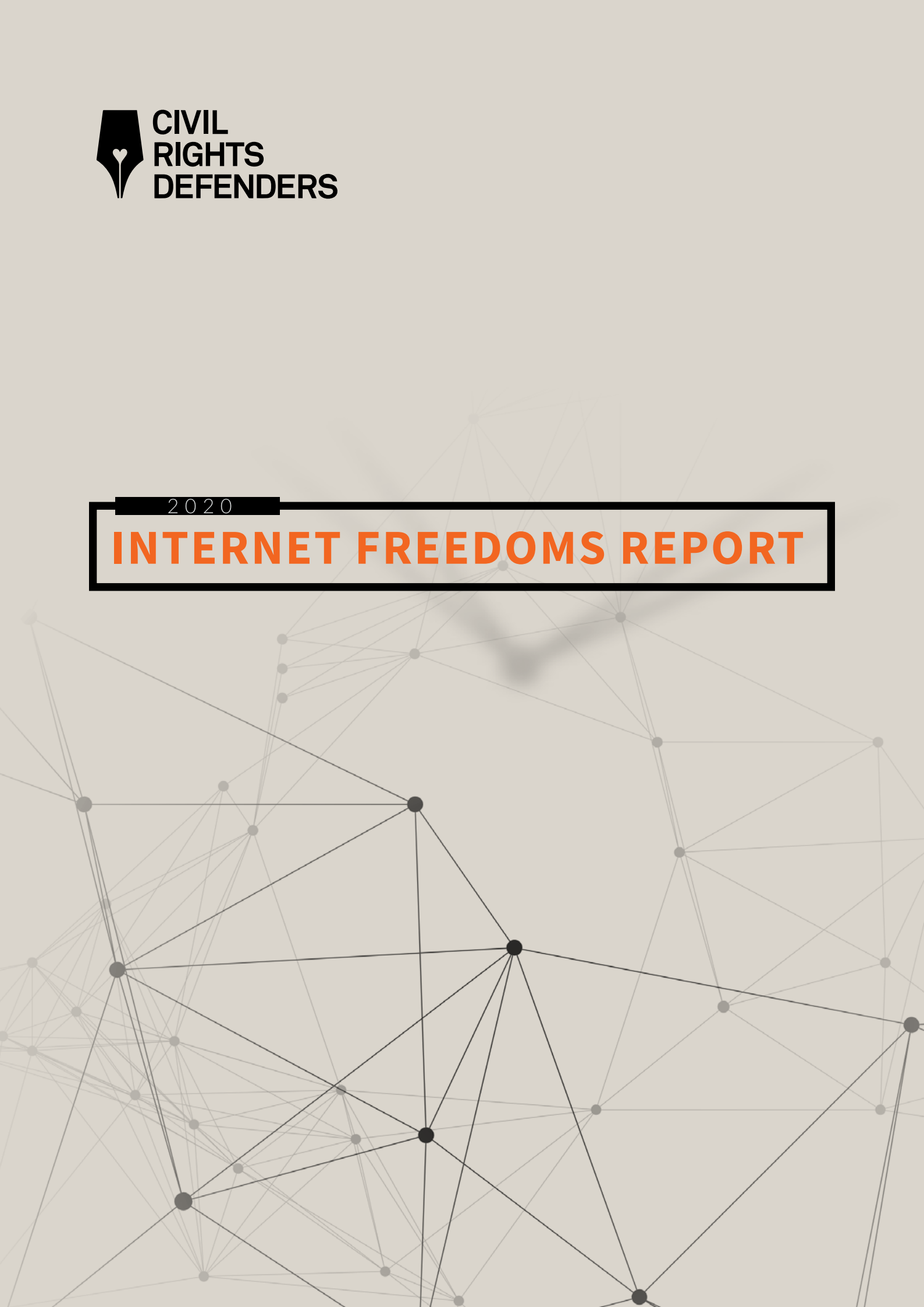




2020

INTERNET FREEDOMS REPORT



IMPRESSUM

Published by

Civil Rights Defenders

For Publisher

Goran Miletic

Authors

SHARE Foundation

Andrej Petrovski

Bojan Perkov

Kristina Cendic

Filip Milosevic

Editors

Neda Mirkovic

Philip Merrell

Design

Marko Kovachevski

INTERNET FREEDOMS IN THE WESTERN BALKAN REGION

INTRODUCTION

Governments in the Western Balkans have continuously jeopardized the right to freedom of expression by shutting down media outlets, social movements' pages and intimidating individual activists online. Furthermore, there is a growing tendency of introducing legislation aimed at censorship of online content. There are also rising concerns in terms of surveillance and lack of efficient personal data protection of citizens. Such measures limit and restrict civic participation and undermine the very foundation of democracy.

The European Convention on Human Rights and recommendations made by the Council of Europe emphasize that member states are responsible for the implementation of human rights and fundamental freedom standards in regards to the internet. More importantly, member states have an obligation to their citizens to respect, protect and promote human rights and fundamental freedoms on the internet.

Civil Rights Defenders in cooperation with SHARE Foundation conducted research on the state of internet freedoms in Serbia, Bosnia and Herzegovina, Kosovo and Albania. This report provides a comparative overview of specific indicators and develops a set of recommendations for governments of these countries to improve the state of citizens' freedoms online.

The indicators for the research were based upon internet freedom indicators included in the Council of Europe Recommendation CM/Rec(2016)5 on internet freedom and adapted in accordance with the local social context. They specifically cover 4 main areas: (1) an enabling environment for internet freedom, (2) the right to freedom of expression, (3) the right to freedom of peaceful assembly and association and (4) the right to private and family life. Each group of indicators provides a deeper insight into the defined area through sub-indicators, which vary in numbers depending on the complexity of the topic.

Such research is necessary to map the most problematic areas in each country and at the same time analyze risks which are common to citizens across the region. This holistic approach is crucial to ensure that recommendations are both practically applicable and of critical importance for the future of internet freedoms in the Western Balkans.

SERBIA

1. AN ENABLING ENVIRONMENT FOR INTERNET FREEDOM

1.1. The protection of human rights and fundamental freedoms on the internet is guaranteed in law, in full compliance with relevant articles of the European Convention on Human Rights (ECHR).

The Republic of Serbia ratified the ECHR in 2003, meaning that the ECHR became part of Serbia's legal system, therefore guaranteeing all human rights and freedoms prescribed by the Convention.¹ The Constitution of the Republic of Serbia, adopted in 2006, although not explicitly mentioning the internet, ensures that human and minority rights are guaranteed by the generally accepted rules of international law, and those confirmed by international treaties and laws are directly applicable.²

1.2. Laws and policies relating to the internet are assessed, at their drafting stage, with regard to the impact that their implementation may have on the exercise of human rights and fundamental freedoms in an inclusive and transparent process which enables the participation of all stakeholders, including the private sector, civil society, academia and the technical community.

The Government of Serbia, i.e. the relevant Ministries, regularly publishes information on public discussions about laws related to the internet and call all relevant stakeholders (academia, civil sector, ICT sector, etc.) to participate. However, there are examples of adopting laws without any public discussion, such as the Law on Critical Infrastructure, the first law regulating this matter in Serbia.³

1.3. Any state body which has regulatory or other competence over internet matters carries out its activities free from political or commercial interference, in a transparent manner and protects and promotes internet freedom.

In terms of independent regulators, there is no state authority specifically overseeing internet content in Serbia in general. The Regulatory Agency for Electronic Communications and Postal Services (RATEL) oversees technical and infrastructure aspects. On the other hand, content of websites which are registered with the Business Registers Agency of Serbia as online media fall under the jurisdiction of the Ministry of Culture and Information, which oversees the application of the Law on Public Information and Media.⁴

1.4. The state protects individuals from cybercrime through effective criminal justice or other measures. Notably they are prescribed by a law, which is accessible, precise, clear and foreseeable; pursue a legitimate aim; are necessary and proportionate in a democratic society and allow for effective remedies.

The Republic of Serbia has ratified the Budapest Convention on Cybercrime in 2009.⁵ Serbia incorporated the elements of the Budapest Convention into criminal law, specifically the Criminal Code of Serbia, which has a separate section only prescribing criminal acts against the security of computer systems (Chapter 27, Articles 298-304a).⁶ There is also a special prosecution office for cybercrime within the High Public Prosecution Office in Belgrade, i.e. the Special Prosecution Office for Cybercrime, led by the Special Prosecutor for Cybercrime. There is also a special unit for cybercrime within the Ministry of Interior, i.e. the Unit for Combating Cybercrime, which operates as a part of the Service for Combating Organized Crime. Also, in 2018, the Government of Serbia adopted the Strategy for Combating Cybercrime from 2019 to 2023, where it is mentioned that Serbia still needs to align the national legal framework with the EU 2013/40/EU Directive on attacks against information systems.⁷

¹ Law on the Ratification of the Convention (Official Gazette of Serbia and Montenegro, No. 9/2003, 5/2005, 7/2005 - corr. and Official Gazette of the Republic of Serbia, No. 12/2010 and 10/2015).

² Constitution of the Republic of Serbia, (Official Gazette of the Republic of Serbia, No. 98/2006).

³ SHARE CERT, The first Law on Critical Infrastructure adopted without public debate, 30 October 2018, Belgrade.

⁴ Law on Public Information and Media (Official Gazette of the Republic of Serbia, No. No 83/2014, 58/2015 and 12/2016).

⁵ Law on the Ratification of the Convention on Cybercrime, (Official Gazette of the Republic of Serbia, No.19/09).

⁶ Criminal Code of Serbia, (Official Gazette of RS, Nos. 85/2005, 88/2005, 107/2005), Chapter 27, Articles 298-304a.

⁷ Strategy for the Fight against Cyber Crime for the period 2019-2023, Pursuant to the Law on Government (Official Gazette of the Republic of Serbia, No. 55/05, 71/05 - corr., 101/07, 65/08, 16/11, 68/12 - US, 72/12, 7/14 - US, 44/14 and 30/18 - state law).

1.5. The state provides media and digital literacy programmes for internet users.

There are programmes and endeavors which aim to increase the digital literacy of the population of Serbia, especially among children and teens. One such endeavor is “Smart and Safe” platform which offers educational and promotional projects in order to contribute to the development of digital literacy, digital competences and digital security of citizens of Serbia, especially youth, women and people with disabilities. Programs to support IT communities, the IT industry, the application of ICT into the economy, staff development and employment in this sector are also encouraged.

2. THE RIGHT TO FREEDOM OF EXPRESSION

2.1. Freedom to access the internet

2.1.1. The internet is available, accessible and affordable to all groups of the population without any discrimination.

There is no discrimination regarding internet access to any group of the population. The Law on Electronic Communications clearly states that among the objectives and principles of regulating the electronic communications sector is “ensuring maximum benefits to users of electronic communications, including persons with disabilities, the elderly and socially vulnerable users, especially regarding the choice, price and quality of services” (Article 3, Paragraph 1, Point 8).⁸

2.1.2. The public has access to the internet in facilities supported by public administration (internet access points), educational institutions or private owners (universal community service).

In certain cases, internet access is provided to the public when it comes to access to the internet in educational institutions. One of the best examples of this is the Academic Network of Serbia (AMRES), founded by the Government of the Republic of Serbia for the purpose of building, developing and managing education and scientific-research computer networks of the Republic of Serbia. To educational and research organisations and other users, this network provides access and use of the internet and information services nationally, as well as connection with other national and international networks. AMRES is one of the most significant resources for scientific, research and academic work in Serbia. Development of AMRES started in the 1990s with the networking of several major faculties, which resulted in the creation of a state-of-the art computer network in Serbia, which currently has more than 300 connected scientific, research and educational institutions, with over 150,000 end users.

2.1.3. The state takes reasonable measures to ensure access to the internet to those with low income, in rural or geographically remote areas and those with special needs such as persons with disabilities.

According to the Law on Electronic Communications, the availability of the universal service to all citizens of the Republic of Serbia and meeting the needs of specific social groups, including persons with disabilities, the elderly and socially vulnerable users must be ensured by law (Article 3, Paragraph 1, Point 4). Also, the same law has a whole chapter dedicated to universal service (Articles 55-58), which in detail prescribes the provision of universal services in Serbia.⁹

2.1.4. There are no general, nationwide restrictions on access to the internet.

There is no state mandated blocking or filtering of internet content on the national level. Internet shutdowns also do not occur in Serbia.

2.2. Freedom of opinion and the right to receive and impart information

2.2.1. Any measure taken by state authorities or private-sector actors to block or otherwise restrict access to an entire internet platform or information and communication technologies, tools, or any request by state authorities to carry out such actions complies with the conditions of Article 10 of the ECHR.

The Constitution of the Republic of Serbia states in Article 50, Paragraph 2 that there is no censorship in the Republic of Serbia and that the relevant court may prevent the dissemination of information and ideas through mass media only if it is necessary in a democratic society to prevent the invocation of violent overthrow of the constitutionally established order or to endanger the territorial integrity of the Republic of Serbia, to prevent the propagation of war or inciting direct violence, or to prevent advocating racial, national or religious hatred, or inciting discrimination, hostility or violence.¹⁰

⁸ Law on Electronic Communications, (Official Gazette of the Republic of Serbia, No.44/10).

⁹ Law on Electronic Communications, (Official Gazette of the Republic of Serbia, No.44/10).

¹⁰ Constitution of the Republic of Serbia, (Official Gazette of the Republic of Serbia, No. 98/2006).

2.2.2. Internet service providers as a general rule treat internet traffic equally and without discrimination on the basis of sender, receiver, content, application, service or device.

The Law on Electronic Communications provides for the principle of net neutrality in Article 3, Paragraph 1, Point 11, which clearly states that the end-users of public communications networks and services should be enabled to have free access to and distribution of information, and to use applications and services of their choice.¹¹

2.2.3. Internet users or other interested parties have access to a court in compliance with Article 6 of the Convention with regard to any action taken to restrict their access to the internet or their ability to receive and impart content or information.

In Article 22, the Constitution of Serbia prescribes that everyone has the right to judicial protection if he or she has been violated or denied a human or minority right enshrined in the Constitution, as well as the right to remedy the consequences of the violation. Under the same article, citizens have the right to apply to international institutions for the protection of their freedoms and rights guaranteed by the Constitution. Article 32 (Right to a fair trial) essentially incorporates Article 6 of the Convention.¹²

2.3. Freedom of the media

2.3.1. The editorial independence of media operating on the internet is guaranteed in law, policy and practice.

Article 4 of the Law on Public Information and Media prescribes the freedom of public information, meaning that public information is free and not subject to censorship. The law also prohibits direct and indirect discrimination against editors of the media, journalists and other persons in the field of public information, especially according to their political orientation and belief or other personal capacity. The law also guarantees free flow of information through the media, as well as that the editorial autonomy of the media must not be jeopardized, in particular by pressures, threats or blackmail of editors, journalists or sources of information. The physical assault on an editor, journalist and other persons involved in gathering and publishing information through the media is punishable by law. The freedom of public information must not be infringed by abuse of office or public authority, property or other rights, or the influence and control of the media and newspapers or electronic communications networks used to distribute media content.¹³

Pressures on media outlets are common, especially in smaller communities. According to Independent Journalists' Association of Serbia (IJAS), a news portal from the northern region of Vojvodina announced in February 2019 that it will stop with reporting on political topics because of pressures.¹⁴

2.3.2. Media are not required to obtain permission or a licence from the government or state authorities, beyond business registration, in order to be allowed to operate on the internet or blog.

The Law on Public Information and Media does not require online media outlets to obtain permission from the government or state authorities to start publication. In addition, according to Article 30, Paragraph 2 of the Law on Public Information and Media, online platforms are legally considered media only if they willingly choose to register with the Media Registry operated by the Business Registers Agency of Serbia.¹⁵

2.3.3. Journalists and other media actors using the internet are not subject to threats or harassment by the state. They do not practise self-censorship because of fear of punishment, harassment or attack.

The experiences with media freedom in practice are quite negative, which was highlighted in the latest reports of international organizations such as Freedom House and Reporters Without Borders. In their latest country ranking, Freedom House explained that Serbia's status changed from “Free” to “Partly Free” in part because of the “continued attempts by the government and allied media outlets to undermine independent journalists through legal harassment and smear campaigns”. Journalists working for investigative portals, such as Crime and Corruption Reporting Network (Mreža za istraživanje kriminala i korupcije - KRIK), Balkan Investigative Reporting Network (BIRN), or Center for Investigative Journalism of Serbia (Centar za istraživačko novinarstvo Srbije - CINS), are often targeted because of their reporting.¹⁶

Also, Reporters Without Borders put Serbia at 90th place in the World Press Index, which is a 14-place decline compared to 2018. RSF stated that “...Serbia has become a place where practicing journalism is neither safe nor supported by the state. The number of attacks on media is on the rise, including death threats, and inflammatory rhetoric targeting journalists increasingly comes from government officials.”¹⁷

¹¹ Law on Electronic Communications, (Official Gazette of the Republic of Serbia, No.44/10).

¹² Constitution of the Republic of Serbia, (Official Gazette of the Republic of Serbia, No. 98/2006).

¹³ Law on Public Information and Media (Official Gazette of the Republic of Serbia, No. No 83/2014, 58/2015 and 12/2016).

¹⁴ Z. Strika, New portal gave up reporting on political topics due to pressures and insults, Independent Journalists Association of Serbia, 28 February 2019.

¹⁵ Law on Public Information and Media (Official Gazette of the Republic of Serbia, No. No 83/2014, 58/2015 and 12/2016).

¹⁶ Freedom House Report, Serbia 2019.

¹⁷ Reporters without Borders, Serbia.

2.3.4. The confidentiality of journalists' and other media actors' sources is protected in law and respected in practice. Article 52 of the Law on Public Information and Media prescribes protection of journalists' sources, except for information relating to criminal offenses or the perpetrator of crimes, for which a sentence of imprisonment of at least five years is prescribed, if the information for that criminal offense cannot be obtained otherwise. Recently, a journalist of "Južne vesti" news portal was under pressure from the police in Niš to reveal a source of his story about malversations in one city municipality, but the Prosecutor dropped the charges against him.¹⁸

2.3.5. Media websites and websites of new media actors are not affected by cyber-attacks or other action disrupting their functioning.

Since 2014, when SHARE Foundation started monitoring the state of digital rights and freedoms in Serbia, there have been a lot of cases of technical attacks against online media outlets, including distributed denial of service (DDoS) attacks, unauthorized access, unauthorized alterations of content, malware injection, etc. It should be noted that targets of technical attacks are media organizations critical of the Government's actions. For example, the online portal "Peščanik" was targeted multiple times with technical attacks in the summer of 2014, after they had published a research article about the plagiarized PhD thesis of Nebojša Stefanović, Minister of Interior and a high-ranking member of the ruling Serbian Progressive Party.¹⁹

2.3.6. There are prompt and effective investigations of threats and crimes against journalists and new media actors. There is no climate of impunity.

In the past several years there were often cases of attacks on journalists in Serbia, such as threats and intimidations, that were unanswered by authorities. According to the Criminal Code of Serbia, endangering the security of journalists because of their work is punishable with a prison sentence from 6 months to 5 years, which is the same level of protection that the highest-ranking state officials have. However, even when those who endanger the security of journalists are found, court proceedings in these cases are known to have significant delays. Also, in December 2016, journalists' associations, the Ministry of Interior and the Republic Public Prosecution Office signed an Agreement on cooperation and measures to raise the level of security for journalists, but it has not yielded expected results.

3. THE RIGHT TO FREEDOM OF PEACEFUL ASSEMBLY AND ASSOCIATION

3.1. Individuals are free to use internet platforms, such as social media and other Information and Communication Technologies (ICTs) in order to associate with each other and to establish associations, to determine the objectives of such associations, to form trade unions, and to carry out activities within the limits provided for by laws that comply with international standards.

Article 54 of the Constitution guarantees the freedom of assembly, i.e. that peaceful assembly of citizens is free, stating that indoor gatherings are not subject to approval or registration. Meetings, demonstrations and other gatherings of citizens outdoors need to be reported to the state authority, in accordance with the law, but with no restrictions in regard to the internet. Also, it is prescribed that the freedom of assembly may be restricted by law only if it is necessary for the protection of public health, morals, rights of others or the security of the Republic of Serbia.²⁰

3.2. Associations are free to use the internet in order to exercise their right to freedom of expression and to participate in matters of political and public debate.

In line with regulations referring to public assemblies, there are no restrictions imposed on associations regarding their right to freedom of expression and participation in political and public debates in the online sphere.

3.3. Individuals are free to use internet platforms, such as social media and other ICTs in order to organise themselves for purposes of peaceful assembly.

According to the Constitution and the Law on Public Assemblies regarding public assemblies, there are no restrictions to freedom of use of the Internet, for the purposes of peaceful assembly.

18 M. Zirojevic, After the reports of Mediana PR, the police asks journalist of 'Juzne vesti' to reveal the source, 20 December 2018.

19 SHARE Foundation Monitoring Database and SHARE Foundation Digital rights monitoring reports.

20 Law on Public Gatherings, (Official Gazette of the Republic of Serbia, No. 6/2016).

4. THE RIGHT TO PRIVATE AND FAMILY LIFE

4.1. Personal data protection

4.1.1. The right to private and family life is guaranteed in compliance with Article 8 of the Convention. Any restriction to this right pursues one of the legitimate aims exhaustively enumerated in Article 8 of the Convention, is necessary in a democratic society and proportionate to the legitimate aim pursued. The law guarantees that all personal data is protected in compliance with Article 8 of the Convention and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) in States which have ratified it.

Serbia has ratified the European Convention on Human Rights and therefore accepted Article 8 of the Convention, however the Constitution of Serbia does not mention privacy as a right per se. The right to privacy is covered in the Constitution with three rights: inviolability of dwellings (Article 40), secrecy of letters and other means of communication (Article 41) and personal data protection (Article 42). Serbia has also ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) in 2006.²¹ Serbia's new Law on Personal Data Protection was adopted in 2018 and started being applied in August 2019. It is based upon European Union's General Data Protection Regulation (GDPR).²²

4.1.2. Personal data are processed lawfully (with the unambiguous consent of the data subject or on the basis of law) for legitimate purposes and not in excess of such purposes, accurately and securely.

The Law on Personal Data Protection clearly states that personal data must be processed lawfully, fairly and transparently in relation to the data subject and be collected for purposes that are specifically specified, explicit, justified and lawful and cannot still be processed in a manner inconsistent with those purposes (Article 5). However, the annual reports of the Commissioner for Information of Public Importance and Personal Data Protection show a lot of problems in the application of the law.²³ In the annual report for 2018, the Commissioner stated that the activities of his office could not prevent numerous cases of unauthorized, excessive or unprotected processing of personal data, or misuse of data for political purposes, because of the lack of strategic measures and support of other authorities in the field of personal data protection. Moreover, even though it is the Commissioner's belief that the Office provided enough elements for criminal prosecution to be initiated for personal data abuses, the vast majority of criminal complaints they submitted were dismissed. Also, the Commissioner states the of misdemeanor courts' policy of issuing fines is rather lenient, particularly in relation to responsible persons who are, practically as a rule, fined at the legal minimum.²⁴

4.1.3. Individuals are not subjected to a decision significantly affecting them based solely on automated processing of data without having their views taken into account.

The Law on Personal Data Protection (Article 38) provides data subjects with the right not to be subject to a decision made solely on the basis of automated processing, including profiling, if that decision produces legal consequences for that person or that decision significantly affects his or her position.

4.1.4. There are effective processes enabling every individual to obtain, on request, information on the processing of his or her personal data and the reason underlying processing; to object to processing; to obtain, on request, rectification or erasure of the personal data; and to consent to, object to or withdraw consent to personal data processing or profiling. An effective remedy exists for individuals when these rights are not respected. Legal frameworks for personal data protection provide adequate safeguards for access to information and freedom of expression.

The Law on Personal Data Protection provides data subjects with rights regarding their data, such as access, copy, rectification, deletion, portability, etc. Citizens can appeal to the Commissioner for Information of Public Importance and Personal Data Protection or to the courts.

4.1.5. The law defines the duties of public and private entities with regard to processing of personal data.

The Law on Personal Data Protection clearly defines the principles of data processing in Article 5 and obliges all entities, public or private, to be responsible for their application in practice.

4.1.6. A supervisory authority, which acts with complete independence and impartiality, ensures compliance with data protection legal frameworks.

Serbia's data protection authority is the Commissioner for Information of Public Importance and Personal Data Protection, an independent state body which oversees the application of the Law on Personal Data Protection.

21 Council of Europe, Chart of signatures and ratifications of Treaty 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Status as of 03/02/2020.

22 Law on Personal Data Protection, (Official Gazette of the Republic of Serbia, No.87/18).

23 Commissioner for Information of Public Importance and Personal Data Protection, Annual Reports.

24 Commissioner for Information of Public Importance and Personal Data Protection, The summarized annual report for 2018.

4.1.7. The state does not prohibit, in law or in practice, anonymity, pseudonymity, confidentiality of private communications or the usage of encryption technologies. Interference with anonymity and confidentiality of communications is subject to the requirements of legality, legitimacy and proportionality of Article 8 of the Convention.

The state does not prohibit anonymity, pseudonymity, confidentiality of private communications. Confidentiality of all communications is guaranteed by the Constitution (Article 41).

4.2. Surveillance

4.2.1. The access to the content of communications is regulated and it done in accordance with Article 8 of the ECHR.

The Constitution of Serbia in Article 41 guarantees the secrecy of letters and other means of communication. Also, deviations are allowed only for a limited time and on the basis of a court decision, if they are necessary for the purpose of conducting criminal proceedings or protecting the security of the Republic of Serbia, in the manner prescribed by law. The Law on Electronic Communication in Article 126 regulates the access to communication in a way that the interception of electronic communications revealing the content of the communication is not allowed without the consent of the user, except for a limited time and on the basis of a court decision, if necessary for the purpose of conducting criminal proceedings or protecting the security of the Republic of Serbia, in the manner prescribed by law.

4.2.2. Operators of electronic communications are obliged by law to retain bulk communications metadata (time, date, location, duration, etc.). The time frame for storage of metadata is defined by law and access to metadata is done with a court order and in accordance with the standards of Article 8 of the ECHR.

Operators in the Republic of Serbia are obligated to retain bulk communication metadata by Article 128 of the Law on Electronic Communications. Access to the retained data is not allowed without the consent of the user, except for a limited time and on the basis of a court decision, if it is necessary for the purpose of conducting criminal proceedings or protecting the security of the Republic of Serbia, in the manner prescribed by law. This retained metadata is stored for a period of 12 months, and the data can only be accessed on the basis of a court decision.

4.2.3 Video surveillance of public spaces by state authorities is regulated. There are specific legal provisions regulating data processing by video surveillance.

Although the new Law on Personal Data Protection came into force and started its application in August 2019, there are no provisions that regulate video surveillance. At this moment in Serbia there are no laws that regulate video surveillance. Furthermore, on data processed by video surveillance, all provisions of the new law on personal data protection are applied.

4.2.4. There is oversight provided by law on how are surveillance and interception of communications done in practice.

According to SHARE Foundation research on data retention which followed access to data retention by state organs from 2014-2018, different state authorities seem to have software for direct access to data retained by mobile network operators, but formally this access can only be granted with a court decision.²⁵ Furthermore, operators that retain data and state authorities that access it, need to submit an annual report on all requests for access to retained data to the Commissioner for Information of Public Importance and Personal Data Protection. Also, the Committee for Oversight of Security Agencies of the Parliament of the Republic of Serbia oversees the constitutionality and legality of the work of security services, which applies to access to retained data and interception of communications.

²⁵ SHARE Foundation, Retaining data on communications: to what extent are we under surveillance?, 26 December 2018.; and SHARE Foundation, Access without transparency-practice of data retention in 2018, 29 October 2019.

KOSOVO

1. AN ENABLING ENVIRONMENT FOR INTERNET FREEDOM

1.1. The protection of human rights and fundamental freedoms on the internet is guaranteed in law, in full compliance with relevant articles of the European Convention on Human Rights (ECHR).

The Constitution of Kosovo, adopted in 2008, in Article 22 of Chapter II (Fundamental Rights and Freedoms) provides for direct applicability of international agreements and instruments. It should be noted that Kosovo is not a party to the ECHR.

In the case of conflict, the following international agreements and conventions have priority over provisions of laws and other acts of public institutions:

- (1) Universal Declaration of Human Rights;
- (2) European Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocols;
- (3) International Covenant on Civil and Political Rights and its Protocols;
- (4) Council of Europe Framework Convention for the Protection of National Minorities;
- (5) Convention on the Elimination of All Forms of Racial Discrimination;
- (6) Convention on the Elimination of All Forms of Discrimination Against Women;
- (7) Convention on the Rights of the Child;
- (8) Convention against Torture and Other Cruel, Inhumane or Degrading Treatment or Punishment.²⁶

1.2. Laws and policies relating to the internet are assessed, at their drafting stage, with regard to the impact that their implementation may have on the exercise of human rights and fundamental freedoms in an inclusive and transparent process which enables the participation of all stakeholders, including the private sector, civil society, academia and the technical community.

There is no available information on public debates regarding internet-related laws.

1.3. Any state body which has regulatory or other competence over internet matters carries out its activities free from political or commercial interference, in a transparent manner and protects and promotes internet freedom.

In the Law on Electronic Communication, it is prescribed that the relevant authorities in the field of electronic communications are the Regulatory Authority of Electronic and Postal Communications and the Independent Media Commission.²⁷ The Regulatory Authority of Electronic and Postal Communications (RAEPC) is the national regulator in the field of electronic communications and postal services which perform tasks defined by this Law and other applicable legislation, and applies the policy and national strategies of the electronic communications sector, defined by the authority. In accordance with the Law on Electronic Communications Article 8, RAEPC is a public, independent, non-budgetary, legal entity with public authority, which exercises its activities in compliance with legislation in force. Authority in its work and decision-making within its competencies is independent. The Independent Media Commission (IMC) is the body responsible for the regulation, management and oversight of the broadcasting frequency spectrum in the Republic of Kosovo. Under Article 141 of the Constitution of Kosovo, IMC is founded as an independent body.

1.4 The state protects individuals from cybercrime through effective criminal justice or other measures. Notably they are prescribed by a law, which is accessible, precise, clear and foreseeable; pursue a legitimate aim; are necessary and proportionate in a democratic society and allow for effective remedies.

In Kosovo, there is a Law on Prevention and Fight of Cyber Crime, adopted in 2010, which aims to “prevent and combat cyber-crime with concrete measures, prevent, discover and sanction violations through computer systems, by providing observance of human rights and safeguard of personal information”. It is noted however that in the case of discrepancies of provisions of that law with the provisions of the Code of Criminal Procedure, the provisions of the Code

²⁶ Constitution of the Republic of Kosovo, June 2008.

²⁷ Law on Electronic Communication, (Official Gazette of the Republic of Kosovo, No. 30/09).

of Criminal Procedure shall be applicable (Article 27).²⁸ There are certain criminal acts in the Criminal Code of Kosovo related to cyber-crime. The Criminal Code includes offences such as Article 199 - Infringing privacy in correspondence and computer databases, Article 232 - Abuse of children in pornography, Article 301 - Issuing uncovered or false cheques and misuse of bank or credit cards, Article 327 - Intrusion into computer systems. The Criminal Code also defines “Child pornography” in Article 225, paragraph 8, where “computer generated images or pictures, whether made or produced by electronic, mechanical or other means” is mentioned.²⁹ However, Kosovo is not a signatory of the Budapest Convention on Cybercrime.³⁰

1.5. The state provides media and digital literacy programmes for internet users.

So far, there have not been media and digital literacy programmes for internet users provided by the state. However, certain international organizations and CSOs occasionally organize trainings on this topic. For example, OSCE Mission in Kosovo and UNICEF Innovations Lab organized events for teenagers within the PONDER Programme in the form of workshops. In total, this programme trained 200 students and reached over 2000 and aimed at improving critical thinking with regard to information and messages received from online media and the internet.³¹

2. THE RIGHT TO FREEDOM OF EXPRESSION

2.1. Freedom to access the internet

2.1.1. The internet is available, accessible and affordable to all groups of the population without any discrimination.

There is no discrimination regarding internet access to any group of the population. According to Article 3, paragraph 1 of the Law on Electronic Communications (Principles for Regulation of Electronic Communications Activities) prescribes that the regulation of electronic communications activities shall be based on the principles of management and use of limited resources, technological neutrality, functional equivalence, proportionality, minimal necessary regulation, legal certainty in a dynamic market, economic development, ensuring effective competition, consumer rights protection, objectivity of regulatory criteria, conditions and procedures, transparency and non-discrimination.³²

2.1.2. The public has access to the internet in facilities supported by public administration (internet access points), educational institutions or private owners (universal community service).

There is no available information on access to the internet in facilities supported by public administration. However, the provision of universal service is described in detail in the Law on Electronic Communications.³³

2.1.3. The state takes reasonable measures to ensure access to the internet to those with low income, in rural or geographically remote areas and those with special needs such as persons with disabilities.

Under the Kosovo Digital Economy (KODE) project, approved in July 2018 by the World Bank Board of Directors, more than 200 villages in Kosovo are expected to obtain high-speed broadband internet connection by 2023. Schools and hospitals will be able to have a free internet connection for five years.³⁴ According to the Law on Electronic Communications, universal service is a minimum set of public electronic communication services of specified quality which is available at an affordable price to all users in the territory of Kosovo, regardless of their geographic location. In Article 28, it is prescribed that the provision of Universal Service shall be ensured on the territory of Kosovo.³⁵

2.1.4. There are no general, nationwide restrictions on access to the internet.

There is no state mandated blocking or filtering of internet content on the national level. Internet shutdowns also do not occur in Kosovo.

2.2. Freedom of opinion and the right to receive and impart information

2.2.1. Any measure taken by state authorities or private-sector actors to block or otherwise restrict access to an entire internet platform or information and communication technologies, tools, or any request by state authorities to carry out such actions complies with the conditions of Article 10 of the ECHR.

There is no information about such measures.

²⁸ Code of Criminal Procedure, (Official Gazette of the Republic of Kosovo, No.74/2010).

²⁹ Criminal Code of Kosovo Cybercrime, (Official Gazette of the Republic of Kosovo, No.2/2019).

³⁰ Law on Prevention and Fight of the Cybercrime, (Official Gazette of the Republic of Kosovo, No.03/L-166).

³¹ OSCE, Spreading Critical Media Literacy among Kosovo youth, 5 April 2018.

Innovations Lab Kosovo, Techstitution: A Platform of Social Innovators in Kosovo, 17 August 2017.

³² Law on Electronic Communication, (Official Gazette of the Republic of Kosovo, No. 30/09). And: BelnKosovo, Communications in Kosovo.

³³ Law on Electronic Communication, (Official Gazette of the Republic of Kosovo, No. 30/09).

³⁴ The World Bank, Villages in Kosovo Start Enjoying High-Speed Internet With World Bank Support, 26 November 2018.

³⁵ Law on Electronic Communication, (Official Gazette of the Republic of Kosovo, No. 30/09).

2.2.2. Internet service providers as a general rule treat internet traffic equally and without discrimination on the basis of sender, receiver, content, application, service or device.

Pursuant to the Law on Electronic Communications, the regulation of electronic communications activities in Kosovo shall be based on the principle of technological neutrality (Article 3, paragraph 1). In the second paragraph of Article 3, it is prescribed that “the principle of technological neutrality means that legal norms must be applied taking into account the objectives to be achieved and ensuring, to a reasonable extent, that their application does not encourage or discriminate the use of specific technologies as well as ensuring that the legal norms are applied, as far as possible, disregarding the technologies employed in the provision of electronic communications networks or services related to a specific legal relationship”.³⁶

2.2.3. Internet users or other interested parties have access to a court in compliance with Article 6 of the Convention with regard to any action taken to restrict their access to the internet or their ability to receive and impart content or information.

The Constitution of Kosovo guarantees the right to a fair and impartial trial in accordance with Article 31, i.e. equal protection of rights in the proceedings before courts, other state authorities and holders of public powers. Although there are no specific information in regards to the internet, this general rule can be applied.³⁷

2.3. Freedom of the media

2.3.1. The editorial independence of media operating on the internet is guaranteed in law, policy and practice.

The right to freedom of expression, media freedom and the right to access to public documents are guaranteed by the Constitution of Kosovo. According to Article 42 (Freedom of Media) freedom and pluralism of the media are guaranteed. Also, censorship is forbidden. It is also prescribed that everyone has the right to correct untrue, incomplete and inaccurate published information, if it violates her/his rights and interests in accordance with the law.³⁸ Freedom of expression is also guaranteed through the Civil Law against Defamation and Insult, which provides for a balance to be struck between freedom of expression and establishing a system that is effective in providing appropriate compensation to those who are harmed by defamation or insult.³⁹

According to Freedom House, there is direct and indirect political interference on the media. For example, the Association of Journalists of Kosovo (AGK) alleged that government officials, business interests, and media owners have threatened journalists and their employers, as well as obstructed reporters’ work in other ways. There are also reports that journalists criticizing public officials are often called traitors or Serbian sympathizers. There have also been cases that media outlet editors have banned their reporters from publishing stories that are critical of the government or of public officials due to the outlets’ political leaning. It should also be noted that media which are not aligned with the government or ruling parties have been intimidated through tax investigations and denied access to public information.⁴⁰

2.3.2. Media are not required to obtain permission or a licence from the government or state authorities, beyond business registration, in order to be allowed to operate on the internet or blog.

In Kosovo, online media outlets and blogs are not subjected to licence requirements whatsoever by the state prior to publication.

2.3.3. Journalists and other media actors using the internet are not subject to threats or harassment by the state. They do not practise self-censorship because of fear of punishment, harassment or attack.

According to Freedom House, there are signs of constant political interference, direct and indirect. Certain media practice self-censorship because they fear punishment, being harassed or attacked, while others continue to inform the public objectively despite the threats.⁴¹

2.3.4. The confidentiality of journalists’ and other media actors’ sources is protected in law and respected in practice.

The Law on the Protection of Journalists’ Sources guarantees that journalists and media professionals cannot be compelled to reveal the sources of their information, unless there is a request of a competent court and only if the revelation of the identity of the source of information is necessary to prevent a serious threat to physical integrity which could lead to the death of one or more persons. Such requests must fulfill the following criteria: the information sought

³⁶ Ibid.

³⁷ Constitution of the Republic of Kosovo, June 2008.

³⁸ Ibid.

³⁹ Civil Law against Defamation and Insult, (Official Gazette of the Republic of Kosovo, No. 24/2008).

⁴⁰ Freedom House Report for Kosovo 2015.

⁴¹ Freedom House Report for Kosovo 2015.

is of great importance in preventing crimes; the information sought cannot be secured in any other way.⁴² Also, the Civil Law against Defamation and Insult (Article 18) prescribes defendants in a defamatory or insulting action cannot be required to reveal a confidential source of information. The court may require that the information related to the proceeding be revealed, but without identifying the source.⁴³ However, according to the report “Freedom of Expression, Media and Information in Kosovo: An Assessment Based on Council of Europe Indicators for Media in a Democracy”, the journalists’ perception of the Law on the Protection of Journalists’ Sources and the confidentiality of journalists’ sources being respected is that only 16% of surveyed journalists believe this to be the case and 46% have the perception that the current framework respects source confidentiality to a certain level. On the other hand, 13% of surveyed journalists feel that it does not entirely and 25% perceive it as not at all.⁴⁴

2.3.5. Media websites and websites of new media actors are not affected by cyber-attacks or other action disrupting their functioning.

Media websites and websites of new media actors are affected by cyber-attacks, such as DDoS, aimed at disabling their functioning. For example, there have been cyber-attacks on kossev.info website and Media Centar Čaglavica in 2017.⁴⁵

2.3.6. There are prompt and effective investigations of threats and crimes against journalists and new media actors. There is no climate of impunity.

According to the report “Freedom of Expression, Media and Information in Kosovo: An Assessment Based on Council of Europe Indicators for Media in a Democracy”, more than 60% of journalists surveyed stated that they feel threatened with violence to a certain level, while 22% of journalists said they feel “completely” threatened. During focus groups discussions, journalists noted that threats vary from physical to verbal ones. The journalists were also surveyed on whether the police offer protection to journalists when most required. Only 14% said that they believed that the police offered protection and 56% said only to a certain level. However, 19% were not entirely convinced that sufficient protection would be afforded and 11% had the view that they do not offer sufficient protection at all.

In relation to the justice system in Kosovo, only 7% of journalists surveyed reported that they believed the justice system would process their case adequately, while 46% stated that this would be done but only to a certain extent. However, 27% of journalists answered that the response of the justice system would not be entirely adequate and 20% of them believed that they would not be treated adequately. Also, while the Association of Journalist of Kosovo issues yearly reports on the number of threats to journalists, their nature remains largely undocumented.⁴⁶

3. THE RIGHT TO FREEDOM OF PEACEFUL ASSEMBLY AND ASSOCIATION

3.1. Individuals are free to use internet platforms, such as social media and other ICTs in order to associate with each other and to establish associations, to determine the objectives of such associations, to form trade unions, and to carry out activities within the limits provided for by laws that comply with international standards.

The Constitution of Kosovo in Article 43 guarantees freedom of peaceful gathering, and that every person has the right to organize gatherings, protests and demonstrations and the right to participate in them. It is also said that these rights may be limited by law, if it is necessary to safeguard public order, public health, national security or the protection of the rights of others.⁴⁷

3.2. Associations are free to use the internet in order to exercise their right to freedom of expression and to participate in matters of political and public debate.

In line with the Article 44 of the Constitution of Kosovo referring to public assemblies, there are no restrictions imposed on associations regarding their right to freedom of expression and participation in political and public debates in the online sphere.

3.3. Individuals are free to use internet platforms, such as social media and other ICTs in order to organise themselves for purposes of peaceful assembly.

According to regulations regarding public assemblies, there are no restrictions to freedom of use of the Internet, for the purposes of peaceful assembly.

⁴² Law on the Protection of Journalists’ Sources, (Official Gazette of the Republic of Kosovo, No.20/2013).

⁴³ Civil Law against Defamation and Insult, (Official Gazette of the Republic of Kosovo, No. 24/2008).

⁴⁴ Civil Rights Defenders, Freedom of Expression, Media and Information in Kosovo: An Assessment Based on Council of Europe Indicators for Media in a Democracy.

⁴⁵ Kossev, Hacked websites of Media Center and program ‘Free Serbian’, 22 January 2019. And: Kossev a victim of a strong hacking attack, 29 September 2017.

⁴⁶ Civil Rights Defenders, Freedom of Expression, Media and Information in Kosovo: An Assessment Based on Council of Europe Indicators for Media in a Democracy.

⁴⁷ Constitution of the Republic of Kosovo, June 2008.

4. THE RIGHT TO PRIVATE AND FAMILY LIFE

4.1. Personal data protection

4.1.1. The right to private and family life is guaranteed in compliance with Article 8 of the Convention. Any restriction to this right pursues one of the legitimate aims exhaustively enumerated in Article 8 of the Convention, is necessary in a democratic society and proportionate to the legitimate aim pursued. The law guarantees that all personal data is protected in compliance with Article 8 of the Convention and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) in States which have ratified it.

The Constitution of Kosovo recognizes the right to privacy in Article 36. As it is prescribed in the Constitution, everyone enjoys the right to have her or his private and family life respected, the inviolability of residence, and the confidentiality of correspondence, telecommunications and other communication. Also, searches of any private dwelling or establishment that are deemed necessary for the investigation of a crime may be conducted only to the extent necessary and only after approval by a court after explaining the reasons why such is necessary. The right of protection of personal data is also guaranteed. Collection, preservation, access, correction and use of personal data are all regulated by law.⁴⁸

Personal data processing in Kosovo is regulated by the Law on Personal Data Protection. Article 3 (Principles of Data Processing) prescribes that personal data shall be processed fairly and lawfully without violating the dignity of data subjects, that it must be adequate, relevant and not excessive in relation to the purposes for which they are collected and /or further processed, that personal data are collected only for specified, explicit and legitimate purposes, and may not be further processed in a way incompatible with these purposes, unless otherwise provided by law, that they must be accurate and kept up to date. Prior to collecting personal data, the data controller verifies the accuracy of personal data by examining an identity document or any other suitable public document of the data subject. Also, personal data may only be stored for as long as necessary to achieve the purpose for which they were collected or further processed. On completion of the purpose of processing, personal data shall be erased, deleted, destroyed, blocked or anonymised, unless otherwise provided by the Law on Archive Material and Archives or any other relevant law.⁴⁹

4.1.2. Personal data are processed lawfully (with the unambiguous consent of the data subject or on the basis of law) for legitimate purposes and not in excess of such purposes, accurately and securely.

According to the Article 5 of the Law on Personal Data Protection (Lawful processing of personal data of law on personal data protection), personal data may only be processed in some cases, when the data subject has given his or her consent; the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract; the processing is necessary for compliance with a legal obligation to which the controller is subjected; the processing is necessary in order to protect the vital interests of the data subject; the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or the processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.⁵⁰ However, there is no data about practice from the National Agency for Personal Data Protection.

4.1.3. Individuals are not subjected to a decision significantly affecting them based solely on automated processing of data without having their views taken into account.

In Article 8 of the Law on Personal Data Protection, it is prescribed that automated decision-making which might produce legal effects or significantly affect the data subject and which is solely based on automated data processing intended to evaluate certain personal aspects, especially the data subject’s performance at work, credit-worthiness, reliability, conduct or compliance with certain conditions, shall only be permitted if two conditions are met. First, if the decision is taken during the conclusion or performance of a contract, provided that the request to conclude or implement a contract submitted by the data subject has been satisfied or if there are appropriate measures to protect his or her legitimate interests, such as arrangements enabling the data subject to object to such decisions or to express his or her position, and second, if the decision is provided by law which also provides measures to protect the legitimate interests of the data subject, particularly the possibility of legal remedy against such decisions.⁵¹

4.1.4. There are effective processes enabling every individual to obtain, on request, information on the processing of his or her personal data and the reason underlying processing; to object to processing; to obtain, on request, rectification or erasure of the personal data; and to consent to, object to or withdraw consent to personal data processing or profiling. An effective remedy exists for individuals when these rights are not respected. Legal frameworks for personal data protection provide adequate safeguards for access to information and freedom of expression.

⁴⁸ Constitution of the Republic of Kosovo, June 2008.

⁴⁹ Law on the Protection of Personal Data, (Official Gazette of the Republic of Kosovo, Law No.03/L – 172).

⁵⁰ Law on the Protection of Personal Data, (Official Gazette of the Republic of Kosovo, Law No.03/L – 172).

⁵¹ Ibid.

The rights of the data subjects are defined in Chapter III of the Law on Personal Data Protection, Articles 21 to 27: Consultation of the Register, Right of access, Procedure for access, Right to supplement, correct, block, destroy, erase, delete and object, Procedure of supplementing, correction, blocking, erasure, destruction, deletion and objection, Judicial protection of the rights of the Data Subject, Temporary Prohibition of Processing the Personal Data.⁵²

4.1.5. The law defines the duties of public and private entities with regard to processing of personal data.

Duties in regards to personal data processing are defined in Chapter II, Subchapter B (Obligations of data controllers and data processors) of the Law on Personal Data Protection, i.e. in Articles 14, 15 and 16 (Security of data processing, Contractual processing, Obligation to secure personal data).⁵³

4.1.6. A supervisory authority, which acts with complete independence and impartiality, ensures compliance with data protection legal frameworks.

In Kosovo, the supervisory authority overseeing the implementation of the data protection legal framework is called the National Agency for the Protection of Personal Data.⁵⁴ As it is stated in the Law on Personal Data Protection, Article 29, it is an independent agency in charge of supervising the implementation of data protection rules. Its members act independently in accordance with this law and must not take any instructions from third parties. It shall be accountable to the Kosovo Assembly.

4.1.7. The state does not prohibit, in law or in practice, anonymity, pseudonymity, confidentiality of private communications or the usage of encryption technologies. Interference with anonymity and confidentiality of communications is subject to the requirements of legality, legitimacy and proportionality of Article 8 of the Convention.

According to the Constitution, (Article 36, Right to Privacy) the secrecy of correspondence, telephony and other communication is guaranteed. It is also said that this right may only be limited temporarily by court decision if it is necessary for criminal proceedings or defense of the country as defined by law. There are no known restrictions to anonymity or pseudonymity.⁵⁵

4.2. Surveillance

4.2.1. The access to the content of communications is regulated and it is done in accordance with Article 8 of the ECHR.

Interception of communications is prescribed by the Law on Interception of Communications. Article 3, paragraph 1, subparagraph 1.3. defines the interception of electronic communications as the interception voice communications, textual communications or other communications through networks of fixed or mobile telephony, including any other similar tool or technological system that transmits data mainly intended to be private.⁵⁶

4.2.2. Operators of electronic communications are obliged by law to retain bulk communications metadata (time, date, location, duration, etc.). The time frame for storage of metadata is defined by law and access to metadata is done with a court order and in accordance with the standards of Article 8 of the ECHR.

As it is prescribed in the Law on Electronic Communications, operators are obliged to retain communications metadata. Article 68 (Personal data preservation and administration for the criminal proceedings purposes) of that law states that regardless of other definitions in this Law, the entrepreneurs of public electronic communications services and networks shall be obliged to store and administrate, for a period not longer than one (1) year, the data files of their subscribers. It is also said that such storage shall be paid for by state funds in accordance with the procedure established by the Government.⁵⁷

4.2.3. Video surveillance of public spaces by state authorities is regulated. There are specific legal provisions regulating data processing by video surveillance.

In the Law on Personal Data Protection, Articles 61-64 (Chapter VI, Subchapter J - Video surveillance) prescribe the rules for data processing in the context of video surveillance. For example, public or private sector persons intending to install video surveillance systems must set up a notice to that effect. Such a notice must be plainly visible and made public in a way that data subjects can easily acquaint themselves with the measures at the latest where the video surveillance begins. Also, through the correct notification form, the data subject shall be deemed to have been informed of the processing of personal data. It is also prescribed that the video surveillance system and the recordings of the monitoring must be adequately protected against unauthorized access and use. Subchapter J covers general provisions regarding video surveillance, monitoring of official and business premises, monitoring of apartment buildings as well as video surveillance in the employment sector.⁵⁸

⁵² Law on the Protection of Personal Data, (Official Gazette of the Republic of Kosovo, Law No.03/L - 172).

⁵³ Ibid.

⁵⁴ Ibid.

⁵⁵ Constitution of the Republic of Kosovo, June 2008.

⁵⁶ Law on Interception of Communications, (Official Gazette of the Republic of Kosovo, No. 18/2015).

⁵⁷ Law on Electronic Communication, (Official Gazette of the Republic of Kosovo, No. 30/09).

⁵⁸ Law on the Protection of Personal Data, (Official Gazette of the Republic of Kosovo, Law No.03/L - 172).

4.2.4. There is oversight provided by law on how are surveillance and interception of communications done in practice.

In 2015, Kosovo has adopted the Law on Interception of Communications. The basic principles laid out in the Law (Article 4) are the respect for human rights and fundamental freedoms recognized and guaranteed by the Constitution and the European Convention on Human Rights and Freedoms, including the interpretation by the European Court of Human Rights through its judicial practice and the prohibition of interception without a respective decision by the court. The Law also recognizes (Article 6) that the procedure for lawful interceptions is implemented in three separate phases: (1) submission of requests for interception from institutions authorized by law; (2) review, approval and submission of requests for interception; and (3) court order for interception. Kosovo has the Commissioner for Oversight of Interception of Communication, established by the Law on Interception of Communications. It is a mechanism functioning within the institutional structure of the Kosovo Judicial Council, conducts yearly control of the lawfulness of interception of communications in accordance with the law, and reports to the Kosovo Judicial Council and the State Prosecutor, as well as respective parliamentary Committees of the Assembly of Kosovo on an annual basis on identified possible violations.⁵⁹ The main problem in practice turned out to be the lack of cooperation among different institutions in Kosovo, because each of them independently signed the agreements with the telecommunications operators. This has allowed for some complaints to be addressed towards the EULEX for intercepting telecommunications without any coordination with local security authorities.⁶⁰

BOSNIA AND HERZEGOVINA

1. AN ENABLING ENVIRONMENT FOR INTERNET FREEDOM

1.1. The protection of human rights and fundamental freedoms on the internet is guaranteed in law, in full compliance with relevant articles of the European Convention on Human Rights (ECHR).

Bosnia and Herzegovina (BiH) has a complex constitutional order established in the Dayton Peace Agreement. There are 14 constitutions - one at a state level, two at an entity level, one in Brčko District of BiH and one in each of the ten cantons of the Federation of BiH). The legislative framework regarding human rights, and thus the right to freedom of expression, involves numerous norms and practices, and is dealt with by a number of institutions. The Constitution of BiH⁶¹, states that “the rights and freedoms set forth in the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocols shall apply directly in BiH” and that they “have priority over all other law.” The same statement is contained in the constitutions of both entities: Federation of BiH and the Republika Srpska, as well as in the Constitution of Brcko District of BiH. The Constitution of the Federation of BiH,⁶² in its Annex “Instruments for the protection of human rights which have legal power of constitutional provisions,” provides twenty one international conventions and declarations, among other: the Universal Declaration of Human Rights (UN), the European Convention for the Protection of Human Rights and Fundamental Freedoms, as well as the International Covenant on Civil and Political Rights. In Article II, paragraph 3, point (g) of the Constitution of BiH “freedom of thought, conscience and religion” are ensured, while point (h), guarantees “freedom of expression.” The Constitution of Federation of BiH in chapter II, Article 1, ensures fundamental freedoms such as “freedom of speech and press and freedom of opinion, conscience and belief...”. Furthermore, the Constitution of Republika Srpska⁶³ in Part II (Human Rights and Freedoms), Article 25 states that “freedom of thought and orientation, conscience and conviction, as well as of public expression of opinion shall be guaranteed.” Article 26 emphasizes that “freedom of press and other media of communication shall be guaranteed,” and that “free establishment of newspaper and publishing houses, publishing of newspapers and public information by other media in accordance with law shall be guaranteed.” In addition, Article 26 also states that “censorship of press and other public information media shall be forbidden,” and that “public information media shall be obliged to inform the public on time, truthfully and impartially.”

⁵⁹ Law on Interception of Communications, (Official Gazette of the Republic of Kosovo, No. 18/2015).

⁶⁰ S. Kursani, Kosovar Centre for Security Studies, Lawful Interception of Telecommunications in Kosovo: Security Implications.

⁶¹ Constitution of Bosnia and Herzegovina, (1995), entered into force 14 December 1995.

⁶² Constitution of the Federation of Bosnia and Herzegovina (Sarajevo, 30 March 1994), Official Gazette of FBiH No.1/94, entered into force 30 March 1994.

⁶³ Constitution of Republika Srpska (1992), Official Gazette of RS No. 28/94, entered into force in 1994.

1.2. Laws and policies relating to the internet are assessed, at their drafting stage, with regard to the impact that their implementation may have on the exercise of human rights and fundamental freedoms in an inclusive and transparent process which enables the participation of all stakeholders, including the private sector, civil society, academia and the technical community.

The legislative framework in BiH was set up by the international community after the war ended in 1995. The implementation of laws is still rather problematic mainly because of political pressures and strong divisions along national lines. Public debates regarding drafting news laws are very rare as well as the involvement of civil society. On one occasion though, the involvement of experts was successful. In 2013, the activities of the civil society sector were set around the proposed amendments to BiH Freedom of Access to Information Act which were posted on the Ministry of Justice website for public discussion and comments, before being sent to parliament. The Act was assessed as restrictive, because it provided more strength to the “rule of exception” making it very easy for public institutions to evoke this Law and retain information. Following expert analysis and wide distribution of the amendments, USAID, Center for Investigative Reporting (Centar za istraživačko novinarstvo - CIN), Open Society Foundation, Human Rights in BiH ombudsman office, Mediacentar, OSCE, and Public International Law & Policy Group (PILPG) participated in online and offline advocacy activities against the adoption of the amendments. The combined efforts were successful as the Ministry tabled the proposed amendments in consideration of public comments. There were numerous events advocating against the proposed changes to this Act, such as “FOIA Draft Law Public Debate” with representatives of Center for Cultural Dialogue, Justice Network, Ministry of Justice and the Agency for the Protection of Personal Data, as well as representatives from other non-governmental organizations. After numerous discussions, it was concluded that the proposed terms of the Draft Law on Amendments to the Law on Free Access to Information were not acceptable.

1.3. Any state body which has regulatory or other competence over internet matters carries out its activities free from political or commercial interference, in a transparent manner and protects and promotes internet freedom.

The Communications Regulatory Agency in BiH (CRA) is in charge of the whole broadcasting sector. The primary reasons for establishing the CRA were “avoiding double or conflicting regulatory authorities at all level of government in BiH; the key role of telecommunications in the economic development of any country; the assumption that opening the market of telecommunications towards competition brings benefits to both consumers and the business sector; the fact that the trend in the communications industry towards the convergence of technology and the way of transmission requires clear and comprehensive regulatory approach; the opinion that the unique regulator will enable a quick and efficient reaction to economic and business conditions.”⁶⁴ Some of the CRA tasks include drafting and ensuring implementation of rules on broadcasting; issuing licenses to broadcasters, etc. However, the CRA also faced political pressures on several occasions because, for example, the Republika Srpska authorities opposed the forming of state-level institutions in order to have a stronger entity authority. Other authorities oppose the activities of the CRA, too, as well as certain media outlets with strong affiliations with political parties and so “legal documents were changed frequently due to short-term political and other interests, often resulting in conflicting legal arrangements, legal uncertainty, and regulatory chaos.”⁶⁵ The appointment of the CRA Director General and the members of the Council came across numerous obstacles for more than a decade, because the CRA was without a Director General between 2007 and 2018. The independence of the CRA is questionable on several levels, because political and economic pressures “aim to reduce the credibility of the agency” and political parties constantly aim at controlling the agency and influencing its decision-making processes, thus “the guarantees of freedom from political control and manipulation have not been working in practice.”⁶⁶

1.4 The state protects individuals from cybercrime through effective criminal justice or other measures. Notably they are prescribed by a law, which is accessible, precise, clear and foreseeable; pursue a legitimate aim; are necessary and proportionate in a democratic society and allow for effective remedies.

Criminal Codes in the Federation of BiH and Republika Srpska approach cyber-crime but the provisions are rather scarce and the adoption of new laws and ensuring their compliance with international standards are stalling. The legislative framework regarding cyber-security is not in line with EU requirements and if the country is to become an EU member, it will have to introduce new laws and bodies regarding cyber-security. The Codes mention “computer crimes” and Chapter XXXII of the Criminal Code of BiH which relates to “Criminal offences against electronic data processing system” contains provisions regarding cyber-security. BiH ratified the Budapest Convention on Cybercrime, but the legislative framework has still not been made entirely compliant with this Convention. The provisions refer to: Damaging Computer Data and Programs, Computer Forgery, Computer Fraud, Disturbing the Work of the Electronic Data Processing System and Network, Unauthorised Access to the Electronic Data Processing Protected System and Network, and Computer Sabotage. For example, according to Article 396 of the Code, “Whoever, by unauthorised access to the electronic data processing system or network, causes the stoppage or disturbance of the work of such system or network, shall be punished by a fine or imprisonment for a term not exceeding three years.”

⁶⁴ H. Mandić, “Regulation of Broadcasting in BiH”, in Halilović, Mehmed and Amer Džihana, Media law in Bosnia and Herzegovina, Internews in Bosnia and Herzegovina, Sarajevo, 2012, p.253

⁶⁵ T. Jusić and N. Ahmetašević, Media Reforms through Intervention: International Media Assistance in Bosnia and Herzegovina, Analitika, 2013, p.34

⁶⁶ S. Hodžić, Bosnia and Herzegovina in Media Integrity Matters: Reclaiming public service values in media and journalism, Peace Institute, Institute for Contemporary Social and Political Studies, 2014, p. 8

When it comes to relevant bodies, in the Police Administration of the Federation of BiH there is a Department for fighting against computer crimes, whereas in Republika Srpska there is the same Department within the Ministry of Interior. These two agencies deal with criminal acts and investigations regarding computer crime and computer-enabled criminal acts. In Brčko District of BiH, cybercrime is investigated by specialised investigators in the Criminal Police. Digital forensics is carried out by the Ministry of Interior in Republika Srpska, the State Investigation and Protection Agency, Border Police of BiH, the Agency for forensics and expert examinations, Brčko District Police and cantons’ ministries of interior. In 2016, the Council of Ministers of BiH made it obligatory for the Ministry of Security of BiH to form the Computer Emergency Report Team for the institutions of BiH. The tasks of BHCERT include dealing with vulnerabilities and management of incidents in the domain of electronic security to all state level institutions and their supporting service providers. Since 2015, the Department for Information Security within the Agency for Information Society of Republika Srpska, has had the function of a CERT at entity level.

1.5. The state provides media and digital literacy programmes for internet users.

The state does not provide media and digital literacy programmes. There are internal trainings and education offered to a small number of employees; at the Civil Service Agency, for example. Their employees have webinars on media and digital literacy available once a year, but there is no data available on how many civil servants actually take these types of trainings. There are no media and digital literacy programs at schools; only at universities within the study of journalism.

2. THE RIGHT TO FREEDOM OF EXPRESSION

2.1. Freedom to access the internet

2.1.1. The internet is available, accessible and affordable to all groups of the population without any discrimination.

There is no discrimination regarding internet access to any group of the population. Policy of the Electronic communications sector in BiH for the period 2017-2021 and the Action Plan for Policy Implementation (“Official Gazette of BiH” No. 46/17) as their subjects also cite, among other new technologies and creating conditions for their introduction.

2.1.2. The public has access to the internet in facilities supported by public administration (internet access points), educational institutions or private owners (universal community service).

The public has access to the internet in some educational institutions such as faculties, but public administration facilities do not provide such services.

2.1.3. The State takes reasonable measures to ensure access to the internet to those with low income, in rural or geographically remote areas and those with special needs such as persons with disabilities.

Over the past few years measures were taken to reach rural and remote areas, although this has proven to be a challenge due to the hilly landscape of BiH and regions that are difficult to be reached. According to the most recent data, half of rural households own a computer, usually with an internet connection. Additionally, two-thirds of rural households live in areas covered by a mobile phone network. More than 90% of young people in rural and urban areas use both computers and the internet, but this usage is still at least 3-4% higher in urban areas. The Government of BiH adopted the Decision on Policy of the development of the information society in BiH for the period 2017-2021.⁶⁷ In this Strategy, the internet was recognised as a ‘significant means for economic and social activities’. This decision acknowledges the importance of the government ensuring access and adjusting public sector websites content to people with disabilities. It also points out the significance of ensuring the internet access in schools, and adjusting the existing legislative to make sure that women with infants and small children can formally work from home. The decision strongly emphasizes the importance of e-Learning and its availability to all of its citizens. However, the implementation of this decision still remains questionable because there is no data on whether these actions have actually taken place.

2.1.4. There are no general, nationwide restrictions on access to the internet except when this is in compliance with Article 10 of the Convention.

There is no state mandated blocking or filtering of internet content on the national level. Internet shutdowns also do not occur in BiH.

2.2. Freedom of opinion and the right to receive and impart information

2.2.1. Any measure taken by state authorities or private-sector actors to block or otherwise restrict access to an entire internet platform or information and communication technologies, tools, or any request by state authorities to

⁶⁷ Decision on Policy of the development of the information society in BiH for the period 2017-2021, (Official Gazette of BiH, No. 42/17).

carry out such actions complies with the conditions of Article 10 of the ECHR.

According to the licenses for internet providers issued by the Communications Regulatory Agency (CRA), the providers must not control the content, but they are obligated to do so if the content is harmful, or to block the access to the content at the request of a public body. In addition, the state can take actions regarding the access of social networks content when it comes to threats to national security. “However, when it comes to radical content, the adopted strategic documents don’t even contain a definition of violent extremism or online extremism, so it’s hard to develop a systemic approach or build a counter-narrative.”⁶⁸ Online content regarding Islamic State in the context of BiH and the Balkans, has decreased over the past few years, but some of the detected content was still available, showing that the state did not take actions to restrict it based on the second paragraph of Article 10 of the European Convention on Human Rights. Furthermore, in 2015, Republika Srpska adopted the Law on Public Peace and Order. This Law was passed without taking into account the comments of academia, the expert community and civil society. The problematic aspect of the Law is that it lacks a definition of a “public space”, and its implementation showed that it includes internet and social media too. The law does not include concrete standards for the definition of social media, it does not explain what constitutes “offensive” or “indecent” material, nor does it deny that citizens can be prosecuted outside of the Republika Srpska entity.

2.2.2. Internet service providers as a general rule treat internet traffic equally and without discrimination on the basis of sender, receiver, content, application, service or device.

Yes, internet service providers treat internet traffic equally and without discrimination. BiH has still not adopted the Law on Electronic Communications, therefore net neutrality is not included in legislation yet. However, there are no data on any type of discrimination in terms of sender, receiver, content, etc.

2.2.3. Internet users or other interested parties have access to a court in compliance with Article 6 of the Convention with regard to any action taken to restrict their access to the internet or their ability to receive and impart content or information.

Users have the access to a court in compliance with Article 6 of the Convention with regard to any action taken to restrict their access to the internet or their ability to receive and impart content or information. However, there have been no such cases before courts in BiH so far. The courts are yet to establish their practice in this respect.

2.3. Freedom of the media

2.3.1. The editorial independence of media operating on the internet is guaranteed in law, policy and practice.

There is no specific law on editorial independence of media operating on the internet. However, the Law on Public Service Broadcasting System of BiH stipulates that the laws on services should comply with its provisions and its goal is to achieve the balance between the independence of each broadcaster and their joint activities within the PSB system. The Law ensures the independence of public broadcasting services and so it covers editorial independence and institutional autonomy, too. According to the Law, public services independently establish their programs, manage their assets, deal with financial and employment issues, and represent broadcasters in legal proceedings. Furthermore, the Law on Public Information of Republika Srpska prohibits censorship, the Law of the Sarajevo Canton envisages freedom of editorial policy in accordance with professional ethical standards, as do other cantonal laws. But in practice, the lack of editorial independence is still visible and so even the Radio Television of BiH (BHRT), faces pressures from political parties and political figures, and its editorial independence is often questionable. In 2011, the statute of BHRT was amended to give its steering committee full editorial and managerial control, including the authority to appoint editors and approve programming, but in practice, this option is rarely applied.

2.3.2. Media are not required to obtain permission or a licence from the government or State authorities, beyond business registration, in order to be allowed to operate on the internet or blog.

Media outlets are not required to obtain such permissions. Most recently, this has been identified as a problem on several debates regarding online media. Namely, as media ownership in the country is not regulated, experts often insist on making impressums mandatory for online media and clearly identifying their owners. Since this issue is connected with the lack of ownership regulation, it remains to be seen which steps will be taken and how online media will be approached in this respect.

2.3.3. Journalists and other media actors using the internet are not subject to threats or harassment by the State. They do not practise self-censorship because of fear of punishment, harassment or attack.

Journalists in BiH face both verbal and physical attacks, and court proceedings referring to these attacks are often

68 E. Dizdarevic, Bosnia Failing in Fight against Extremism Online, BIRN, 13 August 2019.

long and remain incomplete for years. More specifically, according to BH Journalists, the association of journalists from the country, from 2006 to 2015, only 15% of the 60 recorded crimes towards journalists were legally finalised, that is, the court proceedings were completed. On several occasions, it was public figures who made threats to exercised pressures on journalists and other media actors. According to the report by BH Journalists, in 2018 there were 21 cases of verbal and physical attacks on journalists.⁶⁹ Very few attacks are investigated and the European Commission in its report for BiH in 2016 stated that it is necessary to take legal measures in cases of political pressures and intimidation of journalists, and protection and law enforcement must be secured as an answer to the threats against journalists.⁷⁰

2.3.4. The confidentiality of journalists’ and other media actors’ sources is protected in law and respected in practice.

The confidentiality of journalistic sources is, among other, protected by defamation laws. The right of journalists to protect their sources is also included in the Press and Online Media Code of the Press Council in BiH. More specifically, “journalists and persons regularly or professionally engaged in journalistic activity of seeking, receiving or imparting information to the public, who obtained information from confidential source, have the right not to reveal their sources”. Additionally, the Criminal Procedure Code of BiH stipulates that a questioned witness “cannot be a person who by his/her statement would violate the duty of professional secrecy”, and this person is classified as “... a journalist to protect sources of information, unless if exempt from that duty by a special regulation or statement of the person who benefits from the secret being kept”.⁷¹ The Criminal Procedure Code of the Federation of BiH, the Criminal Procedure Code of the Republika Srpska and the Criminal Procedure Code of the Brčko District of BiH contain the same provision regarding the questioned witnesses. On the other hand, if a piece of information was obtained in an illegal manner or if this information is being used without any authorization, then this action is a criminal offense. Furthermore, the Law on the Protection of Classified Information establishes the illegality of acquiring secret data, and specifies persons with access to classified information of a certain degree. Therefore, “the criminal laws and the Law on Protection of Classified Information established the illegality of acquiring data as a condition for the crime”. In addition, the Press Code states that journalists have an obligation to protect the identity of those from whom they receive information in confidence, regardless of whether they explicitly request confidentiality, and so “journalists have an obligation to protect the identity of those who provide information in confidence, regardless of whether or not they explicitly request confidentiality”. The Code of Honor of of BH Journalists also states that journalists have the right not to disclose source of information. It is acknowledged “the sources must trust journalists enough and be comfortable enough knowing that laws protect them because there is always a great risk when discussing important and problematic matters in general”. However, media were pressured to reveal their sources on several occasions. In 2014, an online news portal, www.klix.ba faced an attack on journalists’ right to protect sources.⁷² The Cantonal Court in Sarajevo issued a court order and police raided the offices of the portal, the staff was asked to leave premises and then the police seized computers, documents, notes and other items from the offices, which was assessed as an intrusion into the right of journalists to provide protection to their sources.

2.3.5. Media websites and websites of new media actors are not affected by cyber-attacks or other action disrupting their functioning.

There are no available data on cyber-attacks on media websites or websites of new media actors, not are there records of any disruption of their functioning.

2.3.6. There are prompt and effective investigations of threats and crimes against journalists and new media actors. There is no climate of impunity.

The freedom of expression and the independence of journalists and new media actors were jeopardized on several instances, and investigations cannot be said to be prompt and effective. In 2019, journalists faced several threats that made the international actors react and condemn the attacks. For example, the Editor-in-chief of the news program of BHRT received death threats, a journalist of FTV and the owner of a news portal received threats too, while a journalist of daily newspaper Euroblic, but on a more positive note – the person using their phone to threaten the latter was arrested.⁷³ There are no specific records on attacks and threats made against journalists, and courts, prosecutors and the police do not pay special attention to the attacks on journalists and other media actors. Due to the fact that the country’s Criminal Code does not define a journalist as a state official, attacks on journalists are not considered as attacks on officials performing their obligations.

69 Ibid.

70 European Commission, “Bosnia and Herzegovina 2016 Report”, p. 21.

71 Criminal Procedure Code of Bosnia and Herzegovina, (Official Gazette, No. 03/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09).

72 RTVFBiH, Protests of Journalists in BiH, ordered to return property of Klix, 7 January 2015.

73 N1BiH, Desir and Breton condemn threats to journalists in Bosnia and Herzegovina, 15 February 2019.

3. THE RIGHT TO FREEDOM OF PEACEFUL ASSEMBLY AND ASSOCIATION

3.1. Individuals are free to use internet platforms, such as social media and other ICTs in order to associate with each other and to establish associations, to determine the objectives of such associations, to form trade unions, and to carry out activities within the limits provided for by laws that comply with international standards.

Individuals are free to use internet platforms to associate with each other and to establish associations, but the overall regulation of peaceful assemblies in BiH is rather questionable. The right to freedom of peaceful assembly in BiH is incorporated in the legislative framework of BiH, however, it is contained in 11 laws in total and therefore remains fragmented. The Federation of BiH created a Pre-Draft of the FBiH FoA Law but it was assessed as “an attempt to intimidate future and current assembly organisers, imposing disproportional responsibilities and severe fines for them. Further, the text in the law is unclear, certain terms are not elaborated and the length is deceiving. The final act of the law says that it will be adopted according to the urgent procedure, which is worrying.”⁷⁴

3.2. Associations are free to use the internet in order to exercise their right to freedom of expression and to participate in matters of political and public debate.

In line with regulations referring to public assemblies, there are no restrictions imposed on associations regarding their right to freedom of expression and participation in political and public debates in the online sphere..

3.3. Individuals are free to use internet platforms, such as social media and other ICTs in order to organise themselves for purposes of peaceful assembly.

According to regulations regarding public assemblies, there are no restrictions to freedom of use of the Internet, for the purposes of peaceful assembly. When it comes to using the internet to exercise the right to freedom of expression, associations most often turn to social media such as Facebook to organize assemblies and raise the awareness of certain matters. More specifically, before organising assemblies, it is frequent to create interest groups that would be followed by organising an event. During the assemblies, especially the ones where stronger reactions are expected, participants conduct livestreaming. After the assembly is finished, follow-up actions and impressions are discussed in already created groups and/or events.⁷⁵ But due to the problematic legislative framework and the attacks that organizers of certain events faced, participants very rarely use their individual social media profiles to initiate events or to send invitations referring to attendance at assemblies. Most recently, the internet was widely used for gathering participants for the first Pride march in Sarajevo, and spread awareness of the importance of the event.

4. THE RIGHT TO PRIVATE AND FAMILY LIFE

4.1. Personal data protection

4.1.1. The right to private and family life is guaranteed in compliance with Article 8 of the Convention. Any restriction to this right pursues one of the legitimate aims exhaustively enumerated in Article 8 of the Convention, is necessary in a democratic society and proportionate to the legitimate aim pursued. The law guarantees that all personal data is protected in compliance with Article 8 of the Convention and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) in States which have ratified it.

The Constitution of BiH recognizes the right to privacy as a basic human right. Article 3, paragraph 8 defines it as “the right to private and family life, home and correspondence.” The Constitution of Republika Srpska states that “human dignity, physical and spiritual integrity, personal privacy, personal and family life shall be inviolable.” The Constitution of the Federation of BiH states that the Federation will ensure the application of the highest level of internationally recognized rights and freedoms, including privacy. Since the right to privacy is defined by Article 8 of the European Convention as having priority over all other definitions in laws defining this field, the Constitution of BiH states that “rights and freedoms envisaged in the European Convention on Human Rights and Fundamental Freedoms and in its protocols they are directly applied in BiH” and have priority over all other laws. Finally, there is also the Law on Protection of Personal Data, the purpose of which is “to secure in the territory of BiH for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to the processing of personal data relating to him (data protection).” However, the problem regarding personal data protection and privacy in BiH is the inadequate institutional support, in practice.

4.1.2. Personal data are processed lawfully (with the unambiguous consent of the data subject or on the basis of law) for legitimate purposes and not in excess of such purposes, accurately and securely.

Each data subject has the right to submit an objection to the Personal Data Protection Agency if they believe that the controller or data processor violated their rights or that there is a risk of violation of their rights. Article 30 of the Law on Protection of Personal Data provides the right to submit this objection. In 2017, the Agency received 96 complaints of personal data subjects: 57 against controllers in the public sector and 39 complaints against controllers in the private sector such as banks, micro-credit organizations, various business entities and natural persons. As a result, 36 objections were accepted by the Agency, 6 were partially adopted while 25 objections were rejected. In total, there were 11 conclusions finalized, and therefore the proceedings regarding complaints were completed, but the reason for this was either the lack of jurisdiction or inadequacy of the submission. Only one objection was submitted to the relevant authority. Overall, the Personal Data Protection Agency does not have sufficient support from the authorities and therefore those who violate privacy do not suffer any consequences, and the overall data protection of the BiH citizens remains largely questionable.

4.1.3. Individuals are not subjected to a decision significantly affecting them based solely on automated processing of data without having their views taken into account.

According to Article 4 of the Law on Protection of Personal Data, it is specified that personal data undergoing automatic processing shall be: a) obtained and processed fairly and lawfully; b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c) adequate, relevant and not excessive in relation to the purposes for which they are stored; d) accurate and, where necessary, kept up-to-date; e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

4.1.4. There are effective processes enabling every individual to obtain, on request, information on the processing of his or her personal data and the reason underlying processing; to object to processing; to obtain, on request, rectification or erasure of the personal data; and to consent to, object to or withdraw consent to personal data processing or profiling. An effective remedy exists for individuals when these rights are not respected. Legal frameworks for personal data protection provide adequate safeguards for access to information and freedom of expression.

The Personal Data Protection Agency in BiH is an independent administrative organization established to ensure the personal data protection in the state. In this sense, Article 40 of the Law on Protection of Personal Data⁷⁶ defines the responsibilities of the Agency, as follows: to supervise the implementation of this Law and other laws on personal data processing; to act on data subject’s complaints; to submit to the Parliamentary Assembly of BiH annual reports on personal data protection, which should be available to the public; to follow the personal data protection requirements by giving proposals as to enacting or amending legislation governing the data processing, give opinions on the proposed laws and take care of fulfilment of the criteria relevant to data protection originating from international treaties that are binding for BiH. According to the Law on Protection of Personal Data and its Article 5 “Personal data shall not be processed unless: a) the data subject has unambiguously given his consent; or b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.” In addition, Article 13 stipulates that “the data subject shall have the right to: a) request information on the processing of his or her personal data; b) request the rectification of his or her personal data, or deletion thereof when demonstrated to be incorrect or processed unlawfully.” Furthermore, “the data controller shall not deny access to information to a data subject except where provided by law. The data controller shall state the reason for denial of the information requested.” The legislative framework in this respect is therefore largely in place, but the data on actual implementation of the law are still missing, or not entirely clear.

4.1.5. The law defines the duties of public and private entities with regard to processing of personal data.

According to the Law on Protection of Personal Data and Article 2, the Law shall apply to the processing of personal data by: a) public bodies at the level of BiH, b) public bodies of the entities and the district, c) private bodies of the entities and the district. This law defines the purposes of personal data processing, specifies when personal data shall not be processed, technical data processing, etc. Therefore, privacy protection is found in different laws such as the Law on Protection of Personal Data in BiH which defines the right to privacy regarding personal citizens’ data processed by different public and private bodies, or the Freedom of Access to Information Act, which regulates the access to personal information of citizens controlled by public bodies. The Communication Law of BiH prescribes the authority of the Communications Regulatory Agency over the protection of personal data and privacy. Although privacy is protected by the Laws on Protection against Defamation (two entity laws and one of the district), in court practice, violation of privacy is increasingly treated as a violation of basic human rights. But the citizens may ask for compensation before courts based on the Convention, which is above local legislation, or based on the Law on Obligatory Relations, which, in force in both entities, specifies that everyone is obligated to abstain from actions that cause damage to another person. This includes the damage caused by harming the integrity of one’s personality, personal and family life, and other rights of a person.

4.1.6. A supervisory authority, which acts with complete independence and impartiality, ensures compliance with data protection legal frameworks.

⁷⁴ E. Bavic, Monitoring Right to Free Assembly Bosnia and Herzegovina Country Report 2016-2017, ECNL and Civil Rights Defenders, December 2017.

⁷⁵ Ibid.

⁷⁶ Law on the Protection of Personal Data, (Official Gazette of BiH, No. 32/01).

The authority dealing with the issues of privacy in BiH is the Personal Data Protection Agency. The Agency is supported by the Parliamentary Assembly of BiH and the Council of Ministers of BiH, but certain activities and decisions had influenced the work of the Agency and made its work questionable. In the Agency Report for 2016, the Agency informed the Parliamentary Assembly of BiH and the public about cases that referred to the legality of the Agency's work. In 2013, the Agency began the procedure for the adoption of a new Rulebook on Internal Organization, in order to comply with the Decision on principles for establishing internal organization of administrative bodies of BiH and the Decision on the classification of jobs and criteria for job descriptions of jobs in the institutions of BiH. On this occasion, the Agency did not agree with the proposal made by the Legislative Office of the Council of Ministers of BiH which stated that seven years of work experience should be a condition for the position of Director and Deputy Director. The reason for this was that the Law stipulates five years of experience in management affairs in the administration. In addition, the Agency disagreed with the condition set by the Ministry of Finance and Treasury of BiH to abolish the position of the referent - Head of the office. The work of the Agency has therefore been plagued by administrative and political issues, and its independence remains problematic to a great extent.

4.1.7. The State does not prohibit, in law or in practice, anonymity, pseudonymity, confidentiality of private communications or the usage of encryption technologies. Interference with anonymity and confidentiality of communications is subject to the requirements of legality, legitimacy and proportionality of Article 8 of the Convention.

The state does not prohibit anonymity, pseudonymity, confidentiality of private communications.

4.2. Surveillance

4.2.1. The access to the content of communications is regulated and it is done in accordance with Article 8 of the ECHR.

The Law on Communications of BiH⁷⁷ obliges all outlets providing telecommunication services to ensure the function of a lawful interception of telecommunication services, as well as storing data. On the proposition of the Ministry of Security, the BiH Council of Ministers decides on the capacity of data storage as well as on lawful interception of telecommunications. While Article 8 of the ECHR allows for interference of public authority only in accordance with the law and as necessary in the democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, the protection of health or morals, or for the protection of the rights and freedoms of others, the positive laws under national jurisdictions should specify the criteria. The laws, as explained above, allow a broad discretion scope of the executive power and does not interpret any further the ECHR provision. More specifically, the Sector of the Ministry of Security for the Protection of Classified Information supervises the security vetting; issues security clearance for access to classified information of BiH, other state and international or regional organisations in accordance with the Law or international or regional agreements; monitors the situation in the fields of defining and protecting classified information and aims at improving and implementing physical, organisational and technical standards for the protection of classified information of the public.

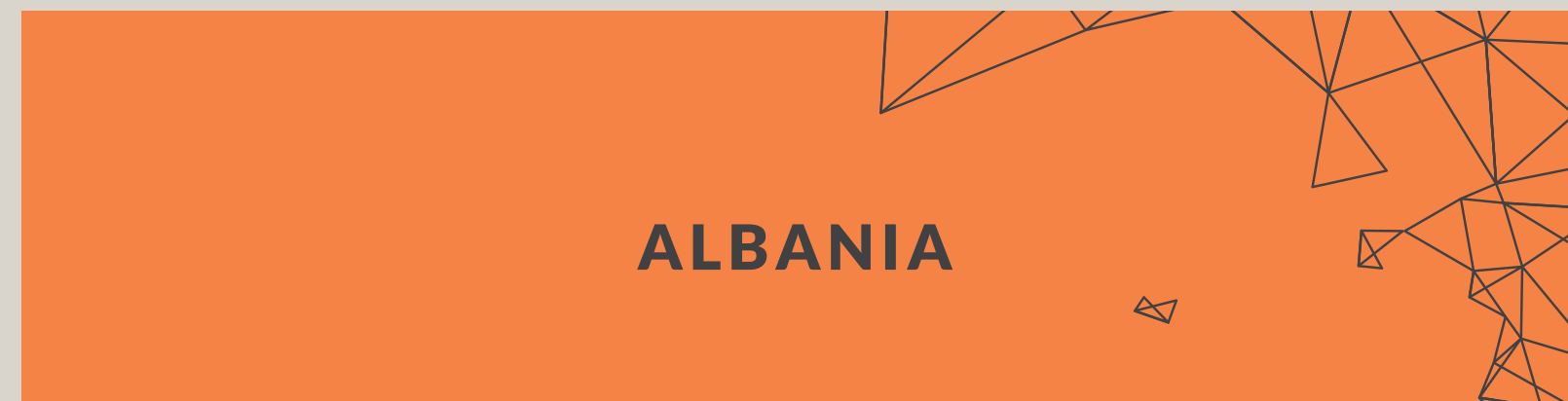
4.2.2. Operators of electronic communications are obliged by law to retain bulk communications metadata (time, date, location, duration, etc.). The time frame for storage of metadata is defined by law and access to metadata is done with a court order and in accordance with the standards of Article 8 of the ECHR.

The Communication Law does put an obligation on the telecom providers to save data. However, it does not specify for how long and in what format. In Article 7, it is stated that telecommunications operators shall meet the following requirements: a) Enter into a written contract with users; b) Make available to their service users, free of charge and in an appropriate manner, a short and clear summary of the tariffs applicable; c) At the request of the Agency deliver, within a reasonable period, business data, network data and traffic data including confidential data, if the telecommunications operator shall have kept such data as confidential.

4.2.3 Video surveillance of public spaces by state authorities is regulated. There are specific legal provisions regulating data processing by video surveillance.

The Law on the Intelligence and Security Agency⁷⁸ establishes the Intelligence and Security Agency of BiH, which is in charge of gathering, analyzing, and disseminating intelligence in order to protect the security, sovereignty, territorial integrity and constitutional order of BiH. The Agency operates in line with the Constitution of BiH. The Agency is entitled to collect information among other, from all publicly available sources, from other bodies and institutions in the country, through electronic surveillance, surveillance in non-public places and through "physical surveillance in public places (i.e. purposeful and systematic observation in order to gain information on specific matters of persons or objects reasonably believed to be involved in any activities or preparation of activities that fall under the scope of responsibilities of the Agency)". Therefore, the Ministry of Internal Affairs mandated by the Law on Agencies and Internal Services for the Protection of People and Property is in charge of video surveillance of public spaces, but it is for the local communities to implement their decisions on this.

4.2.4. There is oversight provided by law on how are surveillance and interception of communications done in practice. Article 71 of the Law on the Intelligence and Security Agency refers to a written application to a judge where one believes on reasonable grounds that surveillance is required to enable the Agency to investigate a threat to the security of BiH. All such applications must contain: the type of communication proposed to be intercepted, the type of information, records, documents or things proposed to be obtained, and the means to be exercised for that purpose. Article 72 states that the warrant must contain the type of communication proposed to be intercepted, the type of information, records, documents or things proposed to be obtained and the powers to be exercised for that purpose.



1. AN ENABLING ENVIRONMENT FOR INTERNET FREEDOM

1.1. The protection of human rights and fundamental freedoms on the internet is guaranteed in law, in full compliance with relevant articles of the European Convention on Human Rights (ECHR).

The Republic of Albania ratified the ECHR in 1996, meaning that the ECHR became part of Albania's legal system, therefore guaranteeing all human rights and freedoms prescribed by the Convention.⁷⁹ The Constitution of the Republic of Albania, in Article 17 states that "limitations of the rights and freedoms provided for in this Constitution may be established only by law, in the public interest or for the protection of the rights of others. A limitation shall be in proportion to the situation that has dictated it." However in paragraph 2 it states that "these limitations may not infringe the essence of the rights and freedoms and in no case may exceed the limitations provided for in the European Convention on Human Rights".

1.2. Laws and policies relating to the internet are assessed, at their drafting stage, with regard to the impact that their implementation may have on the exercise of human rights and fundamental freedoms in an inclusive and transparent process which enables the participation of all stakeholders, including the private sector, civil society, academia and the technical community.

Most recently, numerous international experts analyzed the Draft Laws on Changes and Amendments to the Law on Audiovisual Media and the Law of Electronic Communications in the Republic of Albania. The analysis referred to relevant provisions regarding the content provided through the internet. It was the OSCE that became involved in this process the most, and produced legal analysis⁸⁰ containing recommendations and assessments to make the law compliant with international standards. More precisely, the assessment referred to proposed amendments to Law no. 97/2013 on audiovisual media in the Republic of Albania and to Law no. 9918 of 19 May 2008 on electronic communications in the Republic of Albania, as well as the text of the Prime Minister's "Decision on measures to protect children from access to illegal and/or harmful content on the internet". The proposals have been submitted to the Office of the OSCE Representative on Freedom of the Media after the legal analyses conducted in 2018 on the draft law on "Additions and changes to Law no. 9918, dated 19.5.2008, on electronic communications in the Republic of Albania", and the draft law on "Changes and additions to Law no. 97/2013 on audio-visual media in the Republic of Albania". The assessment showed that there were certain improvements, meaning that the opinion of international experts was taken into account and that changes have been made especially with regards to the draft amendment to Law no. 97/2013. The provisions related to the domain name registration and blocking have been deleted from the draft, and it is now emphasized that Albanian Media Authority (AMA) should focus more on respecting international and regional standards when adopting its decisions. In addition, "another positive element is the fact that the proposal includes a specific adaptation of the right to reply to the new environment of electronic publications. The last version of the draft also incorporates new provisions, which define the object and scope of the law in a better and more precise way, making it clear that the law only applies to audiovisual media services and electronic publications providers. The draft also includes a better and definitely more consistent definition of electronic publications service providers."⁸¹

⁷⁹ European Court of Human Rights, Press country profile-Albania, January 2020.

⁸⁰ J. Barata Mir, Legal Analysis of the draft Law on Media Services in Albania, OSCE, 11 July 2019.

⁸¹ Ibid.

⁷⁷ Law on Communications (Official Gazette of BiH, No. 31/03) of Bosnia Herzegovina entered into force in 2002.

⁷⁸ Law on the Intelligence and Security Agency of BiH, (Official Gazette of BiH, No. 12/04 and 20/04).

1.3. Any state body which has regulatory or other competence over internet matters carries out its activities free from political or commercial interference, in a transparent manner and protects and promotes internet freedom.

Electronic and Postal Communications Authority or AKEP is a state body⁸² which has competence over internet and which also performs the function of a CERT. It is a legal, public, non-budgetary entity, which is governed by a Governing Council that is independent in decision-making and operates on the basis of its own internal rules of procedure. The Governing Council is composed of five members, who are elected by the Parliament on the proposal of the Council of Ministers. Although AKEP is formally an independent institution the fact that the members of its Council are elected by the majority in the Parliament makes it prone to political interference. Other bodies that have competence over internet are critical information infrastructure operators, operators of important information infrastructure, the National agency for computer safety (ALCIRT), the Directorate for Classified Information Security (DSIK) and the National Information Society Agency (AKSHI).

1.4. The state protects individuals from cybercrime through effective criminal justice or other measures. Notably they are prescribed by a law, which is accessible, precise, clear and foreseeable; pursue a legitimate aim; are necessary and proportionate in a democratic society and allow for effective remedies.

Albania signed and ratified the Budapest Convention on Cybercrime, and there is a domestic law similar to laws on information security,⁸³ which establishes a cyber-security authority. In addition, pursuant to Article 192/b, a fine or sentence of up to three years in prison are prescribed for every unauthorized access to a computer system or part of it, violating in this way the security measures. Article 293/b stipulates that for the interference in computer data that leads to damage, change or unauthorized deletion is sentenced with six months to three years in prison. Based on Article 293/c, the interference in computer systems related to unauthorized barriers caused to a computer system with the intention to change or delete data is punished with jail from three to seven years. Based on Article 293/a it is prohibited to peek illegally into non-public broadcasts or computer data, and this is punished with jail from three to seven years. Offense and slander are not included because they are civil and not criminal acts. Albanian Criminal Law also recognizes criminal offenses which are conducted with the help of internet and computer systems in the following articles: 74, 84, 119, 143, 186, 192, and 293 as well as in Articles 117, 147, 148 and 149, if these offenses are conducted with the use of computer systems.

1.5. The state provides media and digital literacy programmes for internet users.

There is no data about state organized media and digital literacy programs. The law that sets the framework on pre-university education in Albania is Law No.69/2012 “On pre-university education in the Republic of Albania.” However, media literacy is not specifically mentioned, although “the law does include in the list of fundamental competencies that students in pre-university level must acquire also “digital competencies”. But apart from media literacy being only a small part of other subjects in state curricula, there are no current attempts to introduce it as a mandatory or optional subject. The initiatives on media and digital literacy mainly come from civil society in Albania. For example, the projects on enhancing digital literacy are conducted by the Albanian-American Development Foundation (AADF) established in 2009 by the Albanian-American Enterprise Fund with the support and encouragement of the United States Agency for International Development (USAID) and the United States Government.

2. THE RIGHT TO FREEDOM OF EXPRESSION

2.1. Freedom to access the internet.

2.1.1. The internet is available, accessible and affordable to all groups of the population without any discrimination.

There is no discrimination regarding internet access to any group of the population. and the Law on Information Security states that AKEP provides access to users with disabilities in Article 15.⁸⁴ The internet in Albania is affordable and well-spread in all groups of society. Media in Albania referred to a survey published by cable.co.uk that concluded that the internet in Albania is the cheapest one in the region.⁸⁵

2.1.2. The public has access to the internet in facilities supported by public administration (internet access points), educational institutions or private owners (universal community service).

There are no data on internet access points and universal community service.

2.1.3. The state takes reasonable measures to ensure access to the internet to those with low income, in rural or geographically remote areas and those with special needs such as persons with disabilities.

⁸² Law on Information Security, (Official Gazette of the Republic of Albania, No.2/2017).

⁸³ Ibid.

⁸⁴ Law on Information Security, (Official Gazette of the Republic of Albania, No.2/2017).

⁸⁵ Oculus News, Albania the cheapest internet price in the region, May 2019.

The Law on Electronic Communications in the Republic of Albania, in bullet 52 states that “Universal service” is “a minimum set of public electronic communication services of specified quality which is available at an affordable price to all users in the territory of the Republic of Albania, regardless their geographic location.” In addition, paragraph 3 of Article 27 states: “Universal service providers may offer optional tariffs, special tariff packages and special payment methods for subscribers with low income and/or special needs, in compliance with the legislation in force.” However, in 2015, it was stated that Albania had the internet of the lowest quality in Europe as far as speed and coverage is concerned. The International Telecommunication Union, ranked Albania 40th in Europe, and 94th amid the 167 world countries.⁸⁶ According to the report “the highest value of the Index of Development in Information Technology is 7.35 points, with the only country in the region, Albania, which is below the average of 5.03 points”. Albania had 4.73 points and the internet speed continued to be low (from 1 mbps up to 8 mbps at home connections) and the price was from 10 euros a month up to 100 euros a month for higher speeds. On the other hand, the internet offered for mobile phones is widely spread through 4G and 4G+ networks. Therefore, with such high prices, the state does not take reasonable measures to offer acceptable speed at acceptable prices, which makes it difficult for people with low income to have internet access.

2.1.4. There are no general, nationwide restrictions on access to the internet.

There is no state mandated blocking or filtering of internet content on the national level. Internet shutdowns also do not occur in Albania..

2.2. Freedom of opinion and the right to receive and impart information

2.2.1. Any measure taken by state authorities or private-sector actors to block or otherwise restrict access to an entire internet platform or information and communication technologies, tools, or any request by state authorities to carry out such actions complies with the conditions of Article 10 of the ECHR.

Recently, there have been numerous debates on the new laws regarding freedom of expression in Albania. International experts assessed the state initiatives as strict and that the newly proposed legislation envisages very concerning conditions for online media outlets. The issues that are currently highlighted in debates are: recent physical attacks against journalists have gone unresolved; top public officials regularly use language that belittles and smears critical journalists; the public administration, including the office of the Prime Minister and the Mayor of Tirana, are not transparent in their interactions with the media and restrict access to critical journalists.⁸⁷ Numerous organizations pointed out that the draft laws “aim to create a registry of online publications and empower a new “Complaints Council” to sanction online media, based on third-party requests, ordering their closure or blocking access to such media in Albania.”⁸⁸ More precisely, the draft laws provide legal mechanisms for the Audiovisual Media Authority AMA and Tax Authority to fine or close online media outlets, blogs and other publications on the internet without clear procedures, which could cause censorship and self-censorship in Albania’s media. In 2018, Albania’s Electronic and Postal Communications Authority has given 44 websites - including BIRN Albania and Reporter.al - a 72-hour deadline to register with tax officials or be closed entirely. On this occasion, AKEP stated that this requirement would be in line with the law, but it was not specified to which law it referred. Moreover, “the move comes after Prime Minister Edi Rama said on Friday that websites must be ‘legalised’ by registering with the tax authorities as part of an ‘anti-defamation’ drive targeting online media.”⁸⁹

2.2.2. Internet service providers as a general rule treat internet traffic equally and without discrimination on the basis of sender, receiver, content, application, service or device.

The Law on Electronic Communication stipulates an equal treatment of internet traffic without discrimination in Article 7, 8, 15, 25 (universal service), and 39.

2.2.3. Internet users or other interested parties have access to a court in compliance with Article 6 of the Convention with regard to any action taken to restrict their access to the internet or their ability to receive and impart content or information.

Article 120 in Law on Electronic Communications refers to Disputes resolution.⁹⁰ More precisely, it defines the tasks belonging to AKEP. Therefore, first it states that AKEP shall resolve disputes between undertakings of electronic communications networks and services, initiate a dispute resolution procedure at the request by any party to the dispute, apply the provisions of the Code of Administrative Procedures to the dispute resolution. In addition, in cases of

disputes, AKEP is obliged to take into consideration the objectives of ensuring effective competition and protection of users’ interests, and publish decisions relating to disputes.

⁸⁶ Albanian Newroom, Albania has the lowest quality of internet in Europe, 1 December 2015.

⁸⁷ Reporters without Borders, Albania: Preliminary findings of joint freedom of expression mission, 21 June 2019.

⁸⁸ B. Likmeta, Albania Rights Groups Condemn ‘Undemocratic’ Media Bills, BIRN, 18 Januae 2019.

⁸⁹ G. Erebara, Albanian Authorities Threaten to Close 44 Websites, BIRN, 15 October 2018.

⁹⁰ Law on Electronic Communications in the Republic of Albania, (Official Gazette of the Republic of Albania, No. 9918/2008, of 19.05.2008).

2.3. Freedom of the media

2.3.1. The editorial independence of media operating on the internet is guaranteed in law, policy and practice.

The editorial independence of media is regulated with Article 4 of the Law on Audio and Audio-Visual Media Services in the Republic of Albania, but just for TV, radio and services on demand; media operating on the internet is not regulated by this law. However, in practice, two shows which were critical of the Prime Minister, were canceled and there were allegations that government pressure was behind their cancellation. The reports of the authorities pressuring media are rather often in Albania. The Prime Minister used “derogatory language against critical journalists to issue threats of lawsuits and push for laws that aim to curb freedom of speech.”⁹¹ Furthermore, the Prime Minister “threatened German newspaper Bild with lawsuits following the publication of a series of intercepted conversations showing the collusion of Rama’s Socialist Party with various criminal gangs for the purpose of election rigging, vote-buying and putting pressure on voters.” Numerous organizations pointed at the Prime Minister also “attempting to create a media censorship system through proposed changes in the country’s audio-visual media laws,”⁹² all of which are likely to cause chilling effects among the media and the public.

2.3.2. Media are not required to obtain permission or a licence from the government or state authorities, beyond business registration, in order to be allowed to operate on the internet or blog.

Most recently, the office of Albania’s Prime Minister proposed changes in two laws envisaging the registration of online media and the policing of news content for a variety of reasons, including “biased” news, news that “damages public morale” and “publications that can incite penal offences”.⁹³ If the Law is not respected, the fines will reach up to 1 million leks (8,000 euros) or even closure of websites. These proposals raised numerous concerns and posed a risk of censorship and a negative effect on the freedom of expression online. More specifically, the first draft amending the Law on the Telecommunication and Postal Authority, will stipulate for the authority that supervises the communications sector, transforming the institution from its current content-neutral status to being responsible for maintaining a “register of online media” and ensuring that “entrepreneurs respect their obligations toward national security, public safety ... and other laws”. The Law would make it obligatory for the website of any physical or legal entity to have contact information and a physical address published on the site and orders the AKEP to close websites based on “Tax Authorities’ request”. The other proposal aims to transform the Albanian Audiovisual Media Authority, AMA, into a policing body, empowered to judge news quality and public morale. Therefore, publishers should have to “respect the ethical and moral rules of the public and should not allow publication ... that can incite penal offences”. There would also be a body, the Complaints Council, which would receive complaints and fine media or order their closure if found in breach of the law. The proposal also states that fines and closure orders should be implemented immediately, regardless of whether the website chooses to send the matter before the courts.

2.3.3. Journalists and other media actors using the internet are not subject to threats or harassment by the state. They do not practise self-censorship because of fear of punishment, harassment or attack.

Journalists and media actors are often targets of attacks in Albania. Some state actors often turn to verbal attacks and smears of journalists, while they do not provide any protection either. For example, Reporters Without Borders (RSF)⁹⁴ stated that a TV journalist was threatened at gunpoint in a small town in northern Albania. Previously bursts were fired with an assault rifle at the home of an investigative reporter in Tirana⁹⁵. Julian Shota, a reporter for commercial TV channel *Report TV*, was covering an explosion in a bar but he was immediately ordered to leave by its owner who used a gun and threatened to shoot him.

2.3.4. The confidentiality of journalists’ and other media actors’ sources is protected in law and respected in practice.

The national media legislation in Albania includes the protection of journalists’ sources. The relevant laws are: the Law on Public and Private Radio and Television, No. 8410, Law on Audiovisual Media adopted in 2013.6, etc. According to Article 159 (1) of Criminal Procedural Code, journalists or any other professionals are not obligated to testify on what they are aware of, if that is part of the professional secret, except in specific cases for procedural authorities. There are no particular provisions on journalists or their right to protect sources for information classified as State Secret Acts 12. The Code of Ethics of the Albanian Media protects the sources of information possessed by journalists. This Code of Ethics was drafted in 1996 and revised in 2006 with the initiative of the Albanian Media Institute, and the two main journalist associations: the Union of Albanian Journalists and the League of Professional Journalists. However, the Code is not binding. Therefore, there is an implicit right for journalists not to disclose their sources of information, and there is the lack of the definition of a “source” and “information identifying a source”, as set out in the Council of Europe Recommendation No. R(2000)7.

2.3.5. Media websites and websites of new media actors are not affected by cyber-attacks or other action disrupting their functioning.

91 V. Karaj, Last TV Shows Critical of Albanian Government are Cancelled, BIRN, 29 August 2019.

92 V. Karaj, Last TV Shows Critical of Albanian Government are Cancelled, BIRN, 29 August 2019.

93 G. Erebara, Albanian Authorities Threaten to Close 44 Websites, BIRN, 15 October 2018.

94 Reporters without Borders, Albanian journalists repeatedly threatened, attacked, 4 September 2018.

95 G. Erebara, Attack on Albania Crime Journalist’s Home Condemned, BIRN, 30 August 2018.

There is no information that Albanian news websites face cyber-attacks, but there are other forms of pressures and disruptions. For example, there are online media in Albania which claim that their online content is being censored by a company called Acromax GmbH. The content of certain media outlets was removed from their Facebook page because they had used other media videos.⁹⁶

2.3.6. There are prompt and effective investigations of threats and crimes against journalists and new media actors. There is no climate of impunity.

There is no data on the effectiveness of investigations regarding those who threaten journalists and media actors, apart from the information provided under section 2.3.3.⁹⁷

3. THE RIGHT TO FREEDOM OF PEACEFUL ASSEMBLY AND ASSOCIATION

3.1. Individuals are free to use internet platforms, such as social media and other ICTs in order to associate with each other and to establish associations, to determine the objectives of such associations, to form trade unions, and to carry out activities within the limits provided for by laws that comply with international standards.

Freedom of assembly in Albania is regulated by Article 46 of the Constitution: “everyone has the right to be organized for any legitimate purpose” and in Article 47: “the freedom of peaceful and unarmed assembly, as well as participation in them is guaranteed. Peaceful gatherings in the squares and in public places are done according to the procedures provided by the law.” Freedom of assembly is regulated by Law no. 8773 dated 23.4.2001 “On Assemblies”, according to which everyone has the right to organize and participate in peaceful assemblies without any exclusion. Other laws that refer to the organisation of assembly are: Law no. 7895, dated 27.1.1995 “The Criminal Code of the Republic of Albania” and Law no.108/2014 “On the State Policy”. According to the Law on Assemblies and its Article 2, the term “assemblies”, includes “peaceful and free of weapons, gatherings, manifestations, meetings and marches, through which a group of people express their demands and views on problems for which they are interested and also includes urgent assemblies.”

3.2. Associations are free to use the internet in order to exercise their right to freedom of expression and to participate in matters of political and public debate.

In line with regulations referring to public assemblies, there are no restrictions imposed on associations regarding their right to freedom of expression and participation in political and public debates in the online sphere.

3.3. Individuals are free to use internet platforms, such as social media and other ICTs in order to organise themselves for purposes of peaceful assembly.

According to regulations regarding public assemblies, there are no restrictions to freedom of use of the internet, for the purposes of peaceful assembly. The most used social network in Albania is Facebook with 1,4 million users. Recently, Facebook was precisely the most used communication channel for organizers and participants of assemblies to spread information, and increase the number of supporters. Overall, the organizers of assemblies usually create a Facebook page, then they identify the name and issue that is being protested and create their own content of the assembly which includes information, “photos, discussions with followers, different posts with articles, videos and declarations from and for the issue of the assembly.”⁹⁸ Social networks are very often used for organising protests and mobilising protesters, and the government does not impose any restriction for the use of the social media. Organizers/ participants can use it before, during and after the organization of the assembly, and based on the survey carried out with 96 surveyed CSOs, none of them have experienced any blocking of the access to online communication.

4. THE RIGHT TO PRIVATE AND FAMILY LIFE

4.1. Personal data protection

4.1.1. The right to private and family life is guaranteed in compliance with Article 8 of the Convention. Any restriction to this right pursues one of the legitimate aims exhaustively enumerated in Article 8 of the Convention, is necessary in a democratic society and proportionate to the legitimate aim pursued. The law guarantees that all personal data is protected in compliance with Article 8 of the Convention and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) in States which have ratified it.

Albania ratified the European Convention on Human Rights, and based on Article 131 of the Constitution, the Constitutional Court controls the compatibility of Albanian legislation with the standards of the ECHR. The right

96 J. Estrada, Acromax Media — Albanian Government’s Tool for Online Political Censorship, 19 August 2019.

97 Reporters without Borders, Albanian journalists repeatedly threatened, attacked, 4 September 2018.

98 K. Kosta, A. Topi and K. Keruti, Partners Albania for Change and Development, Monitoring the right to freedom of Assembly, Country Report - Albania 2016-2017, December 2017.

for a private life is guaranteed under Articles 35, 36, 37 of the Constitution. The Criminal Code of Albania stipulates the protection of private life. Based on Article 121 'Unjust interference in private life' the hearing, registration and transmission of the words or images through specific machines and, the publication of information about private life of the individual without his/her consent are punished with a fine or sentence of up to two years in prison. Article 122 mentions personal information and so a person, who, due to one's own job, collects information on the life of other people, must preserve and not disclose it. Should it occur the person will be subject of a fine or sentenced to one year in prison. According to Article 123, any deliberate action that consists in opening letters, non-delivering or exterminating them, as well as any other correspondence is punished with a fine or sentence to two years in prison. The Law on the Protection of Personal Data No. 9887 defines the rules for the protection and legal processing of the personal data. It is based on Articles 78 and 83, point (1) of the Constitution that guarantees to everyone the right to privacy and protection of personal data. Any collection, storage and elaboration of personal data is to be carried out in accordance with the Law. Article 2 of the Law provides that the legal processing of personal data shall respect and guarantee the fundamental rights and freedoms of persons, and in particular their right to privacy.

4.1.2. Personal data are processed lawfully (with the unambiguous consent of the data subject or on the basis of law) for legitimate purposes and not in excess of such purposes, accurately and securely.

According to the Law on Personal Data Protection, it is the Office of Information and Data Protection Commissioner that oversees the lawful processing of data. The Commissioner is in charge of: "conducting administrative enquiries of public and private controllers focusing especially on areas impacting privacy and reflecting the technological developments in personal data processing; guaranteeing the data subjects' rights and the practical fulfilment of public and private controllers' duties; instilling the spirit and novelties emerging from the General Data Protection Regulation (GDPR) in all internal monitoring and supervising processes and mechanisms". The controllers have been mainly sanctioned by fines for the lack of technical and organizational measures, drafting of the personal data processing regulation, omission to sign the confidentiality declaration with employers who have access to personal data, arranging the relations with processors in cases of data processing delegation, non-publication of privacy policies in official websites, failure to inform the data subject on the presence of video surveillance (CCTV) system, consisting of obligations stemming from the Law No. 9887/2008 "On Personal Data Protection" and Commissioner's Office bylaws. In 2018, the Commissioner's Office issued 30 fine penalty decisions and 61 administrative sanctions.⁹⁹

4.1.3. Individuals are not subjected to a decision significantly affecting them based solely on automated processing of data without having their views taken into account.

According to the annual reports of the Commissioner, the complaints filed dealt mostly with: violation of data subjects rights (right to access, as a paramount data subject right, allowing the latter to receive information from the controller on its data processing); disclosing or transmitting personal data without prior consent of the personal data subject to unauthorized individuals to protect personal data; unlawful and unjust data processing (their dissemination in the media and online portals); installing surveillance cameras in public and private places; direct marketing on unsolicited communications via phone or email; exceeding the personal data collection deadline for a specific purpose. In total, in 2018, 245 complaints were filed and 170 of them were in compliance with the Law. The Commissioner's Office uses the email address info@idp.al available to data subjects for submitting complaints.

4.1.4. There are effective processes enabling every individual to obtain, on request, information on the processing of his or her personal data and the reason underlying processing; to object to processing; to obtain, on request, rectification or erasure of the personal data; and to consent to, object to or withdraw consent to personal data processing or profiling. An effective remedy exists for individuals when these rights are not respected. Legal frameworks for personal data protection provide adequate safeguards for access to information and freedom of expression.

The decision of the Council of Ministers No. 145, "On Creating the State Database "Requests and Responses E-register on the Right to Information"" approved the creation of central requests and responses register. This register was installed in 27 central institutions. Citizens used the option of turning to the Commissioner regarding the violations of their rights in terms of personal data. Therefore, based on Law No. 119/2014 "On the Right to Information", 820 complaints were filed with the Commissioner's Office. According to the Annual Report of the Commissioner for 2018, out of this number, 622 were settled with no intermediation. 37 out of such complaints were settled by a Commissioner's Decision, 116 were outside of the scope, 9 were beyond the deadline, 17 were incomplete and 24 are in the process.¹⁰⁰ Most complaints were settled through intermediation and the majority of complaints were filed by citizens. More precisely, 656 complaints were filed by citizens, while 164 were filed by civil society organizations. This number shows that the citizens' awareness is raising when it comes to the right to information. The Commissioner's Office also maintains its relations with civil society and journalists. Several civil society organizations "operating in overseeing the implementation of the law no. 119/2014 "On the Right to Information" have evaluated this year as well the Commissioner's Office as the most transparent institution at the national level."¹⁰¹

⁹⁹ Office of Information and Data Protection Commissioner, Annual report 2018.
¹⁰⁰ Ibid.
¹⁰¹ Office of Information and Data Protection Commissioner, Annual report 2018.

4.1.5. The law defines the duties of public and private entities with regard to processing of personal data.

Article 32 of the Law on Protection of Personal Data, stipulates the "Obligation to Cooperate". In its first paragraph it is stated that "1. Public and private institutions shall cooperate with the Commissioner providing all the information required by this institution for the fulfilment of its duties." The Law defines the Controller as "the natural or legal person, public authority, agency or any other body, which alone or jointly with others store, process, administer, archive and therefore control personal data." And "Processor" is "a natural or legal person, public authority, agency or other body, except for the employees of the Controller, which processes personal data on behalf of the Controller." "Recipient" is a private individual or legal entity, public authority, agency or any other body to whom data are disclosed.

4.1.6. A supervisory authority, which acts with complete independence and impartiality, ensures compliance with data protection legal frameworks.

In Albania, the Information and Data Protection Commissioner; an independent institution of public administration, is elected by the Assembly, based on the proposal of the Council of Ministers. The structure and salaries of the Commissioner are determined by the Assembly. The scope of work of the Commissioner includes conducting administrative investigation, accessing personal data processing, collecting the necessary information for supervision, issuing orders for the blocking, erasure, destruction or suspension of the unlawful processing of personal data and instructions prior to the data processing ensuring their publication. Furthermore, the Commissioner checks and accesses information and documents, subject to appeal, according to the law on freedom of information or related to the matter under consideration, including information classified as "state secret". In addition, the Commissioner handles the complaints, conducts administrative enquiries for public and private controllers (at its own discretion or on a complaint basis) on personal data processing, attends and conducts hearings with controllers and proposes measures to be adopted in accordance with the Commissioner's powers (recommendation, decision, order); verifies recommendations implementation; registers the Controllers (notice form) with the "Controllers E-register", partly accessible to the public in the IDP website.

The structure of the Commissioner includes the departments of: the right to information, personal data protection, administrative investigation, legal affairs, communication and international relations and internal services and finances. The citizens have the possibility of submitting complaints to the Commissioner related to violations of their rights. The Commissioner regularly publishes reports based on the review of the Information and Data Protection Commissioner (IDP) institutional performance for 2018, concerning the monitoring and implementation of the Law No. 119/2014 "On the Right to Information" and Law No. 9887/2008, "On Personal Data protection", as amended. The rights mentioned in these laws are part of the Constitution of the Republic of Albania, the country's supreme law, set forth more specifically under Article 23 and 25.¹⁰²

4.1.7. The state does not prohibit, in law or in practice, anonymity, pseudonymity, confidentiality of private communications or the usage of encryption technologies. Interference with anonymity and confidentiality of communications is subject to the requirements of legality, legitimacy and proportionality of Article 8 of the Convention.

The state does not prohibit anonymity, pseudonymity, confidentiality of private communications.

4.2. Surveillance

4.2.1. The access to the content of communications is regulated and it is done in accordance with Article 8 of the ECHR.

Lawful interception in Albania is justified by the need to keep up with effective investigation of crimes. Relevant laws have had several amendments to increase the effectiveness of the interceptions, but it is still rather obvious that the implementation has not been adequately developed. There were reports on unlawful interceptions, and the latest amendments of the "Law on interception and the Code of Penal Procedure in 2017 provide for an expansion of the interception competences and the increased use of such procedure through the development of multiple intercepting capabilities."¹⁰³

4.2.2. Operators of electronic communications are obliged by law to retain bulk communications metadata (time, date, location, duration, etc.). The time frame for storage of metadata is defined by law and access to metadata is done with a court order and in accordance with the standards of Article 8 of the ECHR.

According to Vodafone's Law Enforcement Disclosure Report Legal Annex¹⁰⁴ for 2014, when it comes to data retention policies in Albania, they are defined by the Law on Electronic Communications. In Article 101(6) of the Law on Electronic Communications, it is prescribed that the relevant authorities shall be provided with any files stored by operators in relation to their users and such files shall be made available, in electronic format as well, to authorities prescribed in the

¹⁰² Office of Information and Data Protection Commissioner, Annual report 2018.
¹⁰³ A. Dyrimishi, Interceptions of Communications in Albania: Legislation, Practice and Accountability System, Center for the Study of Democracy and Governance, September 2018.
¹⁰⁴ Vodafone, Law Enforcement Disclosure Report Legal Annex June 2014.

Code of Criminal Procedure, upon their request. All such data is retained in accordance with the applicable legislation on personal data protection in Albania.

4.2.3 Video surveillance of public spaces by state authorities is regulated. There are specific legal provisions regulating data processing by video surveillance.

Most recently, the Ministry of Interior lead an initiative for the adoption of a law on new measures to safeguard public security, and this law was passed by the parliament. However, the President refused to support this law because it violates privacy, Albania's constitution and the European Convention on Human Rights. It was stated that according to Article 35 of the Constitution "the law does not respect and protect personal data and the private life of the citizens".¹⁰⁵ There were also concerns in terms of the footage taken from surveillance cameras because it was not clear how it was going to be used and managed. The law makes it obligatory for the administrators of business units, public and private institutions such as schools and kindergartens, private areas used for children as playgrounds and public transport vehicles to install security cameras in what the police identify as "risky areas." The law also made it possible for camera surveillance to be used in private building complexes but in these cases the approval of residents is required.

4.2.4. There is oversight provided by law on how are surveillance and interception of communications done in practice.

Relevant laws regarding surveillance and interception of communications are the Law No. 119/2014 "On the Right to Information" and Law No. 9887/2008, "On Personal Data protection". There is also the important Decision of the Commissioner no.3 as of 5 March 2010 "On processing personal data with video surveillance in buildings and other environments", according to which the use of CCTV is considered lawful and in line with the applicable legislation. In addition, Articles 221-222 of Albanian Code of Criminal Procedure (ACPC) allow the interception of communications and secret surveillance and the use of such evidence in court. Interception of communications is permitted only where there is a proceeding for intentionally committed crimes punished by imprisonment of no less than seven years; and criminal contravention of insult and threat committed by means of telecommunications..

	SERBIA	KOSOVO	BOSNIA AND HERZEGOVINA	ALBANIA
1. An enabling environment for internet freedom				
1.1. The protection of human rights and fundamental freedoms on the internet is guaranteed in law, in full compliance with relevant articles of the European Convention on Human Rights (ECHR).	4	3	4	4
1.2. Laws and policies relating to the internet are assessed, at their drafting stage, with regard to the impact that their implementation may have on the exercise of human rights and fundamental freedoms in an inclusive and transparent process which enables the participation of all stakeholders, including the private sector, civil society, academia and the technical community.	3	2	3	2
1.3. Any state body which has regulatory or other competence over internet matters carries out its activities free from political or commercial interference, in a transparent manner and protects and promotes internet freedom.	3	3	3	2
1.4. The state protects individuals from cybercrime through effective criminal justice or other measures. Notably they are prescribed by a law, which is accessible, precise, clear and foreseeable; pursue a legitimate aim; are necessary and proportionate in a democratic society and allow for effective remedies.	3	2	3	3
1.5. The state provides media and digital literacy programmes for internet users.	3	1	1	1
2. The right to freedom of expression				
2.1. Freedom to access the internet	4	4	4	4
2.2. Freedom of opinion and the right to receive and impart information	3	3	3	2
2.3. Freedom of the media	2	2	3	2
3. The right to freedom of peaceful assembly and association				
3.1. Individuals are free to use internet platforms, such as social media and other ICTs in order to associate with each other and to establish associations, to determine the objectives of such associations, to form trade unions, and to carry out activities within the limits provided for by laws that comply with international standards.	4	3	4	4
3.2. Associations are free to use the internet in order to exercise their right to freedom of expression and to participate in matters of political and public debate.	4	3	4	4
3.3. Individuals are free to use internet platforms, such as social media and other ICTs in order to organise themselves for purposes of peaceful assembly.	4	3	4	4
4. The right to private and family life				
4.1. Personal data protection	4	4	3	2
4.2. Surveillance	2	3	3	2

- 1 Laws, policies and practice are not compliant with international standards at all and urgent improvement is needed.
- 2 Laws, policies and practice are not compliant with international standards and much improvement is needed.
- 3 Laws, policies and practice are compliant with international standards in some aspects, but there is not enough information to fully assess how successful they are.
- 4 Laws, policies and practice are compliant with international standards to some degree, but there is some improvement needed.
- 5 Laws, policies and practice are fully compliant with international standards and no improvement is needed.

105 F. Mejdini, Albania President Blocks Surveillance Law, BIRN, 6 April 2016.

RECOMMENDATIONS

Given the state of internet freedoms in the examined countries, there is clear room for improvement, but certain areas should be prioritized when the capacities of all stakeholders, i.e. the state, the private sector and civil society, are taken into account. Therefore, recommendations for advancing and improving the state of internet freedoms in the examined countries are provided below.

- Private and state actors should discontinue exerting pressures on online media, journalists and internet users. There is a visible trend of a range of verbal attacks, threats, smear campaigns and other forms of pressures which hinder the free flow of information online, which should be investigated with priority and dealt with in accordance with relevant laws.
- State institutions need to encourage a broad multi-stakeholder public debate on all legislative instruments (laws, bylaws etc.) concerning the respect for human rights on the internet and in relation to technology. As there are numerous challenges ahead, such as the possible use of artificial intelligence (AI) for the purposes of law enforcement, a wide social debate with civil society and expert community is necessary.
- States should ensure that media and information literacy programs are carried out on a national scale, especially among youth and in cooperation with educational institutions. Also, there is a need for media and literacy trainings for teachers and other educators.
- Further efforts are needed to protect net neutrality in the examined countries, i.e. in line with EU net neutrality rules, as it is crucial for the healthy development of the digital environment and provision of all digital services under the same standards.
- Taking into account the start of application of the EU General Data Protection Regulation (GDPR) in May 2018, it is needed to align the legal framework for personal data protection with the new EU standards. Serbia is the first country to adopt and start implementing the new Law on Personal Data Protection, which is based on GDPR, but still needs improvement. BiH, Albania and Kosovo should follow the example of Serbia and start reforms of personal data protection legislation as soon as possible.
- In terms of surveillance of electronic communications and access to retain communications' metadata, it needs to be done in accordance with the constitutional guarantees of the secrecy of communications, privacy and the protection of personal data, as well as with international human rights standards such as Article 8 of the European Convention on Human Rights. Also, the jurisprudence of the European Court of Human Rights in these matters needs to be taken into account. Although the countries in question are not EU Member States, all of them are in different stages of joining the EU and should therefore also consult the jurisprudence of the Court of Justice of the EU.

BIBLIOGRAPHY

A. Dyrimishi, Interceptions of Communications in Albania: Legislation, Practice and Accountability System, Center for the Study of Democracy and Governance, September 2018, available at: <https://csdgalbania.org/interceptions-of-communications-in-albania-legislation-practice-and-accountability-system/>

Albanian Newsroom, Albania has the lowest quality of internet in Europe, 1 December 2015, available at: <https://balkaneu.com/albania-lowest-quality-Internet-europe/>

Authority of Electronic and Postal Communications, available at: <http://www.arkep-rks.org/?cid=2,28>

B. Likmeta, Albania Rights Groups Condemn 'Undemocratic' Media Bills, BIRN, 18 Januae 2019, available at: <https://balkaninsight.com/2019/01/18/albania-rights-organizations-oppose-online-media-bills-01-18-2019/>

BelnKosovo, Communications in Kosovo, available at: <http://www.beinkosovo.com/communications-in-kosovo/>

Civil Law against Defamation and Insult, (Official Gazette of the Republic of Kosovo, No. 24/2008), available at: <https://gzk.rks-gov.net/ActDetail.aspx?ActID=2503>

Civil Rights Defenders, Freedom of Expression, Media and Information in Kosovo: An Assessment Based on Council of Europe Indicators for Media in a Democracy, available at: https://crd.org/wp-content/uploads/2018/12/Freedom_of_Expression_Media_and_Information_in_Kosovo_529396.pdf

Code of Criminal Procedure, (Official Gazette of the Republic of Kosovo, No.74/2010), available at: <https://gzk.rks-gov.net/ActDetail.aspx?ActID=2682>

Commissioner for Information of Public Importance and Personal Data Protection, Annual Reports, available at: <https://www.poverenik.rs/en/o-nama/annual-reports.html>

Commissioner for Information of Public Importance and Personal Data Protection, The summarized annual report for 2018, available at: <https://www.poverenik.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2018/ENGRezime2018.pdf>

Constitution of BiH, (1995), entered into force 14 December 1995, available at: http://www.ccbh.ba/public/down/USTAV_BOSNE_I_HERCEGOVINE_bos.pdf

Constitution of Republika Srpska (1992), Official Gazette of RS No. 28/94, entered into force in 1994, available at: http://www.ustavnisud.org/upload/4_8_2009_48_ustav_srpski.pdf

Constitution of the Federation of BiH (Sarajevo, 30 March 1994), Official Gazette of FBiH No.1/94, entered into force 30 March 1994, available at: http://skupstinabd.ba/ustavi/f/ustav_federacije_bosne_i_hercegovine.pdf

Constitution of the Republic of Kosovo, June 2008, available at: <http://www.kryeministri-ks.net/repository/docs/Constitution1Kosovo.pdf>

Constitution of the Republic of Serbia, (Official Gazette of the Republic of Serbia, No. 98/2006), available at: <http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/ustav/2006/98/1/reg>

Council of Europe, Chart of signatures and ratifications of Treaty 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Status as of 03/02/2020, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=cg0M9o77

Criminal Code of Kosovo Cybercrime, (Official Gazette of the Republic of Kosovo, No.2/2019), available at: <https://gzk.rks-gov.net/ActDetail.aspx?ActID=18413>

Criminal Code of Serbia, (Official Gazette of RS, Nos. 85/2005, 88/2005, 107/2005), Chapter 27, Articles 298-304a, available at: <http://www.zakon.co.rs/tekstovi-zakona-na-engleskom-jeziku.html>

Criminal Procedure Code of BiH, (Official Gazette, No. 03/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06 , 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09).

Decision on Policy of the development of the information society in BiH for the period 2017-2021, (Official Gazette of BiH, No. 42/17), available at:

http://www.mkt.gov.ba/dokumenti/informatizacija/ostali_propisi/default.aspx?id=5843&langTag%e2%80%8e=bs-BA&langTag=bs-BA

Development, Monitoring the right to freedom of Assembly, Country Report - Albania 2016-2017, December 2017, available at:

<https://partnersalbania.org/publication/monitoring-right-to-free-assembly-albania-country-report-2016-2017/>

E. Dizdarevic, Bosnia Failing in Fight against Extremism Online, BIRN, 13 August 2019, available at:

<https://balkaninsight.com/2019/08/13/bosnia-failing-in-fight-against-extremism-online/>

E. Bavic, Monitoring Right to Free Assembly BiH Country Report 2016-2017, ECNL and Civil Rights Defenders, December 2017, available at:

<http://ecnl.org/wp-content/uploads/2017/12/ECNL-FoPA-BiH-2017.pdf>

European Commission, “BiH 2016 Report”, p. 21, available at:

https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2016/20161109_report_bosnia_and_herzegovina.pdf

European Court of Human Rights, Press country profile-Albania, January 2020, available at:

https://www.echr.coe.int/Documents/CP_Albania_ENG.pdf

F. Mejdini, Albania President Blocks Surveillance Law, BIRN, 6 April 2016, available at:

<https://balkaninsight.com/2016/04/06/law-on-surveillance-raises-privacy-concerns-in-albania-04-05-2016/>

Freedom House Report for Kosovo 2015, available at: <https://freedomhouse.org/report/freedom-press/2015/kosovo>

Freedom House Report, Serbia, available at: <https://freedomhouse.org/report/freedom-world/2019/serbia>

G. Erebara, Albanian Authorities Threaten to Close 44 Websites, BIRN, 15 October 2018, available at:

<https://balkaninsight.com/2018/10/15/albania-communication-authority-threatens-website-closure-10-15-2018/>

G. Erebara, Attack on Albania Crime Journalist’s Home Condemned, BIRN, 30 August 2018, available at:

<https://balkaninsight.com/2018/08/30/attack-against-albania-journalist-home-condemned-08-30-2018/>

H. Mandić, “Regulation of Broadcasting in BiH”, in Halilović, Mehmed and Amer Džihana, Media law in BiH, Internews in BiH, Sarajevo, 2012.

Innovations Lab Kosovo, Techstitution: A Platform of Social Innovators in Kosovo, 17 August 2017, available at:

<http://kosovoinnovations.org/techstitution-a-platform-of-social-innovators-in-kosovo/>

J. Barata Mir, Legal Analysis of the draft Law on Media Services in Albania, OSCE, 11 July 2019, available at:

<https://www.osce.org/representative-on-freedom-of-media/425462>

J. Estrada, Acromax Media — Albanian Government’s Tool for Online Political Censorship, 19 August 2019, available at:

<https://exit.al/en/2019/08/19/acromax-media-albanian-governments-tool-for-online-political-censorship/>

K. Kosta, A. Topi and K. Keruti, Partners Albania for Change and Development, Monitoring the right to freedom of Assembly, Country Report - Albania 2016-2017, December 2017, available at:

<https://partnersalbania.org/publication/monitoring-right-to-free-assembly-albania-country-report-2016-2017/>

Kossev, Hacked websites of Media Center and program ‘Free Serbian’, 22 January 2019, available at: <https://kossev.info/hakovani-sajtove-medija-centra-i-emisije-slobodno-srpski-iz-caglavice/>,

Kossev a victim of a strong hacking attack, 29 September 2017, available at:

<https://www.facebook.com/notes/kosovo-sever-portal/kossev-pod-jakim-hakerskim-napadom/1129319363879628/>
Law on Communications (Official Gazette of BiH, No. 31/03) of Bosnia Herzegovina entered into force in 2002, available at:

<http://www.ohr.int/ohr-dept/legal/laws-of-bih/pdf/011%20-%20PUBLIC%20INFORMATION/RTV-Communications/BH/HR%20DECISION%20ENACTING%20THE%20LAW%20ON%20COMMUNICATIONS%20OF%20BH%2052-02.pdf>

Law on Electronic Communication , (Official Gazette of the Republic of Kosovo, No. 30/09), available at:

<https://gzk.rks-gov.net/ActDocumentDetail.aspx?ActID=2851>

Law on Electronic Communications in the Republic of Albania, (Official Gazette of the Republic of Albania, No. 9918/2008, of 19.05.2008.), available at:

<http://www.informatica-juridica.com/anexos/legislacion-albania-law-no-9918-2008-of-19-05-2008-electronic-communications-in-the-republic-of-albania/>

Law on Electronic Communications, (Official Gazette of the Republic of Serbia, No.44/10), available at:

<https://www.ratel.rs/upload/documents/Zakon/Electronic%20Communications%20Law.pdf>

Law on Information Security, (Official Gazette of the Republic of Albania, No.2/2017), available at:

https://cesk.gov.al/wp-content/uploads/2016/04/Ligji%20_Per_Sigurine_Kibernetike_Nr_2_Date_26.1.2017.pdf

Law on Interception of Communications, (Official Gazette of the Republic of Kosovo, No. 18/2015), available at:

<https://gzk.rks-gov.net/ActDetail.aspx?ActID=10968>

Law on Personal Data Protection, (Official Gazette of the Republic of Serbia, No.87/18), available at :

<http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2018/87/13/reg>

Law on Prevention and Fight of the Cybercrime, (Official Gazette of the Republic of Kosovo, No.03/L-166), available at:

https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/kosov-2/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print&_101_INSTANCE_hFPA5fbKjyCJ_languageId=pt_PT

Law on Public Gatherings, (Official Gazette of the Republic of Serbia, No. 6/2016), available at:

https://www.paragraf.rs/propisi/zakon_o_javnom_okupljanju.html

Law on Public Information and Media (Official Gazette of the Republic of Serbia, No. No 83/2014, 58/2015 and 12/2016), available at:

<http://kultura.gov.rs/en/dokumenti/media-regulations/law-on-public-information-and-media>

Law on the Intelligence and Security Agency of BiH, (Official Gazette of BiH, No. 12/04 and 20/04), available at:

<https://www.legislationline.org/documents/id/6331>

Law on the Protection of Journalists’ Sources, (Official Gazette of the Republic of Kosovo, No.20/2013), available at:

<https://gzk.rks-gov.net/ActDetail.aspx?ActID=8864>

Law on the Protection of Personal Data, (Official Gazette of BiH, No. 32/01), available at:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806af037>

Law on the Protection of Personal Data, (Official Gazette of the Republic of Kosovo, Law No.03/L – 172), available at:

<https://www.afapdp.org/wp-content/uploads/2012/01/Law-on-Personal-Data-Protection-Kosovo.pdf>

Law on the Ratification of the Convention on Cybercrime, (Official Gazette of the Republic of Serbia, No.19/09), available at:

http://www.podaci.net/_z1/2129877/Z-pkvkri03v0919.html

Law on the Ratification of the European Convention on Human Rights and Fundamental Freedoms, (Official Gazette of Serbia and Montenegro, No. 9/2003, 5/2005, 7/2005 - corr. and Official Gazette of the Republic of Serbia, No. 12/2010 and 10/2015), available at:

<http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/mu/skupstina/zakon/2003/9/4/reg>

M. Zirojevic, After the reports of Mediana PR, the police asks journalist of ‘Juzne vesti’ to reveal the source, 20 December 2018, available at:

<https://www.juznevesti.com/Drushtvo/Po-prijavi-PR-a-Medijane-policija-trazila-od-novinara-Juznih-vesti-da-otkrije-izvor.sr.html>

N1BiH, Desir and Breton condemn threats to journalists in BiH, 15 February 2019, available at:

<http://ba.n1info.com/Vijesti/a316338/D%C3%A9sir-i-Berton-osudili-prijetnje-upucene-novinarima-u-Bosni-i-Hercegovini.html>

Oculus News, Albania the cheapest internet price in the region, May 2019, available at:
<https://www.ocnal.com/2019/03/albania-cheapest-internet-price-in.html>

Office of Information and Data Protection Commissioner, Annual report 2018, available at:
https://www.idp.al/wp-content/uploads/2019/03/ENGLISH_Annual_Report_2018_KDIMDP.pdf

OSCE, Spreading Critical Media Literacy among Kosovo youth, 5 April 2018, available at:
<https://www.osce.org/mission-in-kosovo/376975>

R. Adilagic, Indicators of levels of media freedom and journalists' safety in BiH, 2016, available at:
<http://safejournalists.net/wp-content/uploads/2016/12/Full-BiH-BiH-Digital.pdf>

Reporters without Borders, Albania: Preliminary findings of joint freedom of expression mission, 21 June 2019, available at: <https://rsf.org/en/news/albania-preliminary-findings-joint-freedom-expression-mission>

Reporters without Borders, Albanian journalists repeatedly threatened, attacked , 4 September 2018, available at:
<https://rsf.org/en/news/albanian-journalists-repeatedly-threatened-attacked>

Reporters without Borders, Serbia, available at: <https://rsf.org/en/serbia>

RTVFBiH, Protests of Journalists in BiH, ordered to return property of Kljix, 7 January 2015, available at:
<http://www.federalna.ba/bhs/vijest/117284/Vijesti%20u%2022>

S. Hodžić, BiH in Media Integrity Matters: Reclaiming public service values in media and journalism, Peace Institute, Institute for Contemporary Social and Political Studies, 2014.

S. Kursani, Kosovar Centre for Security Studies, Lawful Interception of Telecommunications in Kosovo: Security Implications, available at:
http://www.qkss.org/repository/docs/Lawful_Interception_of_Telecommunications_in_Kosovo-Security_Implications_333536.pdf

SHARE CERT, The first Law on Critical Infrastructure adopted without public debate, 30 October 2018, Belgrade, available at:
<https://www.sharecert.rs/2018/10/30/prvi-zakon-o-kriticnoj-infrastrukturi-se-uvaja-bez-javne-rasprave/>

SHARE Foundation Monitoring Database, available at: <http://monitoring.labs.rs/>

SHARE Foundation, Access without transparency-practice of data retention in 2018, 29 October 2019, available at:
<https://www.sharefoundation.info/sr/pristup-bez-transparentosti-praksa-zadrzavanja-podataka-u-2018/>

SHARE Foundation, Digital rights monitoring reports available at:
<https://resursi.sharefoundation.info/sr/monitoring-digitalnih-prava-i-sloboda/>

SHARE Foundation, Retaining data on communications: to what extent are we under surveillance?, 26 December 2018, available at:
<https://resursi.sharefoundation.info/sr/resource/zadrzavanje-podataka-o-komunikaciji-u-srbiji-koliko-smo-pod-nadzorom/>

Strategy for the Fight against Cyber Crime for the period 2019-2023, Pursuant to the Law on Government (Official Gazette of the Republic of Serbia, No. 55/05, 71/05 – corr., 101/07, 65/08, 16/11, 68/12 – US, 72/12, 7/14 – US, 44/14 and 30/18 – state law).
<http://otvorenavlada.rs/strategija-za-borbu-protiv-visokotehnoloskog-kriminala-za-period2019-2023-godine/>

T. Jusić, and N. Ahmetašević, Media Reforms through Intervention: International Media Assistance in Bosnia and Herzegovina, Analitika, 2013.

The National Agency for the Protection of Personal Data website:
<http://www.amdp-rks.org/?page=2,10,167#.XcAKR-hKjIU>

The World Bank, Villages in Kosovo Start Enjoying High-Speed Internet With World Bank Support, 26 November 2018, available at:
<https://www.worldbank.org/en/news/feature/2018/11/26/kosovo-villages-start-enjoying-high-speed-Internet-with-world-bank-support>

V. Karaj, Last TV Shows Critical of Albanian Government are Cancelled , BIRN, 29 August 2019, available at:
<https://balkaninsight.com/2019/08/29/last-tv-shows-critical-of-the-government-are-closed-down-in-albania/?fbclid=IwAR3kQzFuT1tCPPRSTyReOzPfaLcbid3Q2vMs0X7jT0vgKUBpr6vuG3tMIMM>

Vodafone, Law Enforcement Disclosure Report Legal Annex June 2014, available at:
https://www.vodafone.com/content/dam/vodcom/sustainability/pdfs/vodafone_law_enforcement_disclosure_report.pdf

Z.Strika, New portal gave up reporting on political topics due to pressures and insults, Independent Journalists Association of Serbia, 28 February 2019, available at:
<http://nuns.rs/info/news/41406/portal-odustao-od-politickih-tema-zbog-pritisaka-i-uvreda.html>

A complex network diagram with numerous nodes and connecting lines, rendered in a light gray color, serves as the background for the entire page. The nodes are represented by small circles, and the lines represent connections between them, creating a web-like structure.

INTERNET FREEDOMS REPORT