes (computer crime, child pornography, credit card abuse, and copyright abuse). **The Police Directorate of Montenegro**, **the Forensic Centre**, monitors the implementation of the Criminal Code concerning cybercrimes. Since 2013 there has been systematized a team for computer and mobile phone testing.[15]

The Agency for Electronic Media monitors the compliance of the electronic media services providers with the Law on Electronic Media and is responsible for implementing the regulation referring to the electronic publications - editorially shaped web pages and/or portals containing electronic versions of print media and/or information from the media in a way accessible to a wider public regardless of their scope. The Agency has the competency to grant licenses for digital or analog terrestrial, cable, Internet or satellite transmission of audiovisual media services. The Internet webcasting is explicitly excluded from the licensing regime and no authorization is required (Article 98, para. 2 of the Law on Electronic Media).

The Agency for Electronic Communications and Postal Services is responsible for protecting the interests of users and solving disputes on the electronic communications market and monitoring operators (Article 11 of the Law on Electronic Communications). The Agency, together with authority in charge of personal data protection, are responsible for prescribing conditions to prevent and repress the misuse and frauds related to electronic mail services, including SMS, and MMS.

Montenegring legislation offers also a judiciary mechanism for the protection of human rights and fundamental freedoms. According to the Constitution and the Law on Courts[16] everybody has the right to refer to a court for the realization of their own rights (Art. 3).

[15] *Idem*
[16] *Law on Courts (Official Gazette of Montenegro, no. 011/15)*

In criminal cases, **the Basic Court** is competent to decide in the first instance for criminal offenses for which the law prescribes as main sanction fine or imprisonment for up to 10 years, regardless of whether the act was committed during peacetime, a state of emergency, imminent danger of war, or state of war. Also, in civil cases Basic Court, in the first instance, is competent to decide in disputes concerning personal-legal relations, as well as in disputes regarding the correction or response for the information contained in the media and claims regarding the violation of personal rights committed in the media.

The legislation also provides for a **non-judicial mechanisms** for the protection of rights and freedoms. Art. 56 of the Constitution prescribes that everyone has the right of recourse to **international organizations** for the protection of their own rights and freedoms guaranteed by the Constitution. As well, Art. 57 provides the right of recourse to the **state authority or the organization** exercising public powers and seek the right to reply.

[17] *Training in Detection and Enforcement (TIDE): Political Finance Oversight Handbook, International Foundation for Electoral Systems (IFES), (Magnus Ohman ed.), 2013*
[18] *Idem*
[19] *Idem*
[20] *Idem*

2. Social media and abuse of state resources during elections

As social media became an increasingly important tool during election campaigning, it is crucial to find ways to monitor also campaign violations that may occur in this space.[17] Bearing in mind that during political campaigning on social media, in the countries where campaign strategies are less prominent, political parties and candidates are unlikely to exceed spending limits through their use of Facebook and similar services.[18] Additionally, political entities may commit other violations on social media that may constitute an abuse of state resources.[19] Namely, social media is an useful tool for documenting further violations like use of state cars or government offices during campaigns.

This refers in particular to the abuse of institutional resources, i. e. "non-monetary material and personnel resources available to the state, including publicly owned media and other communication tools."[20] Specifficaly, misuse of state media, government social media accounts, and public servants' time, as well as their personal social media accounts during campaigning, represent examples of the abuse of institutional resources. In this regard, the international community highlighted the importance of the legal and regulatory framework to prevent specific abuses related to a state's institutional resources and preserve the impartiality and professionalism of the civil service.[21]

When it comes to the institutional resources and usage of the official and personal social media accounts, in Montenegro there are a set of rules and principles prescribed by the Government.

Namely, in 2018, the Montenegrin Government adopted **the Communication Strategy 2018-2020**[22] which defines key themes/campaigns, as well as goals of the state's communication with the citizens. Within the Strategy, the Montenegrin Government established t**he Commission for the Implementation of the Communication Strategy**.

The Commission in 2019 published **the Communication Rules**[23]. The document is composed of 11 Chapters and 20 rules explaining the procedures of planning activities and announcements, defining key messages, adoption of communication plans, answers to media inquiries, organization of press conferences, social media account management, and crisis communication.

Specifically, **Chapter 9 and rule 13** addresses social media accounts management. It provides that records on the activities of ministries on social media and a register with names and contact information of the administrator is maintained by the Public Relations Service of the Government of Montenegro - Bureau for Online Communication and Coordination.

The Bureau, with the consent of the Head of the PR Service of the Government of Montenegro, administers official Government accounts on social media, while ministries and public bodies designate one or more administrators who are responsible for managing the official accounts of the institution on social media.

Chapter 9 provides exact information about what data should be contained in official social media posts, and that data with the degree of secrecy and information outside the competence of the body cannot be published. When it comes to the interaction with the users, since all contents published on official accounts of the Government and public bodies can be interpreted as an official position of the Government, comments and

[21] Joint Guidelines for Preventing and Responding to Misuse of Administrative Resources during Electoral Process, Venice Commission and OSCE/ODIHR, 2016
[22] Communication Strategy 2018-2020, Government of Montenegro, 2018
[23] Communication Rules, Commission for the Implementation of the Communication Strategy. Government of Montenegro, 2019

other announcements of users can be removed if they relate to classified information, defamatory or inaccurate information, and illegal initiatives; offensive and inappropriate requests; issues that concern someone else's competencies.

Chapter 10 encompasses guidelines for private use of social media for state officials and employees. Within the Chapter, **rule 14** provides that the views of state officials expressed through social media are considered public communication, in the same way as attitudes expressed at public gatherings or in traditional media. Consequently, the principles of the Code of Ethics must be applied to the conduct of the latter on social media.

Namely, **the Code of Ethics**[24] prescribes that "out of work time an officer must not behave in a manner that has a negative impact on the reputation of the state body" (Article 5). Additionally, "when presenting the views of the state body and personal views, the public official is obliged to preserve the reputation of the state bodies and personal reputation. In public appearances in which he does not represent a state body, the official may not disclose information from the scope of the state body or his affairs workplace, which could damage the reputation of the state body and the trust of citizens in the work of state body"(Art. 8).

The guidelines provide that this especially applies to private announcements from business trips, from the workspace, participation in events in which the official or employees represent a state body and all other official activities within and outside working hours, as well as in relation to express personal political views about the events in the country and abroad. Failure to comply with these rules shall result in disciplinary action.

Furthermore, **the Law on Civil Servants and State Employees**[25] provides that a civil servant or state employee performs his duties politically neutrally and impartially, in accordance with the public interest, and is obliged to refrain from publicly expressing his/her political beliefs (Art. 9).
The fact that human resources are critically important for election campaigns is recognized also by **the Law on Election of MPs and Councilors**[26] that prescribes that public officials appointed by the Government of Montenegro or elected or appointed by the local government, public servants and state employees may not take part in election campaigns, and neither publicly express their positions regarding elections, during working hours, i.e. while on duty. Also, police officers and members of the National Security Agency may not participate in election campaigns in any manner (Art. 50a).

Additionally, national and local government officials shall be prohibited, during election campaigns, from misusing their media appearances in the capacity of state or other public officials and from using them for advertising a candidate list and/or its electoral program (Art. 51a, para. 2).

[23]Communication Rules, Commission for the Implementation of the Communication Strategy. Government of Montenegro, 2019
[24]The Code of Ethics (Official Gazette of Montenegro, no. 050/18)
[25]Law on Civil Servants and State Employees (Official Gazette of Montenegro, no. 2/2018 and 34/2019)
[26]Law on Election of MPs and Councilors (Official Gazette of RoM, no. 16/2000, 9/2001, 41/2002, 46/2002, 45/2004, 48/2006, 56/2006 and Official Gazette of Montenegro, no. 46/2011, 14/2014, 47/2014, 12/2016, 60/2017, and 10/2018)

3. Online political advertisement during campaign period: experiences from 2016 and 2018 elections

According to the data from January 2020, in Montenegro, there are 1.2 million mobile phone connections, 464.7 thousand internet users (74% of the total population), of which 390 thousand are on social media (62% of the total population).[27]

With this trend of the population present online, which tends to rise every year, it is not surprising that social media has become the central part of the campaign strategies of the political parties in Montenegro. However, this trend is not unique only in Montenegro, but it is a global challenge.

Namely, the main challenges of online political campaigning are the manipulations such as creating the illusion of massive support or the popularity of certain subjects in order to bring in genuine support, the spread of disinformation/fake news/misinformation. Additionally, the existence of the features like trending topics as well as filters and algorithms on the Internet tend to present its users with information to which they are likely to react, that might end up leading to a reduction in the diversity of opinions in the environment itself.

Social networks, among other possibilities, offer election protagonists the opportunity to pay for their advertisements and choose the reach and select audience based on age, gender, location. In that way, even if voters do not follow or like political entities, they will be influenced and exposed to the political content popping up on every site.

Voters do have the right to like political entities on the Internet and follow their work and activities in order to gather information and make a free and informed choice. However, the rising pressures during elections and the abovementioned online propaganda can affect voter's decision not to be present online. As a consequence, they can lack relevant information necessary to make a free and informed choice, or decide not to make a choice at all. The research found that not being exposed to arguments on politicized issues decrease the strength of voters' opinions and their intention to act.[28]

When it comes to the usage of social media and networking during 2016 Parliamentary and 2018 Presidential Elections in Montenegro the rising trend of usage of Internet and social media for the purposes of political campaigning, as well as some illegal activities were rather visible.

[27] *Digital 2020: Montenegro, Datareportal, January 2020*
[28] *Digital Democracy Project, Research Memo 7, Public Policy Forum, October 2019*

2016 Parliamentary Elections

During 2016 Parliamentary elections in Montenegro, the electoral campaign was conducted through standard means: rallies, door-to-door canvassing, billboards, traditional and social media advertisements, and debates. The main theme of the 2016 Elections was Montenegro's accession to NATO.[29]

With regard to social media, 2016 Elections were characterized by blocking of messaging applications, Viber and WhatsApp, for several hours during election day and before it. Namely, the Agency for Electronic Communications and Postal Services ordered electronic communications operators to temporarily ban the use of WhatsApp and Viber with the justification of protecting users from receiving unwanted notifications and spam (Art. 178 of the Law on Electronic Communications).[30] The Agency informed the operators about the reported cases of "unlawful marketing" being spread through the networks and invited them to prevent potential unsolicited communication by adopting adequate measures.[31] According to some media articles, the blackout of messaging apps was a leading topic on social media about the elections.[32]

2016 Parliamentary elections were marked also by the arrest of 20 people, including Serbian and Russian citizens and former state officials, as well as some Montenegrin opposition leaders, who were suspected to have been planning to carry out politically motivated armed attacks against the state. The case was brought before the High Court in Podgorica and the suspects were prosecuted and sanctioned with imprisonment for the criminal offense of terrorism and creation of a criminal organization. The parties made a complaint on the decision of the High Court in Podgorica and currently the proceeding continues before the Court of Appeal.

Russian citizens involved in the criminal act were sentenced to 15 and 12 years in prison, leaders of the opposition five years in prison each, and a retired Serbian police general to eight years in prison, while members of far-right political organizations from Serbia were sentenced to seven years in prison each. Other people engaged in the creation of the criminal organization were sentenced from 1 to 3 years in prison in accordance with the prescribed legal sanctions for the offenses they were found guilty for.[33]

It is important to mention here that the highest number of reported cyber incidents concerning scams via the internet happened in 2016, while the most incidents related to the abuses of profile on social media and incidents regarding the undesired content on the Internet also happened in 2016 as well as in 2015.[34]

2018 Presidential Elections

The political campaigns during 2018 Presidential elections in Montenegro were mostly visible through billboards, but the campaigning took place also through rallies and meetings with voters, door-to-door canvassing, advertisements in traditional media, as well as on social networks.

The main topics of the campaigns were related to corruption and organized crime, employment, foreign investments, security, and local and municipal issues, rule of law and EU integration, and the opposition's critiques towards the long-term ruling of the governing party were present too.[35] As the campaigning focused on individuals rather than political ideologies or policies of the candidates, discriminatory, offensive, or nationalistic rhetoric was used every so often by the candidates.[36]

[29]OSCE/ODHIR, International Election Observation Mission Montenegro – Parliamentary Elections, Statement of Preliminary findings and conclusions, October 2016
[30]Council of Europe Report, Montenegro Media Sector Inquiry with Recommendations for Harmonisation with the Council of Europe and European Union standards, December 2017
[31]Idem
[32]WhatsApp and Viber Blocked on Election Day in Montenegro, Advox Global Voices, October 2016
[33]All accused of 'coup d'etat' found guilty, Radio Free Europe, May 2019
[34]Cyber Security Strategy for Montenegro 2018-2021, December 2017

However, during the campaign for Presidential elections in 2018, fundamental freedoms were respected, in particular equal access to public places, a public broadcaster, and free airtime, as well as freedoms of assembly, movement, and association.[37] According to the reports, the Agency for Electronic Media did not receive any media-related complaints.[38]

Although there are no exact data about the online political advertisement from the 2016 and 2018 elections period, the campaign strategies of the political parties and public opinion pool demonstrated the rising importance of social media for future elections. The public opinion research, conducted in 2017 before the elections, showed that for the voters the television is still the primary source of news, while Internet usage is growing throughout the years as online media have a wider reach.

Even though international community welcomes the progress Montenegro has made in filed of the freedom of speech and media, the media should actively cover the campaign in an impartial and professional manner, rather than relying on the coverage submitted by the political parties.[40] Concerning the hate speech, publicly hate speech and other forms of hatred remain the concern as intolerant political statements, especially around election times, as well as comments that contain abusive language, insults and hate speech towards other groups (national minorities, LGBTIQ population) do occur.[41]

With that regards, the latest elections in the region clearly indicate the rising role of online tools and social media during political campaigns. Considering the context of COVID-19 pandemic, while most of the traditional means of political campaigning are restricted, it is very likely that the campaigning in 2020 Parliamentary elections as well as during future elections in Montenegro will be conducted predominantly on social media.

[35]OSCE/ODHIR, International Election Observation Mission Montenegro – Presidential Election, Statement of Preliminary findings and conclusions, April 2018
[36]Idem
[37]Montenegro Presidential Election 2018, ODIHR Election Observation Mission Final Report, June 2018
[38]Idem
[39]Public Opinion Research, CISR-IPSOS, October 2017
[40]Montenegro Parliamentary Elections 2016, OSCE/ODIHR Election Observation Mission Final Report, January 2017
[41]ECRI report on Montenegro, Fifth Monitoring Cycle, September 2017

4. Comparative practice

The Internet and social media are extremely wide concepts, thus it is almost impossible to regulate it in all its segments, especially since this field overlaps with the spectrum of basic human rights, including the right to freedom of expression and opinion. However, the question is whether there is the possibility of controlling this field because we are witnessing many cases of abuse, violations, and inappropriate content being created daily. With that regard, many countries globally took certain measures in the form of adopting legal acts and regulations granting specific competencies to the national authorities, state bodies, and media outlets in terms of controlling and preventing abuses and violence on the Internet. This also because many media laws are practically inapplicable in the digital world.

The aim of this comparative section is to give an overview of national practices worldwide related to social media and cyber space. The examples, i.e. states presented below, are selected based on their increased efforts in field of social media regulations to protect fundamental human rights and freedoms of citizens online.

Key takeaways:

- Development of the practice on how to regulate and monitor social media is still ongoing
- Each country faces different threats concerning cybercrime and abuses on the Internet, thus a more unique approach - adapted to each country individually - is needed
- The legal solutions may give more control of the state about what is being created and shared online, however, it might bring forward censorship and violations of basic human rights such as freedom of expression
- Conducting reforms, in terms of introducing social media legal frameworks, may take longer period of time and its efficiency and impact could be under question as technology evolves on fast pace
- Existing domestic laws should be updated in line with technological developments to address the issue of abuse on social media.
- Implementation of new monitoring methodologies by the state institutions, i.e. capacity building, should be potentiated with regards to social media
- Improvement of cooperation between state institutions should be promoted, as well as between them and the private and CSO sector in this field (multistakeholder approach).

Germany

In December 2019 Germany approved the State Treaty on the modernization of media legislation **(State Media Treaty (MStV))**[42] that should enter into force in September 2020. With this Treaty, Germany simultaneously implement the amended European Parliament and Council Directive 2018/1808/EU[43] concerning the provision of audiovisual media services in view of changing market conditions.

The new Media Treaty expands its scope and includes also social media platforms, search engines, and video portals, subjecting them to independent, non-governmental oversight by Germany's media authorities (*Landesmedienanstalten*). Two significant obligations have been introduced: obligation of transparency and prohibition of discrimination. The obligation of transparency is related to algorithmic transparency, i.e. a clear presentation of the criteria according to which the contents are presented, as well as the announcement of changes in these criteria, while the discrimination provision essentially refers to the prohibition of discrimination against certain journalistic and editorial offers. The problem of the Treaty is insufficiently elaborated details such as not sufficiently defined standards for distinguishing appropriate from inappropriate content, but social

platforms have complete freedom of assessment in relation to their standards, as well as who all belong to the group of media intermediaries.

The amended Directive on audiovisual media services, as well as the new Treaty on the modernization on the media legislation are also the reasons for the federal government to draft the Law to amend **the Network Enforcement Act (NetzDG)**[44]. The existing NetzDG Law came into force in 2017, putting an obligation on social network platforms to crack down on hate speech and other extremist messaging on their digital platforms. However, in June 2020 German Parliament passed a reform that extends NetzDG by requiring companies to remove any content that is unlawful[45] within 24 hours of it being brought to their attention, with prescribed fines should they fail to comply. The law allows for up to seven days for the companies to decide on the content that has been flagged as offensive, but which may not be clearly defamatory or inciting violence. Also, the Law is placing a reporting obligation on platforms (every six months, companies will have to publicly report the number of complaints they have received and how they have handled them) which also requires them to report certain types of "criminal content" to the Federal Criminal Police Office.

A reform of the NetzDG Law remains ongoing. However, the main novelties of the law are: strengthened user rights, more user-friendly reporting channels, simplified enforcement of information claims, broadened transparency reporting requirements.

France

Following the German example, France also adopted a Law n° 2020-766[46] aimed at combating hateful content on the internet on June 24, 2020, requiring social platforms to remove illegal content such as hate speech based on race, nationality, gender, disability, or sexual orientation within 24 hours. Additionally, the contents linked to terrorism or child pornography must be removed within one hour, otherwise the given companies will be fined large amounts of money. Social media are required to report the amount of illegal content on an annual basis, for any concealment of information they will be penalized. The law was approved due to the spreading of misinformation regarding COVID-19.

Strong anti-hate speech law already existed in France often with criminal penalties, but those rules, instituted before the emergence of social media platforms have little sway online.

United Kingdom

Although the UK criminal law legislation applies to online activity in the same way as to offline activity, in August 2018, the Crown Prosecution Service has published guidance on offenses on social media.[47]

Additionally, in 2019 UK policymakers drafted an **Online Harms Law**[48] that would restrict certain violent and extremist content from being shared online. It is clearly stated that the legislative frameworks of Great Britain are not set wide enough and that changes are necessary regarding the regulation of the area of social networks. The new regulatory framework would cover social media companies, public discussion forums, retailers that allow users to browse products online, non-profit organizations, file-sharing web sites, and hosting providers.

[42]State Media Treaty (MStV), 2020
[43]European Parliament and Council Directive 2018/1808/EU amending Council Directive 2010/13/EU, European Parliament and Council, November 2018
[44]Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG), (Federal Law Gazette I, p. 3352 ff. , October 2017)
[46]Law n° 2020-766 (JORF no. 0156)
[47]Social Media - Guidelines on prosecuting cases involving communications sent via social media, UK Crown Prosecution Service, August 2018
[48]Online Harms White Paper, April 2019

Content monitoring should be carried out by an independent regulator. It is proposed here to strengthen the role of authority which has so far been involved in monitoring media and radio content. It is proposed that the platforms themselves clearly define what is meant by what is permitted and what is prohibited content and that these guidelines be clearly presented to the competent authority that would monitor this.

However, the law is still the draft and was criticized and some respondents raised concerns that it could impact freedom of expression online, lead to increased censorship and removal of non-harmful content.

When it comes to the institutional framework in the UK, many regulators have a role in relation to certain types of online activity e.g. Ofcom, the Competition and Markets Authority, the Advertising Standards Authority, the Information Commissioner's Office, and the Financial Conduct Authority.[49]

European Union

The European Parliament and Council **Directive 2018/1808/EU** amending Council Directive 2010/13/EU[50] extend the rules to social media services, which have become an important medium for information exchange and entertainment and education, including providing access to user-generated programs and videos.

The question - which social networks should be covered by this Directive - has been resolved by stating that these are all social networks whose main purpose is to provide the possibility of setting up programs and videos. If the posting of video content and sharing is a separate part of the service provided by a particular social network, then the Directive regulates only that part. Videos that are part of the content of electronic newspapers and animated images such as GIFs are not covered by this Directive. This Directive 2018/1808/EU does not regulate non-economic activities such as the provision of audio-visual content on private websites and non-commercial communities of interest. This directive lists ten tools that video providers should use to meet the requirements concern the protection of minors from inappropriate content. These tools relate to conditions such as age verification, parental control, and the possibility of adopting even stricter rules for video providers.

However, these measures do not represent too much of a burden for video providers, because they are already some of the measures they apply. The key novelty is that the video provider will be subject to the media regulator and will have to register. In addition, this Directive requires that 30% of catalogs must consist of European content.

The Directive on security of network and information systems (NIS Directive) 2016/1148[51] of the European Parliament and of the Council, adopted in 2016, concerns measures for a high common level of security of network and information systems across the Union. With the Directive a Cooperation Group was established to support and facilitate strategic cooperation, discussions and exchanges on good policy practices between the Member States regarding the security of network and information systems. It also provides that security and notification requirements should apply to operators of essential services and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported.

[50]European Parliament and Council Directive 2018/1808/EU amending Council Directive 2010/13/EU, European Parliament and Council, November 2018
[51]The Directive on security of network and information systems (NIS Directive) 2016/1148, European Parliament and the Council, July 2016

Council of Europe

Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries[52], adopted in 2018, calls on states to create a secure online environment where all parties, both users and platforms, know their rights and obligations. Within the document, search engines and social media are defined as internet intermediaries.

The Council proposes strengthening self-regulatory and co-regulatory mechanisms. Namely, it imposes obligations of States with respect to the protection and promotion of human rights and fundamental freedoms in the digital environment as well as the responsibilities of internet intermediaries with respect to human rights and fundamental freedoms that States should aim to ensure.

Provisions relating to state governments state that governments may interfere with Internet content only if it is regulated by law, and must be done in a manner consistent with that law. In addition, the scope of the Government's authority must be clearly stated to prevent possible abuses. Governments are required to verify that these platforms have clear and effective mechanisms for removing inadequate content. More transparency is required from service providers on how to apply restrictions to content. When restricting the content, it must be clearly stated on what legal basis the given content is restricted. One of the issues that is extremely problematic and requires to be regulated is the issue of social bots, these are algorithmically controlled accounts that mimic the activity of human users but operate at a much faster pace. Service providers must provide detailed information on how algorithmic and automated tools work. In order for a government to control a particular algorithm, it must possess comprehensive information that may conflict with some of the basic human rights.

Moreover, while implementing the Recommendation, states and intermediaries are obliged to fulfill their responsibilities to respect human rights in line with **the United Nations Guiding Principles on Business and Human Rights**[53] and the Recommendation **CM/Rec(2016)3** of the Committee of Ministers to member States on human rights and business[54].

When it comes to social media and online contents, Council of Europe provides its Member States with a number of recommendations, just to mention: Recommendation CM/Rec(2016)5 on Internet freedom[55], Recommendation CM/Rec(2016)1 on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality[56], Recommendation CM/Rec(2015)6 on the free, transboundary flow of information on the Internet[57], Recommendation CM/Rec(2014)6 on a Guide to human rights for Internet users[58], Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines[59], Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services[60], etc.

[52]Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, Council of Europe, March 2018
[53]United Nations Guiding Principles on Business and Human Rights, UN Office of the High Commissioner, 2011
[54]Recommendation CM/Rec(2016)3, Council of Europe, March 2016
[55]Recommendation CM/Rec(2016)5, Council of Europe, April 2016
[56]Recommendation CM/Rec(2016)1, Council of Europe, January 2016
[57]Recommendation CM/Rec(2015)6, Council of Europe, April 2015
[58]Recommendation CM/Rec(2014)6, Council of Europe, April 2014
[59]Recommendation CM/Rec(2012)3, Council of Europe, April 2012
[60]Recommendation CM/Rec(2012)4, Council of Europe, April 2012

USA

In the USA, there is no federal or state laws that expressly govern social media sites and online content. The current legal framework is composed of **the Constitution of the United States (First Amendment)**[61] and **Section 230 of the Communications Decency Act of 1996 (CDA)**[62].

Namely, the First Amendment provides protection against state action when individuals have alleged the violation of their free speech rights online. The First Amendment generally protects the freedom of speech but its protections do not apply in the same way in all cases as not every government regulation, affecting content posted on social media sites, would be analyzed in the same way. However, the First Amendment does not prohibit the regulation of conduct.

The actions of private companies are regulated by Section 230 of the Communications Decency Act. The CDA is known as the most important law protecting internet speech. However, the CDA's Section 230 provides broad immunity to interactive computer service providers, including social media providers. Section 230 provides immunity from any lawsuit that seeks to hold a service provider liable for publishing information that was created by an information content provider, effectively protecting social media sites from liability for hosting content. Also, it provides immunity for sites that take „good faith action" to restrict access to content that the provider or users deem obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.

In 2019 the Biased Algorithm Deterrence Act[63] was introduced, which would consider any social media service that used algorithms to moderate content without the user's permission or knowledge to be legally considered a publisher, not a platform, thereby removing Section 230's protections. The Ending Support for Internet Censorship Act[64] was also introduced, which would require that, in order to be granted Section 230 protections, social media companies would have to show the Federal Trade Commission (FTC) that their content moderation practices were politically neutral. However, neither of those bills went anywhere. The latest attempt is a bipartisan bill - the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT)[65] introduced in March 2020. This act is aimed at the prevention of child pornography as an avenue to both erode Section 230 and end encryption by requiring companies to follow a set of "best practices" or else lose their Section 230 immunity due to child pornography charges.

Bearing in mind presented legal framework, in the USA, users' rights on social media platforms are governed primarily by the private policies created by information service providers and companies.

Mexico

Besides above presented legal attempts to regulate social media and protect users rights, Mexico is in particular interesting case for this comparative section as its gives an example of regulating social media throughout the use of national tactics to deter corruption.

Namely, the Superior Chamber of the Electoral Tribunal of Mexico confirmed the judgement issued by the Monterrey Regional Chamber of the Electoral Tribunal in which it annulled the election of federal representatives in one polling station during Legislative and Local elections, held in Mexico in 2015.[66] The judgement stated that the election results from one polling station were annulled as the Governor violated the impartiality and equality

[61] *Constitution of the United States, First Amendment*
[62] *Communications Decency Act, 47 U.S. Code, Section 230 - Protection for private blocking and screening of offensive material*
[63] *Biased Algorithm Deterrence Act, H.R.492 — 116th Congress (2019-2020), 2019*
[64] *Ending Support for Internet Censorship Act, S.1914 — 116th Congress (2019-2020)*
[65] *EARN IT Act, S.3398 — 116th Congress (2019-2020), 2020*
[66] *Electoral Tribunal of Mexico, Case PAN v. PRI (SM JIN 0035 2015)*

of elections because his involvement in the election became public knowledge. The Governor posted photos on his personal Twitter account which was transitioned to the official webpage of the government, including him traveling to polling stations with candidates. The photos published on social networks were used as evidence suggesting a violation of impartiality and abuse of state resources.[68]

In this way, a different perspective on how to regulate social media is presented. Furthermore, this example shows that not all aspects of abuses on social media are (or should be) regulated by the specific law, but the activities of the state bodies and their capacity to use social media as a tool to monitor violations are crucial, in particular during elections and campaigning.

[67] *Idem*
[68] *Idem*

Conclusions and Recommendations

Based on the analysis of legal and institutional framework, as well of experiences from 2016 and 2018 Elections in Montenegro, it is obvious that further improvements considering the protection of citizens' rights and fundamental freedoms on the Internet are necessary.

With the development and progress in the field of information technology, internet service providers also suffer cyber-attacks on their infrastructure. However, there is no coordinated response, such as safe communication channels at the national level in order to resolve such situations. Another significant problem is that in Montenegro there is no defined way to monitor or record malicious flow of data entering the country.

Through the analysis of comparative practice, it is demonstrated there are a variety of attempts for regulating the spreading of unlawful and harmful contents within social media, as well as to protect and secure cyberspace worldwide. However, different institutional and legal, as well as the cultural background of each country in great measure determines which mechanism and regulations fit the best, in order to assure full enjoyment and protection of digital rights of users, i.e. citizens. For example, even though Germany made a great contribution concerning the responsibility of media intermediaries, thanks to the high level of independence of media in the country, it is not likely that the same mechanism could be replicated in other countries or EU Member States where the level of media independence is lower.

Still, the need to regulate the field of the Internet and secure the cyberspace remains the necessity of the modern world with the aim to prevent possible abuses and violations of fundamental freedoms and the human rights of the users. A brief overview of some of the key recommendations that emerged from the analysis are set out below.

Key recommendations

For public sector:

- Provisions about restriction to state employees being banned from engaging in campaigning while on duty or a mandate to maintain impartiality and political neutrality may need to be explicitly updated to address the use of personal social media accounts.
- National authorites may consider improving domestic anti-corruption tactics to regulate usage of social media, in particular during elections and political campaigns.
- Adopt more cooperative manner when building mechanisms to support at-risk users in a coordinated manner with multi-stakeholder approach that could include physical security support, legal support, awareness raising, and digital security support.
- Scale-up training activities for law enforcement officials and the judiciary on hate crime, online offenses, cybercrimes, by conducting seminars/conferences/courses on international standards and case-law concerning protection of digital rights, as well as for conducting efficient investigations and legal proceedings relating to online offenses.

For CSOs and media:

- Strengthen digital literacy skills of citizens, in particular of younger population through formal and informal education with the aim to educate, inform, and sensitize the youth about information system security, online risks, abuses, and how to protect their rights and freedoms, in particular during elections.
- Conduct awareness-raising informative campaign for public about online ads, manipulations, violations of users' rights online, and mechanisms of protection.

Literature

1. Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Council of Europe, 2003
2. All accused of 'coup d'etat' found guilty, Radio Free Europe, May 2019
3. Biased Algorithm Deterrence Act, H.R.492 — 116th Congress (2019-2020), 2019
4. Communication Rules, Commission for the Implementation of the Communication Strategy. Government of Montenegro, 2019
5. Communication Strategy 2018-2020, Government of Montenegro, 2018
6. Communications Decency Act, 47 U.S. Code, Section 230 - Protection for private blocking and screening of offensive material
7. Constitution of Montenegro (Official Gazette of Montenegro, no. 1/2007 and 38/2013 - Amendmentsi I-XVI)
8. Constitution of the United States, First Amendment
9. Convention on Cybercrime (Budapest Convention), Council of Europe, 2001
10. Council of Europe Report, Montenegro Media Sector Inquiry with Recommendations for Harmonization with the Council of Europe and European Union standards, Council of Europe, 2017
11. Criminal Code of Montenegro (Official Gazette of the Republic Montenegro, no. 70/2003, 13/2004, 47/2006, and Official Gazette of Montenegro, no. 40/2008, 25/2010, 32/2011, 64/2011, 40/2013, 56/2013, 14/2015, 42/2015, 58/2015, 44/2017, and 49/2018)
12. Cyber Security Strategy for Montenegro 2013-2017, July 2013
13. Digital 2020: Montenegro, Datareportal, January 2020
14. Digital Democracy Project, Research Memo 7, Public Policy Forum, October 2019
15. EARN IT Act, S.3398 — 116th Congress (2019-2020), 2020
16. ECRI report on Montenegro, Fifth Monitoring Cycle, September 2017
17. Electoral Tribunal of Mexico, Case PAN v. PRI (SM JIN 0035 2015)
18. Ending Support for Internet Censorship Act, S.1914 — 116th Congress (2019-2020)
19. European Parliament and Council Directive 2018/1808/EU amending Council Directive 2010/13/EU, European Parliament and Council, November 2018
20. House of Commons, Social Media Regulation, Briefing Paper, Number 8743, February 2020
21. Joint Guidelines for Preventing and Responding to Misuse of Administrative Resources during Electoral Process, Venice Commission and OSCE/ODIHR, 2016
22. Law n° 2020-766 (JORF no. 0156)
23. Law on Civil Servants and State Employees (Official Gazette of Montenegro, no. 2/2018 and 34/2019)
24. Law on Courts (Official Gazette of Montenegro, no. 011/15)
25. Law on Election of MPs and Councilors (Official Gazette of RoM, no. 16/2000, 9/2001, 41/2002, 46/2002, 45/2004, 48/2006, 56/2006 and Official Gazette of Montenegro, no. 46/2011, 14/2014, 47/2014, 12/2016, 60/2017, and 10/2018)
26. Law on Electronic Commerce (Official Gazette of RoM, 80/04)
27. Law on Electronic Communications (Official Gazette of Montenegro, no. 40/2013)
28. Law on Electronic Media (Official Gazette of Montenegro no. 046/10, 040/11, 053/11, 006/13, 055/16, 92/2017, 82/2020)
29. Law on Information Security (Official Gazette of Montenegro, no 014/10 and 040/16)

30. Montenegro Parliamentary Elections 2016, OSCE/ODIHR Election Observation Mission Final Report, January 2017
31. Montenegro Presidential Election 2018, ODIHR Election Observation Mission Final Report, June 2018
32. Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG), Federal Law Gazette I, p. 3352 ff. , October 2017
33. Ohman, M. (Ed.), Training in Detection and Enforcement (TIDE): Political Finance Oversight Handbook, International Foundation for Electoral Systems (IFES), 2013
34. Online Harms White Paper, April 2019
35. OSCE/ODHIR, International Election Observation Mission Montenegro – Parliamentary Elections, Statement of Preliminary findings and conclusions, October 2016
36. OSCE/ODHIR, International Election Observation Mission Montenegro – Presidential Election, Statement of Preliminary findings and conclusions, April 2018
37. Public Opinion Research, CISR-IPSOS, October 2017
38. Recommendation CM/Rec(2012)3, Council of Europe, April 2012
39. Recommendation CM/Rec(2012)4, Council of Europe, April 2012
40. Recommendation CM/Rec(2014)6, Council of Europe, April 2014
41. Recommendation CM/Rec(2015)6, Council of Europe, April 2015
42. Recommendation CM/Rec(2016)1, Council of Europe, January 2016
43. Recommendation CM/Rec(2016)3, Council of Europe, March 2016
44. Recommendation CM/Rec(2016)5, Council of Europe, April 2016
45. Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, Council of Europe, March 2018
46. Social Media - Guidelines on prosecuting cases involving communications sent via social media, UK Crown Prosecution Service, August 2018
47. Cyber Security Strategy for Montenegro 2018-2021, December 2017
48. The Code of Ethics (Official Gazette of Montenegro, no. 050/18)
49. The Criminal Procedure Code (Official Gazette of Montenegro, no. 57/09)
50. The Directive on security of network and information systems (NIS Directive) 2016/1148, European Parliament and the Council, July 2016
51. United Nations Guiding Principles on Business and Human Rights, UN Office of the High Commissioner, 2011
52. WhatsApp and Viber Blocked on Election Day in Montenegro, Advox Global Voices, October 2016


CeMI