DCAF Geneva Centre for Security Sector Governance

Cybersecurity and Human Rights in the Western Balkans:

MAPPING GOVERNANCE AND ACTORS

By the Western Balkans Cybersecurity Research Network

An initiative of DCAF – Geneva Centre for Security Sector Governance, in the context of the project, 'Good Governance in Cybersecurity in the Western Balkans', supported by the UK's Foreign, Commonwealth and Development Office (FCDO)

September 2022

INTRODUCTION

FRAMING AN ANALYSIS OF HUMAN RIGHTS AND CYBERSECURITY

By Laylo Merali and Ena Bavčić | DCAF

INTRODUCTION

FRAMING AN ANALYSIS OF HUMAN RIGHTS AND CYBERSECURITY

Just like the business adage, 'you can't manage what you can't measure', it is also true that 'you can't change what you don't map' – an important reality relevant to the nexus between cybersecurity and human rights in the Western Balkans.

Definitions of cybersecurity usually emphasize the protection of state and other institutions' assets and digital environment[1]. However, these definitions neglect many security challenges that individuals face online. This publication examines national cybersecurity policies in the economies of the Western Balkans through a human-centric approach and evaluates levels of cybersecurity in terms of human rights protections. Put another way, cybersecurity merits a more human-centred analytical approach that highlights not only issues affecting state actors, but also issues that the actors cause for people.

This human-centric approach to cybersecurity follows from the broader theory of good security sector governance (SSG).[2] Good SSG focuses on protecting not only the state's networks, systems and stability but also the rights of individuals within democratic society. It incorporates principles such as accountability, participation, inclusiveness, effectiveness, efficiency, and transparency. This leads to better provision of security and allows for its democratic oversight, which in turn prevents abuse of power by security providers. 'Cybersecurity' can thus be defined as security of the people and their human rights online, and of the networks and services that are essential for this objective, which together protect the democratic order and the rule of law.

A considerable body of research already exists on the links between cybersecurity and human rights.[3] For decades, activists, academics, and representatives of governments and the private sector have been working to define what we mean by 'human rights online', 'human rights on the Internet', and 'cybersecurity and human rights'.[4] Country assessments looking at cybersecurity also regularly assess how governments have incorporated existing human rights standards in the online sphere.[5]

In this publication, authors from a variety of backgrounds consider the extent to which human rights are currently being realized in the six Western Balkan economies: **Albania**, **Bosnia and Herzegovina**,

1 International Telecommunications Union (ITU) *Definition of Cybersecurity.*

2 DCAF, *Guide to Good Governance in Cybersecurity* (Geneva: Geneva Centre for Security Sector Governance (DCAF); 2021)

3 Global Partners Digital (GPD) publications on *CybilPortal*.

4 Microsoft's initiative on *technology and human rights*.

5 Freedom House's *Freedom on the Net*.

Kosovo,* **Montenegro**, **North Macedonia**, **and Serbia**. Where challenges to certain rights are evident, they ask why this is the case and examine how principles of good governance are being met. In particular, they look at laws and practice and the capacities of (cyber)security actors and oversight actors. Why do violations keep happening, including at a systemic level, if we have international standards on how human rights should be applied at the national level? Are the standards not clear enough or not sufficiently detailed to enable them to be applied to different national contexts? Or rather, are these standards not being understood? How is it possible that a country can have transposed standards into law but they have not been implemented?

As one of the flagship initiatives of the DCAF project Good Governance in Cybersecurity in the Western Balkans, which is supported by the Foreign, Commonwealth and Development Office of the UK, the Western Balkans Cybersecurity Research Network has embarked on an important mission to produce illuminating, groundbreaking research, which begins with this collection of papers. This publication focuses on **mapping cybersecurity-related human rights opportunities and challenges**, and represents an area that is under-explored in the region.

There are six chapters in total, one for each economy in the Western Balkans. Each begins with essential conceptual background information regarding the cybersecurity and human rights contexts of each economy. They then each explore four core thematic issues: **cybersecurity and the right to privacy, cybersecurity and freedom of expression, cybersecurity and freedom of peaceful assembly (and, where relevant, freedom of association), and cybersecurity and anti-discrimination**. Finally, they present ways forward, with concrete recommendations for stakeholders.

What are the specific priority issues that these papers set out to explore? There are many, but some examples are outlined here.

- **On Albania, Megi Reçi and Sara Kelmendi of the Institute for Democracy and Mediation (IDM)** look at the country's generally strong legal framework in terms of cybersecurity measures (which is aimed at harmonization with EU regulation), as well as its weaknesses in cooperation on cybersecurity and on capacity development. The chapter highlights the country's various items of human rights-related legislation but also notes that the cybersecurity dimension of these rights is sometimes not developed as explicitly as is needed. Some of its recommendations are targeted at public actors, for example regarding amendments needed to regulations or specific measures relating to data protection, while others are aimed at non-public actors, for example the role that civil society plays in monitoring violations and creating awareness.
- **On Bosnia and Herzegovina, Aida Mahmutović and Aida Trepanić of the Balkan Investigative Reporting Network (BIRN BiH)** describe the multiple barriers posed by the complexity of the country's judicial system, making it difficult for people to realize human rights related to cybersecurity and leading to an erosion of trust. They highlight the need for policy leaders to widen their understanding in order to better consider the human rights implications of cybersecurity-related issues, the need for institutions to collaborate more effectively, both domestically and internationally (particularly governmental institutions but also civil society), and the need for further training for actors in the judicial system. The chapter also discusses the space needed for dialogue to facilitate collaboration among stakeholders.

* This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo declaration of independence.

- **On Kosovo, Lulzim Peci and Valdrin Ukshini of Kosovar Institute for Policy and Research (KIPRED)** articulate the evolution of the state's legal and policy frameworks since its declaration of independence in 2008, even though the legal framework remains incomplete and policy guidance lacks specificity. They describe how Kosovo requires much greater development in terms of its cybersecurity capacity generally and its relation to human rights, and report that the main victims of cybercrime are women, the LGBTQI+ community, the minority Roma people, and other vulnerable groups. Recommendations are presented for Kosovo's continued institutional development in order to strengthen human rights in the realm of cybersecurity.
- **On Montenegro, Milica Kovačević and Tijana Velimirovic of the Centre for Democratic Transition (CDT)** highlight the need for greater awareness about the human rights dimensions of cybersecurity, which can potentially provide a foundation for the development of human rights norms. Additionally, they note the need for more thorough expert review of laws and regulations on cybersecurity that impact human rights, and for comparison of these with good practices elsewhere. The chapter also examines the connection between defending against hybrid cyber threats and ensuring that such actions at the same time protect human rights, including in judicial, media, electoral, and other contexts that have cyber dimensions. The financial resourcing implications are also examined.
- **On North Macedonia, Bardhyl Jashari, Goce Arsovski, and Elida Zylbeari of Metamorphosis Foundation** outline the country's purposeful steps towards improving cybersecurity, including legal and policy aspects in alignment with EU standards, but also describe weaknesses in their implementation. Recommendations are presented to ensure stronger inclusion of human rights in laws on cybersecurity, alongside training initiatives and improved awareness and engagement by civil society, media, and other non-governmental stakeholders.
- **Serbia Maja Bjeloš and Marija Pavlović of the Belgrade Centre for Security Policy (BCSP)** outlines the country's relatively strong legal framework in relation to cybersecurity, but notes the challenges associated with a lack of qualified personnel and a lack of training, which means that it is falling behind advances in technology and is having to deal with competing priorities. The chapter notes that there are limited mentions of women, LGBTQI people, human rights defenders, and journalists in documents relating to cybersecurity, in a context of insufficient understanding about inclusive processes. It also describes how violations of citizens' digital rights are frequently tolerated in relation to cybersecurity, which can affect human rights protections.

Thematically, four main cross-cutting issues are analysed.

- **Cybersecurity and the right to privacy:** This is one of the concerns most frequently raised in relation to human rights in the cybersecurity domain. The authors explore whether there have been data breaches caused by state and/or non-state actors in the economy in question, how cybersecurity hygiene can contribute to increased rights to privacy, and what the general level of resilience is to such breaches.

- **Cybersecurity and freedom of expression:** More precisely, civil societies in the region have experienced issues with online censorship, defamation, and disinformation, leading to cyber violence. The authors explore the responses of state institutions to such breaches, as well as potential involvement in these responses by the private sector, academia, international organizations, and local CSOs.
- **Cybersecurity and freedom of peaceful assembly and association:** The authors explore the extent to which issues such as video surveillance and facial recognition technologies, Internet/mobile network shutdowns, cyber threats and violence against activists, and issues with online assemblies have occurred in the Western Balkans. Where such issues have been reported, they explore further whether they have been related to certain types of assembly, what actors have been involved, and what responses have been recorded.
- **Cybersecurity and anti-discrimination:** The authors explore whether cybersecurity breaches have targeted specific groups and whether responses differ for groups that are under-represented. The research aims to explore how much access groups that are discriminated against have to cybersecurity protections in general.

Overall, the chapters in this publication are intended to help improve understanding of what cybersecurity capacities are in relation to specific rights – the rights to privacy, freedom of expression, freedom of assembly and association, and anti-discrimination – in different economies of the Western Balkans. The study as a whole aims to offer recommendations for the inclusion of human rights standards in cybersecurity governance and for better implementation of cybersecurity norms within the human rights frameworks of the Western Balkans region.

CHAPTER 1

ALBANIA
Bridging the Gap Between Cyber Policy Fragmentation and Human Rights

By Megi Reçi and Sara Kelmendi | Institute for Democracy and Mediation (IDM)

CHAPTER 1

ALBANIA – BRIDGING THE GAP BETWEEN CYBER POLICY FRAGMENTATION AND HUMAN RIGHTS

GENERAL CYBERSECURITY CONTEXT IN ALBANIA

Legal framework on cybersecurity

Cybersecurity governance will need to develop a human rights approach, to mitigate the human rights risks accompanied by digitalization

The Global Cybersecurity Index 2020 ranked Albania 80th out of 132 countries at the global level and 40th out of 46 countries at the European level, based on an evaluation of cybersecurity measures taken by the country. According to this Index, Albania performs best regarding legal measures which are considered an area of relative strength, while the lowest points scored concerned cooperative measures and capacity development.[6] The legal framework on cybersecurity was largely developed in the context of harmonization of national legislation with European Union (EU) directives and adherence to Council of Europe (CoE) conventions. The ratification of the Convention on Cybercrime and its Additional Protocol have influenced the alignment of the national criminal legislation with the standards it establishes regarding cybercrimes and electronic evidence. In 2022, Albania signed the Protocol amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Being a recently adopted document, its impact on the Albanian legal system remains to be assessed in the upcoming years. According to the European Commission, the country is moderately prepared in the field of information society and needs to further improve the legal and policy framework, align the legislation on cybersecurity and electronic communications with EU legislation, and improve the collection of statistical data on digital performance and competitiveness.[7]

6 International Telecommunication Union, *Global Cybersecurity Index 2020* (ITU; 2021).

7 European Commission, *Albania 2021 Report* (Strasbourg: Directorate-General for Neighbourhood and Enlargement Negotiations; 2021).

The main legislative acts that form the national legal framework on cybersecurity are analysed below.

Law No. 7895/1995 **Criminal Code of Albania** ('the Code') prescribes criminal acts in the area of information and communications technology (ICT) and is overall in line with the above-mentioned CoE conventions. The Code protects the right to private life through various previsions, including by criminalizing intrusion into someone's privacy, spreading of personal secrets, and violation of private correspondence. With regard to threats, insults, and electronic dissemination of discriminatory content, the Code limits the motives to racism or xenophobia, but other potential motives are not addressed. With regard to inciting hatred or strife – race, ethnicity, religion, and sexual orientation are covered as motives, leaving out gender identity. The Code provides that such acts can take place using any means or form, therefore including electronic ones. Sexual harassment committed via any means or form is also addressed, whilst with regard to stalking, the Code fails to cover online cases. Nevertheless, discrimination is considered an aggravating circumstance for any criminal offence. Lastly, defamation, and spreading of false information that arouses panic, are criminally punishable and have been applied to articles, social media statuses, or opinions published online. The rules of procedure for investigating and prosecuting crimes and offences established by the Code are established by Law no. 7905/1995 **Code of Criminal Procedure**. Further, Law No. 2/2017 on **Cybersecurity** ensures security in cyberspace and applies to communication networks and information systems, the infringement or the destruction of which would have an impact on the health, security, economic well-being of citizens, and the effective functioning of the economy in Albania. On the other hand, a separate law, No. 9918/2008 on **Electronic Communications** ensures the secrecy of electronic communications and the protection of personal data, while interception of communications is allowed only when legally required (for example, in the framework of a criminal investigation). The law prescribes remedies for violations and ensures equal access to electronic communications and services, without discrimination, with an emphasis on the accommodation of the needs of persons with disabilities. Law No. 18/2017 on the **Rights and Protection of the Child** addresses various forms of violence against children, such as bullying, sexual abuse, trafficking, and so forth, as well as children's safety on the internet. Furthermore, Decision No. 465/2019 of the Council of Ministers establishes concrete measures for the protection of children from access to illegal and/or harmful content on the internet, establishing obligations for various actors. Lastly, other laws that impact the sector include: Law No. 9880/2008 on **Electronic Signature** which establishes the rules for the recognition and use of electronic signatures; Law No. 107/2015 **Electronic Identification and Trust Services** which defines the rules for electronic identification of safe, electronic seals, services using electronic transmission, and website authentication; and Law No. 10128/2009 on **Electronic Commerce** which sets out the rules for e-commerce activity, the privacy of consumers, and penalties for breaches, and is applicable to online media that offer subscription services to generate revenue.

Policy framework on cybersecurity

In various strategic cybersecurity policy documents, the Albanian government focuses on building infrastructure and the capacities of public institutions, improving public services and e-governance, as well as regulating the market for online services and online economic activities. The cybersecurity sector looks at systems and infrastructure as assets to be protected, regulated, and maintained, but does not apply the human security lens to ask what the security threats for individuals are. As a result, cyberspace in Albania is widely treated as a market and a space for services. Citizens are seen strictly as customers and risk assessments and mitigation measures on the threats posed to their human rights, are lacking. The only exception to this norm seems to have been made regarding children's protection on the internet for which, as indicated above, a certain level of regulation and policy attention is provided. The policy emphasis duly put on the protection of children from online abuse and the need to increase their internet safety,

Cybersecurity governance will need to develop a human rights approach, to mitigate the human rights risks accompanied by digitalization

should be extended to other pressing human rights issues affecting different targeted groups and the public at large. Eventually, cybersecurity governance will need to develop a human rights approach, to mitigate the human rights risks accompanied by digitalization.

The main strategic documents on cybersecurity are analysed below through the human rights lens.

The **National Cybersecurity Strategy and its Action Plan 2020-2025** cover different areas for intervention including cybercrime, radicalism, violent extremism, and protection of children on the internet. Except for the focus on the protection of children, the strategy does not intersect with any other human rights issues, and the protection of other groups at risk in cyberspace such as women, or ethnic, racial, and sexual minorities, fails to be addressed. When this strategy was drafted, civil society organizations working on children's rights participated in the consultation, nevertheless none of the independent institutions[8] dealing with human rights were consulted.[9] On the other hand, the **National Strategy for Cyber Protection 2021-2023** is strictly focused on matters of national defence, therefore no direct correlation to human rights issues is made. Further, the **Intersectoral Strategy 'The Digital Agenda of Albania' 2015-2020** covered digitalization of economic, social, institutional, and administrative processes. This strategy was more service-oriented than citizen-oriented and no direct correlation to human rights issues was made in any of its objectives. It is worth noting that consultations on the new Digital Agenda and Action Plan 2022-2026 reportedly took place during October-November 2021 while independent institutions dealing with human rights were not involved, and the report on the results of the public consultation is very vague regarding the stakeholders that were consulted.[10] The only strategic document on cybersecurity issues in the country with a human rights approach was the **Action Plan for a Safer Internet for Children in Albania 2018-2020** and it can serve as a good example for the sector.

Institutional framework on cybersecurity

There is currently no institution within the government of Albania with centralized and policymaking competencies regarding matters of cybersecurity, ICT, electronic communications, or media. The last government body of this nature was the Ministry for Innovation and Public,[11] which was dissolved in 2017, due to a government restructuring. Currently, the main stakeholders for cybersecurity governance are technical agencies rather than policymakers. They consist of central government institutions (prime minister's office and ministries) and their subordinate agencies, as well as independent institutions. Further, the government plans to create a National Centre of Cybersecurity Operations as well as a Centre of Excellence for Cybersecurity[12] and it remains to be seen how these institutions will affect cybersecurity governance and policymaking. In this process, the government will receive assistance

8 Commissioner for Protection from Discrimination; Information and Data Protection Commissioner; Ombudsperson.

9 Information provided by AKCESK via a freedom of information request, 28 April 2022.

10 Information provided by AKSHI via a freedom of information request, 10 May 2022.

11 Decision of the Council of Ministers no. 943/2013.

12 Decision of the Council of Ministers no.1/2022.

The diverse nature of all actors involved in cybersecurity matters can create challenges in coordination and blur the traditional boundaries between accountability and oversight

from Jones Group International, a US-based company, the contract with which was being negotiated at the time of writing of this analysis. It is worth noting that the Commission created for the negotiation of this contract does not include any of the independent institutions dealing with human rights.[13] The diverse nature of all actors involved in cybersecurity matters can create challenges in coordination and blur the traditional boundaries between accountability and oversight. Therefore, coordination of efforts is needed and the risk of leaving a number of areas with inadequate or no oversight must be mitigated when creating or restructuring institutions.

The role of the country's key cybersecurity actors is described below.

The **National Authority for Electronic Certification and Cybersecurity (AKCESK)**, a subordinate agency of the prime minister's (PM) office, is responsible for setting national cybersecurity measures and overseeing the enforcement of laws on electronic signatures, electronic identification, trust services, and cybersecurity. AKCESK serves as the main contact point in cases of attacks and incidents related to cybersecurity and is the key institution responsible for the implementation of the National Cybersecurity Strategy and its Action Plan. Furthermore, there are two dedicated units responsible for **cybercrime investigation** within the Tirana Police Directorate and the General Directorate of Police, under the subordinance of the **Ministry of Interior**. Local police directorates do not have such units or dedicated officers; therefore, these two Tirana-based units cover cybercrime reports at a national level.[14] To enable citizens to report cybercrime, the police have also created a dedicated section on the website; however, it is currently out of service.[15] In addition, the **Prosecutor's Cybercrime Investigation Unit** carries out criminal prosecution against cybercrimes. Another crucial actor in the ICT sector is the **National Agency for Information Society (AKSHI)**, a subordinate agency of the PM's office. This agency is responsible for the state databases and for administering and maintaining e-governance services provided through e-Albania, a one-stop shop for online public administration services.[16] AKSHI is also responsible for administering the ICT systems of public institutions and is the key institution with regards the drafting and implementation of the Digital Agenda Strategy. Further, the **Electronic and Postal Communications Authority (AKEP)** is an independent regulatory body that oversees electronic communications and postal services and has the authority to issue administrative sanctions in cases of violation. AKEP can request internet service providers (ISPs) to remove illegal content based on the decisions of the competent authorities, however, there is no unified definition of what is considered illegal and/or harmful content, or of the competent authorities that can request such a removal.[17] The law on electronic communications alone is not sufficient to address this, and references to other laws need to be made. Regarding the protection of children from harmful or illegal content on the internet, the **State Agency for the Protection of Children's Rights** is the responsible government agency. It oversees the application of protection and/or preventive measures employed by ISPs, educational institutions, and any other public or private

13 Law 34/2022 for the assignment of the special procedure for the negotiation and implementation of the contract with Jones Group International for the strengthening of cybersecurity.

14 Authors' interview with a representative of the C-Unit of the General Directorate of the State Police, Tirana, Albania, 26 May 2022.

15 Albanian State Police (ASP), *State Police website, Online reporting form*.

16 AKSHI, *About e-Albania*.

17 BIRN, *Internet Governance in Albania and its role in media freedom* (Tirana: Balkan Investigative Reporting Network in Albania; 2020).

institutions. Lastly, the **Ministry of Defence (MoD)** is responsible for handling cyber incidents related to the MoD and Air Force and oversees the implementation of the National Strategy for Cyber Protection.

CYBERSECURITY AND HUMAN RIGHTS FRAMEWORK[18]

Overall, Albania complies with international human rights instruments and has ratified most international conventions related to the protection of fundamental rights.[19] According to the Constitution of Albania, human rights restrictions cannot exceed the limitations provided by the European Convention on Human Rights (ECHR), granting this convention a special status within the national legal system. The ECHR ensures the protection of fundamental rights and freedoms including those analysed in this report: the right to private and family life, freedom of expression, prohibition of discrimination, and freedom of assembly and association. It is now widely accepted that international law applies in cyberspace as well;[20] therefore, the standards established by the ECHR, as well as the case-law of the European Court of Human Rights (ECtHR), apply to cases where rights violations intersect with cybersecurity, either by taking place in cyberspace or being enabled by it.

The right to privacy entails the protection of personal data and the obligation to provide them only under strict circumstances/criteria, as envisioned by the law (for example, in the framework of a criminal investigation). Consent is required when collecting, using, and publishing data, while everyone has the right to know what data is collected about them and has the right to request their correction or deletion if the data are untrue, incomplete, or collected in violation of the law. Law No. 9887/2008 on Protection of Personal Data provides the criteria for lawful data processing, restrictions, and limitations as well as the available remedies for when violations occur. This law is currently undergoing a process of harmonization with the General Data Protection Regulation.[21] The Information and Data Protection Commissioner (IDP Commissioner) is an independent institution responsible for conducting administrative investigations, and issuing recommendations and administrative sanctions against private or public actors for violations of this law.

Freedom of expression, freedom of the press, the right to information, and prohibition of censure are guaranteed. There is no specific law on online media in Albania and a legal definition of online media is also lacking. The last attempt to regulate online media was made in 2019 through the controversial 'anti-defamation' legal package.[22] The draft laws of this package were widely contested by local and international media freedom organizations over concerns of censorship, while the Venice Commission recommended its revision.[23] On the other hand, the audiovisual media environment is regulated by Law No. 97/2013 on Audiovisual Media, which obliges media to respect human dignity and fundamental human rights while broadcasting. The law prohibits the broadcasting of materials that justify or incite violence, hatred, intolerance, and criminal offences. The Audiovisual Media Authority (AMA), an independent regulatory body that oversees audiovisual media, is responsible for licensing, fighting piracy

18 To map the individual cases analysed under sections 2.1-2.4, 15 experts were interviewed and 19 activists and journalists provided information via an anonymous survey.

19 European Commission, *Albania 2021 Report* (Strasbourg: Directorate-General for Neighbourhood and Enlargement Negotiations; 2021).

20 DCAF, *Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cybersecurity Governance Approach* (Geneva: Geneva Centre for Security Sector Governance (DCAF); 2021).

21 IDP Commissioner, *Public consultation on the protection of personal data and law amendments for the right to information*, 16 December 2021.

22 Ndrevataj, Entenela, *"Anti-defamation" laws swim against democracy*, Kosovo 2.0, 9 April 2020.

23 Venice Commission, *Opinion No. 980 / 2020*, European Commission for Democracy through Law (Venice Commission), 19 June 2020.

of copyrighted content, reviewing complaints, and issuing administrative sanctions in cases of violations. AMA's mandate does not cover online media, and holding the latter accountable for violations often becomes a challenge. Despite the mandate limitations, AMA can influence online media, for example in 2019, when AMA required that AKEP block content that was available online in 86 cases, all of which related to copyright infringement.[24] Lastly, the Criminal Code, Law on Protection of Personal Data, Law on Protection from Discrimination, Law on Copyright and Related Rights impact the media sector through the restrictions they establish whilst legal provisions that ensure protection from SLAPPs[25] are currently lacking.

The principle of equality and prohibition of discrimination is guaranteed, while Law No. 10221/2010 on Protection from Discrimination provides a broad (and open) list of grounds including race, gender, sexual orientation, and gender identity among others. Furthermore, it defines forms of discrimination, including hate speech, harassment, sexual harassment, intersectional discrimination, and so forth. The law applies to violations which occur in any environment and by any means, therefore being applicable to cyberspace as well, without explicitly mentioning it. Nevertheless, it fails to address concepts related to algorithmic bias, which account for discriminatory automatic decision-making. Other laws addressing discrimination such as Law No. 9970/2008 on Gender Equality in Society and Law No. 96/2017 on Protection of National Minorities do not have any provisions on violations that take place in cyberspace. The only provision within the Law on Gender Equality in Society that can correlate with cyberspace is the prohibition to publish discriminatory, offensive, or gender stereotyping content. Nevertheless, this is strictly applicable to the media and not to other actors. The Commissioner for Protection from Discrimination (CPD) is the independent institution that has the authority to conduct administrative investigations, and issue recommendations and administrative sanctions against private or public actors in cases of discrimination. When discriminatory actions contain elements of a crime or offence, the Criminal Code is applied, as analysed in the previous section.

Freedom of peaceful and unarmed assembly is regulated by Law No. 8773/2001 on Assemblies, which is largely in line with the Guidelines on Freedom of Peaceful Assembly of the OSCE Office for Democratic Institutions and Human Rights (ODIHR) (2010). Nevertheless, the law does not elaborate on the right to assemblies online, spontaneous assemblies, or counter-assemblies. Furthermore, this law allows the police to monitor assemblies (using audio/video recording or photography) when there is reason to believe that there might be an immediate risk posed to public order and security. Such a possibility, if not duly balanced, can be misused at the cost of criminally prosecuting or intimidating human rights defenders (HRDs), assembly organizers, and participants both in the context of physical and online assemblies. The ombudsperson and the state police are among the main actors when it comes to the upholding of freedom of assembly. Despite not having a particular mandate to deal with human rights violations in cyberspace, the role of the ombudsperson could be of interest, inter alia, in the light of dealing with violations coming from public authorities in the cybersecurity sector, that fall under the mandate of the ombudsperson. Such possibilities are yet to be explored since to date, the ombudsperson has not received any complaints[26] about rights violations correlating to cyberspace.

---

24 BIRN, *Internet Governance in Albania and its role in media freedom* (Tirana: Balkan Investigative Reporting Network in Albania; 2020).

25 Strategic lawsuits against public participation (SLAPPs) are lawsuits used by politicians, wealthy individuals, and corporations to intimidate and silence public critics by forcing them into legal battles they cannot afford until they cease their criticism or opposition. Anti-SLAPP laws are designed to allow individuals to have the lawsuit against them dismissed at a very early stage if that lawsuit qualifies as a SLAPP.

26 Information provided by the Office of the Ombudsperson via a freedom of information request, 17 February 2022.

Several **strategic documents on human rights** have been developed to safeguard the rights of certain groups that are particularly threatened. Nevertheless, these documents lack a perspective that ensures protection to these groups from human rights violations in cyberspace, just like the cybersecurity strategies analysed in the previous section lack a human rights approach. By way of illustration, some of these strategic documents on human rights are analysed below.

The National Strategy for Gender Equality 2021-2030 aims to increase protection from all forms of gender-based violence, however, it makes no direct reference to online gender-based violence. On the other hand, the National Action Plan for LGBTI+ people 2021-2027 recognizes online hate speech and discriminatory language against the LGBTI+ community as one of the challenges faced by the community, but does not address it with any concrete measures. Furthermore, the National Action Plan for Equality, Inclusion, and Participation of Roma and Egyptians in Albania (2021-2025), which represents Albania's first political engagement in tackling antigypsyism,[27] includes the elimination of hate speech and hate crimes against these minorities as one of its specific objectives. This Action Plan recognizes several challenges regarding hate speech and hate crimes (including when they happen online), among which are weak institutional mechanisms, the under-reporting of cases due to a lack of trust in institutions, and the lack of statistical and disaggregated data regarding hate speech and hate crimes. This document also prescribes financing civil society organizations (CSOs) from public funds to monitor and report hate speech cases and increasing the capacities of the relevant authorities in investigating and monitoring hate crimes and hate speech. Lastly, the National Action Plan for Persons with Disabilities (PWDs) 2021-2025 aims to ensure accessibility to ICT, electronic services, and online public services for PWDs. The Ministry of Health and Social Protection is the key institution responsible for the implementation of these four strategic documents.

A 2019 parliamentary resolution,[28] providing recognition and support to HRDs, is another important document as it recognizes the challenges faced by HRDs, including threats, smear campaigns, and attacks, without making references to violations taking place in cyberspace. According to the resolution, the parliament should draft a detailed report on the situation of HRDs in Albania with recommendations, as well as approve an action plan, but to date, such documents have not been approved.[29] The Parliamentary Committee on Legal Matters, Public Administration and Human Rights and its Subcommittee on Human Rights are responsible for this resolution, and overall play a key role in the development of the national human rights framework.

Cybersecurity and right to privacy

In 2021, **data breaches** topped the list of cybersecurity threats in Albania. Just a few weeks before parliamentary elections in April, the personal data of 910,000 Albanian citizens were leaked to the public.[30] The database, which was shared among citizens and online media, contained sensitive information about the voting-age population in Tirana, including individuals' identification numbers, current employment, addresses, phone numbers, and assumptions on voting preferences. The leak indicated that a 'patron'[31]

27 Racism against Roma and Egyptian minorities.

28 Resolution of the Parliament of Albania in support of Human Rights Defenders, 3 March 2019.

29 Information provided by the Parliament via a freedom of information request, 20 April 2022.

30 Taylor, Alice, *Exit Explains: The Leak of Over 910,000 Albanians Personal Data to Politicians and the Public*, Exit News, 16 April 2021.

31 'Patron' is used to refer to individuals assigned by the ruling party to track each individual voter and log their personal data in a national database.

was assigned to every citizen, aiming to monitor voting preferences and in several cases, indicating potential vulnerabilities of citizens that could influence their voting behaviour. Additional comments containing sensitive data related to the individual's health, family situation, religious views, or ethnicity were annotated in the database.

The institutional response to the data breach illustrates how the right to privacy is handled, whilst raising opportunities for tackling the fragmentation of cybersecurity governance. Following the data breach, accusations unfolded blaming the incumbent Socialist Party (SP) for the leak. Although the SP did not admit ownership of the leaked database, it admitted to having collected personal data over the years for electoral purposes on a door-to-door basis.[32] This was later also confirmed by the Information and Data Protection (IDP) Commissioner who assessed that some data had been supplied by the patrons. However, the IDP Commissioner[33] concluded that there was insufficient evidence that the database had been created by the SP or that it was illegally leaked from state databases.

In addition to data supplied by the patrons, the database contained up-to-date personal information that citizens provide and/or access themselves through e-Albania, an e-governance website that was frequently used during the COVID-19 national lockdown to request permissions for commuting. This led to most citizens associating the data breach with the National Agency for Information Society (AKSHI), responsible for administering the multifunctional portal. However, since the data breach scandal, AKSHI maintains that e-Albania neither stores, administers, nor processes any data,[34] but rather serves as a government gateway that enables users to interact with public institutions. Hence, data are stored and administered in the databases of relevant institutions – in this case, the General Directorate of the Civil Registry. Administrative investigations conducted by the IDP Commissioner on the premises of the SP, AKSHI, and the Civil Registry could not reach definitive conclusions on the matter, failing to ensure accountability. While the results of these investigations reveal severe data protection and security issues, the institution responsible for the data breach has not been indicated.

More specifically, administrative investigations targeting AKSHI and the Civil Registry office revealed that the IDP Commissioner deemed it possible for the data 'to have been harvested by relevant institutions or (sub)contracted authorities that manage and/or process these data, and the maintenance of critical infrastructure, due to a lack of security measures'.[35] In contrast to AKSHI's official position, in its report in the framework of the 2020 Resolution of the Parliament of Albania, the IDP Commissioner stated that AKSHI has an important role in data protection. The IDP Commissioner recommended AKSHI to include protocols in its data privacy framework, covering all data processing procedures.[36] When contacted for this report, AKSHI failed to respond on whether it had taken any measures to address the recommendations of the IDP Commissioner. The IDP Commissioner's 2020 report noted that although the existing measures on personally identifiable information (PII) cover some safeguarding principles, including security requirements and the rights of the individual owners of the data, the framework prevents individuals from understanding which categories of PII are stored and the purpose of their processing. For each type of sensitive PII, such as personal identification numbers, institutions must be required to identify the level of confidentiality and accessibility, before storing, processing, or transferring it. Generally, encryption and/or pseudonymization of personal data are recommended before transferring files to external sources or

32 Sinoruka, Fjori, *Massive Data Leaks in Albania Pose Public Security Question*, BalkanInsight, 13 December 2021.

33 Recommendation No. 44, 19 August 2021, of the Commissioner for the Right to Information and Data Protection.

34 Information provided by AKSHI via a freedom of information request, 10 May 2022.

35 Recommendation No. 43, 19 August 2021, of the Commissioner for the Right to Information and Data Protection. See also *Monitor.al*, 2021.

36 IDP Commissioner, *Report to Parliament for 2019*, 2020.

portable devices, such as laptops and mobile phones.[37] Currently, there is no available information on the modalities of data storage by AKSHI, nor is there any regulation that stipulates the specifics of PII when transferred to internet service providers or other third parties.

This is particularly relevant for the data breach since the IDP Commissioner's 2020 report reveals that AKSHI had assigned a private subject (processor) to handle the physical storage of data.[38] According to the report, the agreement failed to adequately address the regulations on data safeguarding, legal requirements, and dispositions compliant with the Law on Protection of Personal Data. Administering operators of key information infrastructure such as AKSHI and the General Directorate of the Civil Registry are subject to periodic audits conducted by the National Authority for Electronic Certification and Cybersecurity (AKCESK) to ensure the implementation of minimal security measures.[39] However, private processors are exempted from auditing and are not obliged to maintain the basic security measures established by AKCESK for important information infrastructure. While policy fragmentation is inevitable in cybersecurity governance, the lack of accountability of private subjects can be regulated by intersectoral compliance mechanisms. Arguably, intersectoral cooperation between representatives of the central government and independent institutions in this regard could improve data protection oversight and compliance of contracted private processors. It is crucial to ensure, from the drafting stage, that agreements with third parties entail a risk management approach as well. The private processor's capacities to meet minimal compliance standards must be evaluated considering the capacities of state institutions to monitor the implementation of effective risk management measures.

The controllers and processors are often exempt from liability in cases of data breaches if proven that the responsibility for the infringement is shared (or lies solely) with the individual owners of the data. In light of this issue, the data breach scandal could serve as a wake-up call for all citizens who choose to accept the terms and conditions of websites where they deliberately provide personal and sensitive data and consent to data management procedures, while being unaware of the risks.[40] Overall, the incident exposed the need for heightened digital literacy among citizens and increased awareness for quality e-services.

In December 2021, the media reported a new data dump: two separate databases were circulating among citizens and contained the personal information and salaries of 690,000 people, employees of the public and private sectors alike. The databases consisted of payroll data as declared in the National Tax Directorate system in January and April 2021, and were later proven to have been leaked by two internal employees of the Directorate, who were subsequently arrested.[41] Shortly after the payroll scandal, a third data leak exposed a detailed vehicle licensing database with 530,452 licence plates, vehicle models and colour, issued registration numbers, and ownership details. Administrative investigations are under way on both operators of critical information infrastructure linked to the data breaches – the National Tax Directorate and the General Directorate of Road Transportation Services.[42]

There have been no reported cybercrime incidents that have occurred as a consequence of the data breaches or in relation to them. However, these incidents illustrate the fragility of the cybersecurity and communications infrastructure in Albania, indicating severe confidentiality breaches and eroding public trust in state institutions. While the lack of accountability of state institutions following the first data breach scandal failed to generate constructive discussions on the topic of online security of personal data, the

37 United States Government Accountability Office, *Report to Congressional Requesters: Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information* (GAO; 2008).

38 IDP Commissioner, *Report to Parliament for 2019*, 2020.

39 Information provided by AKCESK via freedom of information request, 28 April 2022.

40 Authors' interview with civil society representative, 15 March 2022

41 Bogdani, Aleksandra, The unsafety of personal data threatens Albania*'s '*digital governance*'*, Reporter.al, 21 February 2022.

42 Authors' interview with a representative of the Commissioner for the Right to Information and Data Protection, 7 April 2022.

ensuing data leaks prompted the Albanian government to contract Jones Group International (JGI), a US-based company to strengthen the security of the digital systems. In January 2022, the Minister for Infrastructure and Energy signed a memorandum of understanding (MoU) assigning JGI to be in charge of designing a multi-dimensional strategy for raising awareness for data privacy, targeting both institutions that manage and process data, as well as citizens. According to Law No. 34/2022 on 'Determining the special procedure for the negotiation and implementation of the agreement with Jones Group International', AKSHI is the responsible institution for providing JGI with the mapping of cybersecurity institutions, their scope of work, and systems used. The draft agreement will be negotiated by a commission composed of representatives of the ministries of infrastructure and energy, defence, public order, finance and economy, the State Attorney General's Office, AKCESK, and the Classified Information Security Directorate. While the MoU with JGI has not been shared with the IDP Commissioner[43] – nor is the latter part of the negotiating committee for the draft agreement – AKSHI is shortly expected to receive written approval from all relevant agencies on the proposed projects, before finalizing the agreement.[44] The agreement presents an opportunity to conceptualize the cyber security framework in Albania following a 'stewardship approach'[45] – engaging public and non-public actors on an equal basis such as NGOs, the private sector and citizens, to share the responsibility of upholding privacy principles.

Currently, the responsibility for addressing online privacy violations that meet the criteria of offences/crimes lies with the state police. Police cybercrime units receive reports from citizens across Albania, all of who have to travel to Tirana to file their complaints.[46] A shortage of human resources and outdated technical equipment limit the capacity of the police officers to address complaints in a timely manner and prevent cyber threats from escalating. In turn, this also impacts citizens' perceptions of the effectiveness of the institution, discouraging citizens from reporting the violations in the first place.

While the Ministry of Internal Affairs has reported an overall increase in the number of cyber incidents in the past three years, suggesting raised awareness of digital safety, many cybercrimes often go unreported, according to human rights activists. When asked about their motives for not reporting these crimes, interviewees expressed little confidence that the institutions would pursue the investigations. Several activists contacted for this report claimed to have been subject to the publication and/or distribution of their private photos, videos, or other personally identifiable materials without their consent. After having publicly criticized the discriminatory and sexist language of an imam, a feminist activist saw her name, photo, and Facebook account shared by a controversial historian, attempting to publicly incite hatred against her. Photos and videos of LGBTI+ activists have reportedly been subject to trolling and bullying, as further elaborated in the following sections. Only in one of the identified cases did the subject report the violations to the state police. In the given case, a human rights activist had her photos and articles stolen from social media and later used to bully, intimidate, and threaten her; however, the state police failed to follow up on the case.

The reluctance to report violations is often also attributed to fear of victim blaming or public denigration. Several cases of **sextortion**[47] of young girls and children have been exposed by the media in the past couple of years. The media has also been the subject of criticism due to unethical reporting on the cases,

---

43 Ibid.

44 Law Nr. 34/2022 on *Determining the Special Procedure for the negotiation and implementation of the agreement with Jones Group International*, Article 5 on Negotiation Procedure.

45 Deibert, Ronald J., *Black Code: Inside the Battle for Cyberspace*, as referenced in McClelland and Stewart, *Privacy and Cyber Security. Emphasizing privacy protection in cyber security activities* (n.d.).

46 Authors' interview with a representative of the C-Unit of the General Directorate of the State Police, Tirana, Albania, 26 May 2022.

47 Sextortion refers to the practice of extorting money or sexual favours from someone by threatening to reveal evidence of their sexual activity.

often exposing personal information on the victims.[48] By way of illustration, the case of sextortion of a 15-year-old girl who had been abused by the school security guard and some other young men triggered massive public reaction and a wave of protests throughout the country in 2020.[49]

In all the reported cases the victims were girls under the age of 18 and the perpetrators were men. In most instances the victim knew the perpetrator, either as an acquaintance, fellow pupil, or former partner, indicating that sextortion may have occurred when the victim was manipulated or pressured into sharing sexually explicit content. Alternatively, intimate images shared in confidence may have been used for blackmail. The media has reported on several cases where women (particularly minors) were subject to **unauthorized sharing of explicit photos and videos** which were used to humiliate and coerce them into engaging in intercourse. Considering digital permanence, cyberviolence against women and girls threatens to result in severe repercussions on their right to privacy, impacting their mental health and well-being.

Interviews with human rights activists revealed the need to address gender-based concerns in cyberspace in Albania. As illustrated above, women are disproportionately targeted through revenge porn and sextortion. In addition, **doxing**[50] also impacts the digital well-being of women activists. An activist of Organizata Politike recalls that after having been detained for participating in a student protest, online media deliberately chose to use photos of her taken at the beach to illustrate the article about the protest. 'I suppose this was done on purpose, considering the majority of the public is very conservative and seeing a semi-clad girl on the beach would impact their perception of me as someone that is not to be taken too seriously,' says the activist, whose Facebook account was also hacked after participating in another protest.

These cases attest to the urgency in bridging the digital gender gap in Albania, which does not consist of merely providing equal opportunities for internet access, but rather building a gender-responsive policy that embraces the perspective of all stakeholders.[51] This can be achieved by integrating gender considerations in cybersecurity policymaking and implementing a multistakeholder approach from the policy formulation phase. In this context, bringing together human rights institutions and cybersecurity stakeholders provides an opportunity to promote more inclusive public policy and improve citizen representation in the cybersecurity framework, ultimately influencing the user experience for women, children, members of the LGBTI+ community, PWDs, ethnic minorities, and other groups.

The digital age has changed the nature of privacy threats, often exposing the intersection between privacy violations and other rights, such as freedom of speech. While the previous violation revealed the impact that unethical reporting has on an individual's privacy or public image, other violations attest to the poor protection for the privacy of citizens, and in particular journalists, whose personal data may be targeted for intimidation or extortion purposes. E.H., a journalist, reported a personal data breach in April 2022. E.H. had occasionally discovered that his account on e-Albania was accessed by A.B., a public notary. The same thing had happened to his wife. The notary had generated a family certificate and a certificate of his wife's social and health care contributions, which shed light on her job occupation, salary, and employer. Neither of them had solicited any services from the notary, nor had ever worked with A.B. before. Through an institutional agreement between AKSHI and the National Chamber of Notaries, registered notaries

48 Bezati, Valbona, *Women in Albanian Media: From Secondary Victimisation to 'Slut-Shaming'*, 27 May 2022.

49 Exit.al., *Albanians Protest against Sexual Violence following Rape of Minor*, 4 June 2020.

50 Doxing refers to searching for and publishing private or identifying information (about a particular individual) on the Internet, typically with malicious intent.

51 World Wide Web Foundation, *React with gender-responsive ICT policy: the key to connecting the next 4 billion* (Washington DC: World Wide Web Foundation; 2017).

can access certificates or other necessary personal information of their clients through e-Albania.[52] The agreement facilitates service provision for all notaries and reduces the waiting time and paperwork for their clients. While there is no evidence yet linking this **unwarranted access** to personal information to E.H.'s journalistic activity, international organizations such as safejournalists.net, Committee to Protect Journalists, and European Centre for Press and Media Freedom appealed to the authorities to investigate the case, considering it journalistic intimidation. The data breach was also registered on the Council of Europe 'safety of journalists platform' as a second level threat categorized under 'other acts having a chilling effect on media freedom'. The case has been reported to the IDP Commissioner and the Tirana Prosecutor's Office and a final verdict is still awaited.

Together with other potential implications, the case raises concerns about the security standards notaries apply and the safeguards that this agreement provides when accessing or processing personal information. Given the sensitivity of their records, notaries are prone to intentional or unintentional data breaches.[53] Therefore, to mitigate these risks, compliance with data protection law and strong guarantees must be provided. However, e-Albania does not provide its users with the possibility to give electronic consent before a notary can access their information. Nor do the notaries require written authorizations from their clients before accessing their data online. The swift pace of digitalization which allows Albanian citizens to access more than 1,200 services online, appears to have an uneven impact on the country's efforts towards data privacy.

To foster safer cyberspace with respect to the right to privacy, strengthening the cybersecurity of critical institutions, as well as investing in assets, is needed. Appropriate budgetary forecasting is crucial in this regard, hence, the upcoming Digital Agenda of Albania 2022-2026 and its draft action plan have envisioned, among other measures, the improvement of the digital systems for the National Civil Registry and the social insurance system. According to the draft of the Digital Agenda, by 2026 Albania is expected to employ big data usage and artificial intelligence for scientific research purposes and to offer proactive services. However, the lack of accountability with which public institutions managed the 2021 data breaches raises major concerns in respect of the right to privacy in Albanian cyberspace. The negotiation process of the agreement with JGI, if made inclusive, represents an opportunity to strengthen collaboration with independent oversight institutions, and guarantee that the right to privacy is taken into account while strengthening national security and the sustainability of the national cybersecurity framework. Ultimately, increased transparency on tracking and PII processes is also necessary for ensuring citizens are well informed about the implications of future privacy violations.

Cybersecurity and freedom of expression

The government's attempts to exert control over media outlets and journalists have resulted in an overall hostile media environment. Compared to 2021, Albania dropped 20 points, ranking 103/180 in the *Reporters Without Borders 2022 Index*, which highlights media regulation, organized crime, and political violence as factors threatening the physical and/or professional integrity of journalists.[54] In Albania, the main challenges in relation to freedom of expression online are of an institutional and ethical nature.

52 AKSHI, *E-Albania, citizens will need fewer documents when heading to notaries* (*e-Albania, qytetarët më pak dokumente në letër para noterëve)*, (AKSHI; 2017).

53 Lewis, M., *The Identity Protection Crisis*, National Notary Association, 20 November 2015.

54 Reporters without Borders, Albania (RSF; 2022).

Previously there were government-initiated attempts to institutionalize control of online media by introducing the commonly referred to 'anti-defamation' legal package in 2019. This initiative was widely contested over concerns of censorship and the Venice Commission recommended that it be revised.[55] Along with other concerns, the anti-defamation package, if approved, would confer on AMA almost judicial powers on the activity of online media. However, the impartiality and independence of this institution cannot be guaranteed, as it is currently run by close associates of the government.[56] Amidst drastic legal amendments and ethical concerns about the implementation of the anti-defamation package, self-regulation of the media would be a more feasible solution, aiming to achieve a fair balance between the need for regulation and freedom from censure. In this framework, the Alliance for Ethical Media was established in 2020, bringing together 19 online media outlets pledging to comply with ethical journalistic standards and striving to protect freedom of speech. The Alliance serves as a self-regulating mechanism with an independent board where citizens can address any ethical complaints.

The scope of the anti-defamation draft laws was overly broad and would threaten to target not only online media, but also individual bloggers and users of social networks. Despite the fact that the anti-defamation package has not been approved, there have been numerous incidents where social media users were investigated as a consequence of online content they had published on their personal profiles. After sharing a public status on his Facebook profile, appealing for citizens to gather at a protest, a political activist was arbitrarily prosecuted as the organizer of the event. Similarly, other activists have been prosecuted after reacting against the poor working conditions of miners and for criticizing AlbChrome, the leading mining company in Albania, for mismanagement. The deaths of eight miners since 2013 prompted many citizens, including activists of Organizata Politike (OP) – a left-wing group – to appeal for better working conditions for miners in support of the Syndicate of Unified Miners of Bulqiza.[57] OP activists made similar appeals on their social media profiles and were later investigated by the police based solely on Facebook content these users had created or shared from other public pages. Being affiliated with the left-wing group, these accusations suggest that the activists are subject to **electronic surveillance** and consequently targeted for their political viewpoints.

In the case of a natural disaster, a government's attention generally shifts to prioritize humanitarian assistance to ensure basic rights and needs, related to physical security as well as economic and social protection needs. However, during these times, it is crucial to closely monitor and promote other civil and political rights as well, such as freedom of speech. For instance, autocratic regimes generally attempt to suppress potential political opposition by restricting freedom of speech and association.[58] Two recent scenarios in Albania were the November 2019 earthquake that caused 51 casualties, and the impact of the COVID-19 pandemic. These exposed subtle, yet worrying, factors that contributed to the deterioration of freedom of expression and media freedom in the country.

Following the devastating earthquake, a 26-year-old activist, Xh.A., was **criminally prosecuted** for sharing a number of Facebook posts on her personal profile. Xh.A. had posted an article from an Italian news portal that claimed that the Porto Romano gas deposits in Durrës had been damaged in the earthquake and there was imminent risk for the population; she appealed to the citizens of Durrës to move to safety. Xh.A. had previously overheard officials mentioning the damage and she had therefore requested information from the state authorities to confirm the information but had not received any response. She was detained for two days, accused of causing panic and urging citizens to leave the

55 Venice Commission, *Opinion No. 980 / 2020*, European Commission for Democracy through Law (Venice Commission), 19 June 2020.

56 European Centre for Press & Media Freedom, *Media Freedom Rapid Response*, ECPMF, 13 July 2021.

57 Taylor, Alice Elizabeth, *Two Miners Injured in Albchrome Mine amidst Ongoing Protests*, Exit News, 7 January 2020.

58 Lin, Thung-Hong, *Governing Natural Disasters: State Capacity, Democracy, and Human Vulnerability*, *Social Forces*, March 2015, pp. 1267-1300, Oxford University Press.

city, even though her Facebook status had received only 26 reactions. After legal proceedings lasting 11 months, Xh.A. was found not guilty by the District Court. Xh.A.'s case became an important precedent for subsequent decisions, ensuring that no one can be condemned for their thoughts or opinions.[59]

Online portals and information channels have frequently come under pressure from the authorities, with the justification of tackling fake news. A popular online portal, joqalbania.com – known for being critical of the government – was **shut down** by AKEP over accusations of triggering panic related to the 2019 earthquake. The Albanian Media Council reacted by denouncing the prime minister for blocking the website without legitimate cause.[60] Similarly, five journalists and three online media administrators were prosecuted for allegedly spreading fake news about the earthquake that caused panic. These arrests raised concerns about the mechanisms used to filter content that can be labelled as fake news and the relevant competences of the state police to identify and tackle such news. Referring to the case, the AMC maintains that the responsibility to filter content or monitor the implementation of ethical standards should lie with independent bodies.[61]

The data breach scandal of April 2021, discussed above, and the events that unfolded thereafter, exposed inter alia, issues related to freedom of the press and protection of journalistic sources. Besides circulating via encrypted communication platforms online, the database containing the personal data and alleged political preferences of 910,000 citizens was initially published by Lapsi.al, an online media outlet. In the course of its investigations, the Special Prosecution Office against Corruption and Organized Crime (SPAK) ordered the **seizure of equipment** from Lapsi.al upon refusal of the latter to provide SPAK with the origins of the database, with the aim of protecting their journalistic sources. Such sources enjoy protection under Albanian law, and the move was widely seen as a threatening precedent to freedom of speech. The involvement of the highest entity on anti-corruption and organized crime in this issue was perceived by many experts to be a disproportionate measure and an attempt to intimidate journalists into revealing the source of the leaked database from the Socialist Party. The management of the online portal submitted an urgent request to the European Court of Human Rights (ECtHR) which ruled in favour of Lapsi.al and ordered SPAK to halt the seizure of the journalists' equipment. The national courts upheld this decision, setting an important precedent for the protection of journalistic sources. It should be noted that the ECtHR only intervenes in such a manner in extreme cases,[62] and this is only the second time in the history of this court that such a procedure was applied to address a violation of freedom of expression.[63]

These cases attest to the limitations in the freedom to impart information and ideas in the Albanian cyberspace. Significant differences are observed in the institutional approach towards the freedom to hold opinions, as exemplified by the cases of political activists who were arbitrarily prosecuted for content posted on their social media. In contrast, smear campaigns (explored below) targeting journalists and activists continue to go unnoticed by the state police. Moreover, the mandated shutdown of the JOQ Albania website and the attempt to intimidate Lapsi.al journalists into disclosing their sources, indicate a tendency to react hastily, shrinking the media environment that expresses opposing views.
The government's approach to public information during the COVID-19 pandemic further reduced the distinction between official information and political propaganda. The prime minister's social media and personal online broadcaster ERTV became the main source of information for updates on important governmental decisions. While in national lockdown, press conferences were inaccessible to journalists, as the result of a clear centralization of information, in particular to PWDs and people with limited access

59 Emiri, Geri, *'Shpërndarje paniku': Policia përndoqi gazetarët pas tërmetit dhe COVID-19*, Reporter.al, 20 July 2020.

60 Albanian Media Council, *Declaration of Concern about the Government Attitude Towards Media*, AMC, 1 December 2019.

61 Emiri, Geri, *Albania's War on 'Fear Mongers' Leaves Rights Activists Uneasy*, BIRN, 29 July 2020.

62 Rule 39 of the ECtHR's Rules of Court on interim measures.

63 Authors' interview with a human rights lawyer, 14 April 2022.

to the Internet. Other groups of interest such as journalists and CSOs also had to rely on social media to obtain information on the latest legal amendments, which in some cases were published on social media before appearing in the official gazette.[64] The shift to social media governance drew criticism from the ombudsperson and non-governmental groups such as the European Center for Freedom of the Media and the Press, and Safejournalists.net, among others. In addition, the establishment of a new Agency for Media and Information (AMI), announced in September 2021,[65] raised additional red flags on further centralization of the flow of information. AMI is expected to monitor online media and manage relations and communication between ministries and the media, which may result in potential violations of the right to information.

In January 2021, a series of **distributed denial-of-service (DDoS) attacks** impacted the website of the Albanian Federation of Football (FShF) and several online media outlets which reported disruption of service or servers, and other aspects related to their online presence.[66] The cyber attacks occurred shortly after the media[67] released an audio recording of the mayor of Tirana, Erion Veliaj, using intimidating and foul language against the head of the FShF, Armand Duka, and attempting to interfere in the upcoming elections within the FShF. Evidently, the attacks aimed to render the websites inaccessible to prevent the leaked audio from being shared. Among other remarks of concern, in what the mayor deemed as 'locker-room talk', he blatantly indicated the political capture of SPAK, while accusing the head of the FShF of corruption.[68] When asked about their experience in dealing with cyber attacks, a representative of an online media platform, which was subjected to a DDoS attack aimed at deleting the online archive, indicated that the process of identifying the perpetrator was complicated and expensive. According to the person interviewed, in these situations, online media concentrate all of their energies on retrieving data and minimizing the damage, instead of reporting the perpetrator, who in this case, remained unidentified.

There have been numerous issues involving online harassment and defamation of journalists over the past years. Female journalists seem to be particularly targeted, while one of the most recent cases involves A.T., a female journalist who received death threats over Facebook. Even though A.T. had done her own investigative work and found information that could identify the perpetrator, no actions were taken by the state police.[69] Previously, another female journalist, S.M., was the subject of discredit, threats, and online bullying after having criticized a doctor on her Facebook account.

While scoping the social media environment in Albania, cases of **coordinated inauthentic behaviour (CIB)** were reported where the accounts of media and HRDs were subject to coordinated reports that aimed to shut down their accounts. These coordinated reports appeared after the publication of investigative or controversial op-eds or videos. In one instance, the subject claimed that more than 50 people were commenting on a video and inciting one another to report the author's social media accounts. This online behaviour is not new to Albania, and according to a Facebook whistleblower, several networks of fake pages and profiles that engage in attempts to disrupt political discourse operate within the country.[70]

---

64 Madhi, Gentiola, *Albania: public information becomes a casualty of COVID-19*, OBC Transeuropa, 11 June 2020.

65 *Council of Ministers*, 2021.

66 Mapping Media Freedom, *Cyber attacks against various media outlets after publishing on alleged election scandal*, 24 January 2022.

67 RTV Ora, Lapsi.al, Doja.al, Syri.net, Maska.al, Gijotina.al, Faktor.al, and SportEkspress were affected by these cyber attacks.

68 Exit.al, *Armand Duka Wins Sixth Term as President of Albanian Football Association*, Exit.al, 15 March 2022.

69 BalkanInsight, *Women as a liability*, 2022.

70 Taylor, Alice, *Albanian Government Considered Buying Hacking Group from NSO Group Competitor in 2014*, Exit News, 23 July 2021.

The importance of tackling CIB is also highlighted by a representative of the Albanian Media Council. During an interview, he said: 'The problem is that they [online media outlets] use a platform with which Albania has no contacts, whatsoever. [...] The entire interaction is based on Facebook's algorithms and this produces a unilateral relationship. Facebook blocks sharing of the content time after time or they ban the entire page – and some of the reasons they cite for doing that relate to the article not complying with Facebook's regulation.' The media expert indicated that the time frame for blocking varies from a one- or three-day ban to a week – and up to a 10-month-long ban. However, the expert argues that the media's lack of interaction with Facebook's administration prevents Albanian media outlets from resolving these issues promptly. Albanian journalists who have attempted to appeal the ban, describe the process as untransparent and the duration of the review is often unknown. It is currently unclear whether Facebook has an established control mechanism that filters out content in the Albanian language, the absence of which indicates that content banning relies solely on the platform's algorithms and policies, which have a disproportionately negative impact on critical media. A pilot study conducted by the AMC on portals which disseminate their articles through Facebook, suggests that the social media platform tends to censor investigative reports and op-eds, citing in most cases ethical standards.[71]

Findings from interviews with journalists and HRDs confirm that coordinated reports of online content of political, environmental, economic, or LGBTQ+ themes are frequently successful. The social media platform blocks the content whereas users are left speculating about the motives. Interviewees suggest that the coordination often occurs through different communication channels, rendering it difficult for Facebook to intervene.

Content that is particularly critical of the work of the government, or that mentions oligarchs, is reportedly deleted by Acromax Media GmbH, a digital rights management company based in Germany. Articles published on websites that have a contract with Acromax can be removed without providing the author with prior notice.[72] Concerns over political censorship grew in 2019 when the Albanian owner of the company claimed that Acromax was collaborating with the Socialist Party for the purpose of reporting fake news about party members on Facebook. Reports from journalists indicated that selected content, critical of the government, or Tirana's mayor, was being systematically removed from the Internet. Acromax currently operates under copyright agreements with several Albanian digital broadcasters, enabling the company to censor the content produced by these media groups on their behalf.[73] For instance, if a journalist wants to make reference in an article to a statement provided by a government official during an interview, he is unable to. Acromax could prevent the journalist from quoting the official in an article, even though the journalist may have conducted the interview himself.[74] However, observations show that the company applies a double standard when it comes to content that promotes or praises the work of the government, which, if shared, is rarely flagged down by Acromax.

During the past couple of years, Albania has witnessed a variety of violations of freedom of expression, including electronic surveillance, criminal prosecutions, coordinated inauthentic behaviour, and other forms of censoring and intimidation. Cases of government-mandated shutdowns, targeted cyber attacks, online harassment of journalists, and a shrinking space for the freedom to receive and impart information, further attest to the recent decline in freedom of the media. With the increase in online avenues for censoring that stifle criticism and the promotion of government propaganda, independent journalism is

---

71 AMC, *The Albanian Media Council presents the pilot study Problems with Ethical Regulation of the Albanian Media from the Facebook platform*, 25 February 2022.

72 Authors' interview with a journalist, 3 February 2022.

73 Konrad-Adenauer-Stiftung, *The Shrinking Space for Media Freedom in Southeast Europe in the Midst of COVID-19 Pandemic and State Emergency: A Comparative Overview* (KAS; 2020).

74 Laufer, Daniel, *A German company is responsible for the deletion of videos critical of the Albanian government*, Netzpolitik.org, 19 March 2020.

faced with increasing challenges. Instead of the 'state regulation of the media' approach, self-regulation and ethical reporting should be promoted, as well as more governmental transparency. This could provide the media landscape in Albania with the positive shift it is lacking.

Cybersecurity and prohibition of discrimination

Cyberspace may represent a new realm where human rights violations flourish and certain groups are targeted more than others. Violations taking place in this somewhat ungoverned environment often go unpunished whilst institutions fail to respond to new realities and guarantee the same rights online and offline. Among the most common forms of discrimination identified in the digital environment in Albania are hate speech and harassment. A national survey revealed that about 58% of Albanian citizens consider hate speech to be very prevalent in the country, whilst among citizens belonging to vulnerable groups, nine out of 10 consider that hate speech is very widespread.[75] According to 64%, social media is thought to be the environment where hate speech is predominant. Other available data indicate that the groups commonly targeted by such violations are women,[76] children,[77] and minority groups such as Roma, Egyptians,[78] and LGBTI+ people.[79] Worryingly, it is noticed that those who defend these groups, such as human rights defenders, are targeted and smeared online as well.[80]

In recent years, the Ombudsperson and CPD, have acknowledged these problems in their annual reports, their decisions and public statements. Addressing these issues is crucial since they can, among other repercussions, lead to hate crimes.[81] Nevertheless, an overall comprehensive data collection system that would enable a thorough assessment of the situation at the national level is lacking. This is also confirmed by the European Commission against Racism and Intolerance (ECRI) and the OSCE/ODIHR, according to which, Albania has not systematically reported the number of hate crimes registered by the police.[82] By way of illustration, the Annual Report of the General Prosecutor, *On the situation of criminality during 2020*, reveals that six cases of inciting hate were prosecuted during 2020, with only one conviction. The report does not indicate whether they took place online or offline and which groups were targeted.[83] Furthermore, according to the same report, no reports of racist or xenophobically motivated threats or cases of distribution of racist or xenophobic content via computer systems were registered during 2020. With regard to sexual harassment, 58 cases were prosecuted in 2020, and 18 persons were convicted. Similarly, the report does not indicate whether the harassment took place online or not. Such limited data do not allow for a comprehensive analysis to be made to identify areas for intervention in tackling hate speech, harassment, or other forms of discrimination or criminal offences motivated by discrimination that take place in cyberspace. The report itself recognizes the shortcomings in the data collection system, pointing out the need to process data on the motives of the crimes, as well as the need

75 CPD, *Beyond definitions, a call for action against hate speech in Albania*, The Commissioner for Protection from Discrimination (CPD) ; 2021.

76 *Reporter.al*, 2021.

77 *iSIGURT.al*, 2021.

78 European Commission against Racism and Intolerance, *ECRI Report on Albania (sixth monitoring cycle)* (ECRI; 2020).

79 The Commissioner for Protection from Discrimination, *Beyond definitions, a call for action against hate speech in Albania*; 2021.

80 Civil Rights Defenders, *Human Rights Defenders in the Western Balkans: Intimidation instead of recognition, Albania* (CRD; 2020).

81 Authors' interview with a representative of the Commissioner for Protection from Discrimination, 14 April 2022.

82 European Commission against Racism and Intolerance, *ECRI Report on Albania.* (ECRI; 2020).

83 General Prosecutor's Office, *General Guideline 17/2020 of the General Prosecutor*, 2020.

for a functional automated system at the national level. Further, it states that the improvement of the data collection system requires a coordinated and harmonized approach that goes beyond the internal needs of each institution involved. According to the same report, in 2020, a dedicated register for the collection and processing of data related to violence against women and children, hate-motivated crimes, and domestic violence, was created. Nevertheless, the mandate of the General Prosecutor[84] that regulates the functioning of this register and the way statistical data are collected and processed, only covers crimes against minors.

Despite the many shortcomings in addressing these issues, some good practices that can be built upon have been identified. In 2019, the Alliance Against Hate Speech was established, through a memorandum of cooperation signed between the Ombudsperson, CPD, AMA, and the AMC.[85] This alliance of key actors aims to coordinate and unite efforts to prevent hate speech, raise awareness and jointly advocate against this phenomenon. The establishment of the Albanian national hotline for Internet safety by the Child Rights Centre Albania is another positive example of coordinated efforts between CSOs, public institutions, and the Internet and communications industry. This is a platform where child harassment and hate crime/speech cases can be reported, to then be referred to the relevant authorities. In addition, the approval of the General Guideline of the General Prosecutor[86] on the effective criminal investigation of violence against women, domestic violence, and hate-motivated violence, was another positive step taken in 2020. The guideline aims to unify institutional practice in this regard and ensure efficiency in prosecuting these crimes. It also defines aspects of cyber stalking, the use of social media for hate crimes as well as providing a wide list of discriminatory motives that could lead to hate crimes, going beyond the Criminal Code which fails to do this.

Even though the human rights violations concerning hate speech and harassment that take place in cyberspace seem to rarely make it through the Albanian criminal justice system, the situation is more encouraging when it comes to the response of the independent human rights institutions. In recent years, several cases of discrimination in cyberspace have been addressed, mainly via complaints filed by CSOs, but in some cases also initiated by the CPD ex officio. Some decisions taken by the CPD provide in-depth analysis of hate speech cases, as a form of discrimination, as well as its interrelation to freedom of expression and the limits of the latter. The CPD in its decisions has referred to international standards of human rights and cyber law, the ECRI's recommendation No. 15 on combating hate speech, as well as the case law of the ECtHR and the European Court of Justice. On the other hand, case law of national courts in this regard is almost inexistent.

With regards **racial discrimination**, an online portal (joq.al) used discriminatory and stereotyping language against the Roma and Egyptian communities in a Facebook post, which prompted a CSO to file a complaint with the CPD. The CPD found that the online portal had directly discriminated against Roma and Egyptians, based on race, in the form of harassment and required them to cease sharing discriminatory content.[87] This case is of interest due to its several dimensions. Firstly, during the administrative investigation the CPD was very proactive, and after several unsuccessful attempts to locate and communicate with the administrators of the portal, reached out to Facebook (the company) directly and requested the removal of the post in question. This highlights the challenges faced when trying to identify owners/administrators of online media in order to ensure accountability, since they are not registered. The implementation of the decisions of the CPD in such cases depends on the willingness of the media administrators or the social media platforms to remove the discriminatory content, otherwise

84 Order 124/2020 of the General Prosecutor.

85 Ombudsperson, *Annual Report of the Ombudsperson for 2020*, 2021.

86 General Guideline 17/2020 of the General Prosecutor.

87 Decision No. 135, 13 June 2018, of the Commissioner for Protection from Discrimination.

it cannot be enforced.[88] Furthermore, the decision analysed above made references to the Convention on Cybercrime and its Additional Protocol, and also elaborated on the impact that the given online portal could have, due to its large audience and popularity, in contributing to an overall aggressive, negative and discriminatory attitude against Roma and Egyptians.

Moreover, the CPD has dealt with several **discrimination cases against the LGBTI+ community** that have taken place in cyberspace. Addressing a complaint submitted by CSOs, the CPD found the language used in a Facebook post of a political party (Aleanca Kuq e Zi) to be discriminatory, in the form of hate speech against the LGBTI+ community.[89] The post made a public call for a protest against the legalization of same-sex marriage and against the Pride parade. The post received many hate comments calling for violence towards and death of LGBTI+ persons. According to the CPD's decision, both the Facebook post and the subsequent comments incited hate based on sexual orientation and gender identity. Even though the political party deleted the post, the CPD fined them and requested the issuing of a public apology. This decision was challenged later on before the Tirana Administrative Court of First Instance, which upheld the decision of the CPD.[90] Both the decision of the CPD and that of the court are among the first of this nature, taken only a few years after the approval of the Law on Protection from Discrimination, and can be considered landmarks on protection of LGBTI+ from online hate speech.

Discrimination based on disability is another form of discrimination that has been identified. Stigmatizing language was used against people with Down syndrome during a reality show on Top Channel television, and was also broadcast on its social media channels. The CPD took action on its own initiative and found the language used to be discriminatory on the basis of disability, in the form of harassment, and required the television channel to issue a public apology.[91] Like a similar case described above, this brings attention to the impact of audiovisual media on cyberspace, and the utilization of anti-discrimination legislation in addressing hate speech taking place via television channels, their social media channels, and the comments that are consequently generated. Nevertheless, ensuring accountability of the latter remains a challenge since online media are not registered and the management of comments is not regulated.

In addition, PWDs can be exposed to indirect discrimination when they do not have **accessible online public services**. As of May 2022, all public services are offered online, while assessments on the impact this decision may have on certain groups are lacking. This could expose PWDs or those who lack digital literacy to unfair treatment. Such groups often face an added financial burden as well, since they are increasingly reliant on private businesses to receive assistance with online applications for services. Digitalization of services, without ensuring reasonable accommodation and accessibility, can result in a violation of the Law on Protection from Discrimination, and the Law on the Inclusion and Accessibility of PWDs. On the other hand, while about 88.3 per cent of Albanian families have **access to Internet services**,[92] there are no data with regard to the groups who do not have access to the internet and, as a result, may be discriminated against, being unable to benefit from online public services. This gap in available data has become even more evident since the COVID-19 pandemic began, when many institutions started working remotely, and must be addressed in light of the digitalization of public services.[93]

88 Authors' interview with a representative of the Commissioner for Protection from Discrimination, 14 April 2022.

89 Decision No. 125, 1 August 2014, of the Commissioner for Protection from Discrimination.

90 Decison No. 3127, 9 June 2015, of the Tirana Administrative Court of First Instance.

91 Decision No. 155, 30 October 2020, of the Commissioner for Protection from Discrimination.

92 Institute of Statistics *ICT in families*, 2021.

93 Authors' interview with a representative of the Commissioner for Protection from Discrimination, 14 April 2022.

Sexual harassment was listed as a form of discrimination by the Law on Protection from Discrimination in 2020. When the legal threshold and criteria set by the Criminal Code are met, it can be classified as a criminal offence as well. Since this law is relatively recent, the body of sexual (cyber) harassment cases reviewed by the Commissioner for Protection from Discrimination is limited. Furthermore, the insufficient technical capacities of the CPD affect its capability to conduct thorough administrative investigations in cases where sexual harassment takes place online. By way of illustration, in a case of sexual harassment in the workplace, the main evidence presented to the CPD were messages exchanged on the WhatsApp application. Unable to verify their authenticity, the CPD suspended the administrative investigation. The claimant filed a criminal report in addition to the complaint filed with the CPD (which do not interfere with each other) and the Prosecution requested the verification of the messages for the sake of the criminal investigation. Only when provided with the act of expertise (produced within the criminal investigation) certifying the authenticity of the WhatsApp messages, was the CPD able to resume the administrative investigation and found the claimant had been discriminated against on the basis of gender in the form of sexual harassment.[94]

Gender-motivated hate speech is another form of discrimination which is increasing in Albania. A 2020 monitoring of online media conducted by CSOs revealed that 70 per cent of cases of hate speech are aimed at women,[95] and studies indicate that this group are particularly targeted when engaged in activism and public activity. The same data show that during the past two years, sexist and gender-motivated hate speech cases have doubled. A report on HRDs in Albania reveals that **women human rights defenders** (WHRDs), are the second most at-risk group of HRDs, after LGBTI+ activists.[96] Particularly targeted seem to be WHRDs working with victims of human trafficking or domestic violence, feminist or LBT+ activists and journalists.[97] They are exposed to continuous harassment, not only because of their gender but also because of the work they do, therefore the motives, in this case, become **intersectional**. Given that intersectional discrimination and multiple discrimination were recently enhanced by the Albanian anti-discrimination legislation, institutional practice and public awareness are limited in this regard. The WHRDs contacted for this report revealed cases when they were sexually harassed on social media, received hateful misogynistic comments, were cyberbullied and trolled by the sharing of their private photos and information, received rape threats, and were smeared online due to their gender and political, feminist, and/or human rights activism. The majority of the WHRDs (with one exception) had not reported these violations, mainly due to a lack of confidence that the authorities would respond at all or provide any effective solution. Only one feminist activist, who chose to remain anonymous, had reported a case of cyber harassment to the police, but no action was taken by the latter. The lack of response by the police and prosecution on cases of gender-based cyber harassment is also evidenced in a report by DCAF, wherein the given case study on Albania, despite several incidents being reported, there was no action taken by the authorities.[98] In the given case of a feminist activist, the cybercrime unit within the state police played an advisory role, rather than a law enforcement role and failed to provide effective protection.[99] Meanwhile, the prosecution did not initiate a criminal investigation because they did not regard the actions as a 'threat'.[100] These institutions need to be empowered as they often have insufficient

94 Decision no. 259, 29 December 2021, of the Commissioner for Protection from Discrimination.

95 Citizens Channel, *Monitoring: About 70% of hate speech and discrimination on online media affects women and girls*, 2020.

96 Civil Rights Defenders, *Human Rights Defenders in the Western Balkans: Intimidation instead of recognition, Albania* (CRD; 2020).

97 Ibid.

98 DCAF, *Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cybersecurity Governance Approach* (Geneva: Geneva Centre for Security Sector Governance (DCAF); 2021).

99 Authors' interview with human rights expert, 03 February 2022.

100 DCAF, *Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cybersecurity Governance Approach* (Geneva: Geneva Centre for Security Sector Governance (DCAF); 2021).

human resources and lack technical infrastructure and training, making it difficult to duly respond to the reports they receive.[101]

Alongside WHRDs, the most targeted category of human rights defenders in Albania are **LGBTI+ activists** and those working on the rights of sex workers, according to a Civil Rights Defenders report.[102] They are more likely than others to face anonymous threats, while online hate speech against these activists is quite common. K.P., an activist and founder of an LGBTI+ organization, left Albania and was granted asylum in another country, after receiving dozens of death threats and denigrating messages on social networks.[103] Xh.K, another frontline LGBTI+ activist, was subjected to online hate speech and threats after appearing on national television speaking in favour of parental rights for LGBTI+ people.[104] A trans activist, who wished to remain anonymous, said he had been subjected to hate speech and threats on social media platforms when publicly coming out as trans and publishing statements on LGBTI+ rights. To date, no perpetrator has been held legally accountable for any of these violations.[105] As with WHRDs, LGBTI+ individuals rarely report the online threats they receive, because of the prevailing belief among these activists that homophobic online threats are not taken seriously by the police or the prosecution. They argue that while there is considerable impunity even when it comes to physical homophobic hate crimes, the sensitivity of authorities towards cyber attacks is almost inexistent. None of the cases they had ever reported were prosecuted as the authorities either failed to identify the individuals hiding behind fake profiles, or the evidence was not deemed sufficient for the reported threat to reach the threshold of illegality and be classified as a criminal offence.[106]

With regard to **discriminatory automatic decision-making,** otherwise referred to as **algorithmic bias,** institutional practice and regulation as well as public awareness are lacking. In this regard, one case was identified, concerning the unfair disqualification of some families that applied for state-provided financial aid via a pilot electronic system introduced by the government in 2014.[107] The automated system evaluated the citizens' applications for financial aid based on 52 variables and according to the CPD it seemed to favour families with a higher number of members, and often left out single mothers, elderly living alone, Roma and Egyptians and so on, even though they met the legal criteria. The CPD found that there was discrimination and recommended the automated electronic system be improved in order for it not to allow for differentiated treatment and unfair disqualification of citizens who fulfilled the legal criteria, to benefit from the financial aid.[108]

In conclusion, more efforts are needed in terms of effectively addressing discrimination cases that take place in cyberspace, building trust and awareness, as well as tackling prevailing impunity, particularly within the criminal justice system. Furthermore, a comprehensive data collection system for hate incidents at the national level should be established. Such data would enable the identification of areas for intervention in tackling hate speech, harassment, or other forms of discrimination or criminal offences that take place in cyberspace. Finally, the relevant legal framework should be brought up to date, and institutions should be empowered with additional knowledge and infrastructure to respond to emerging challenges of human rights in cyberspace, and in order to provide equal protection online as well as offline.

---

101 Civil Rights Defenders, *Human Rights Defenders in the Western Balkans: Intimidation instead of recognition, Albania* (CRD; 2020).

102 Ibid.

103 Dritare.net, *Received death threats, K.P. forced to flee Albania*, 2017 (title edited for privacy).

104 Norwegian Helsinki Committee, *Albania investigates threats against Xh.K.*, 2021 (title edited for privacy).

105 Authors' interview with a LGBTIQA+ activist, Tirana, Albania, 29 March 2022.

106 Ibid.

107 Authors' interview with former Commissioner for Protection from Discrimination, 6 May 2022.

108 Decision no. 185, 24 December 2015, of the Commissioner for Protection from Discrimination.

Cybersecurity and freedom of peaceful assembly

The Internet and the wider cyberspace are the key contemporary places where people interact and participate in public affairs. Over the past decade, they have become increasingly central to exercising freedom of peaceful assembly, serving both as a space and a tool. The crucial impact of such means in Albania and globally was particularly felt during the COVID-19 pandemic lockdowns, when HRDs, CSOs, and citizens intensively used the Internet to plan, organize, advertise, record, and participate in assemblies and public events. During this time Albania saw its first online pride parade,[109] while a good majority of the protests organized in the past few years have been initiated and disseminated via social media.

There is currently no public debate taking place in Albania on online assemblies or their regulation, and awareness among stakeholders regarding the challenges posed to the exercise of freedom of assembly in cyberspace is generally lacking. Nevertheless, different groups of activists and movements such as the feminist movement,[110] environmental groups,[111] youth and students,[112] LGBTIQA+ persons,[113] and so forth, are increasingly utilizing social media platforms, mainly Facebook, to reach out to the public and to organize and coordinate protests and events. The government has not imposed any restrictions on the use of social media, and organizers/participants in assemblies can use it before, during, and after the organization of a gathering. To date, no cases of blocking access to online communication have been registered.[114]

Some of the most common threats identified regarding the exercising of freedom of assembly online, concern the **targeting of HRDs involved in the organization of protests** through smear campaigns, threats, as well as DDoS attacks on their personal social media accounts. A trans activist, who chose to remain anonymous, was harassed on social media, receiving over 500 hate comments after sharing a post inviting people to join the Tirana Pride. The perpetrators managed to block his account for almost a month, via organized reportings. Activists of the left-wing political organization Organizata Politike have faced similar harassment and online smears due to their involvement in the student protests of 2019, as well as their public activity in support of the rights of miners. They believe the attacks came from actors affiliated with the government and local businessmen. Several activists from the same organization had unidentified persons try to access their personal social media accounts, following a demonstration they had organized against the prime minister. Such tactics of coordinated trolling and reporting of activists are quite common and aim to flood social media in a strategic way, with the sole goal of misleading public opinion[115] and discouraging their actions. To minimize such risks, some activists reported having started using safer online platforms for internal coordination purposes.

---

109 United Pro LGBT Albania, *Albania holds its first online parade: There is no justice for LGBTI people if there is no democracy for everyone else*, 20 May 2020.

110 *Reporter.al.*, 2020.

111 Mediacentar Sarajevo, *Communicating citizens' protests, requiring public accountability: Case studies from Albania, Bosnia and Herzegovina and Macedonia*; 2016.

112 Ibid.

113 United Pro LGBT Albania, *Albania holds it first online parade: There is no justice for LGBTI people if there is no democracy for everyone else*; 2020.

114 Partners Albania, *Monitoring the right to free assembly : Albania country report 2016-2017*, 2017.

115 Civil Rights Defenders, *Human Rights Defenders in the Western Balkans: Intimidation Instead of Recognition* Rights Defenders; 2020).

Activists' perception is that their social media activity related to the organization of protests or criticizing governmental policies is monitored

Regarding the **surveillance of assemblies**, activists' perception is that their social media activity related to the organization of protests or criticizing governmental policies is monitored by the authorities, political parties, or other actors acting on their behalf.[116] This impression comes as a result of several red flags that have been raised regarding government surveillance. Firstly, the creation of the above-mentioned AMI, which will monitor social media to evidence public perception and attitudes towards the activity of public administration institutions, and which is seen as a mechanism of potential surveillance.[117] Further, an e-mail leak indicated that the Albanian government considered buying software in 2014 from The Hacking Team, known over allegations of hacking journalists, politicians, and activists on behalf of global governments.[118] In light of these observations, an activist for Roma and Egyptian rights said she refrained from posting about protests on social media since she feared being surveilled, particularly during the state of emergency, when an absolute ban was imposed on assemblies, as well as a EUR 40,000 fine for those who violated this rule. Other activists, who wished to remain anonymous, revealed that when being questioned by the prosecution with regard to participation in a protest, they were asked to disclose the names of the administrators of the social media pages they used for activism. Requests for access to their personal accounts or phones were also made, but the activists refused. In similar cases, when brought in for questioning, they did not bring their phones with them; nevertheless, they were asked by the police officers to log into their personal social media accounts from the police office computers instead. Such actions, when the person being questioned has not officially been accused of a crime, are in violation of the Code of Criminal Procedure and could interfere with the right to not incriminate oneself.[119] Additionally, activists have experienced cases where the police had referred to social media posts to arbitrarily identify the organizer of a given protest in order to criminally prosecute them. Such practices can have a chilling effect on HRDs and other participants in assemblies, discouraging the use of social media for assembly.[120]

Another important element concerning the exercise of freedom of assembly online is **the role of media** in documenting and communicating activities and protests taking place. Social media is widely used to disseminate information in real-time on activities as they unfold and without any formal editorial process. Such an inclusive approach to reporting may help to increase awareness of protests, holding the authorities to account for their actions during the protest, but it may also help mobilize other people to join the activity.[121] Transparent, uncensored, and unbiased reporting becomes even more important in countries like Albania, where the mainstream media environment is dominated by pro-government propaganda and where journalists are constantly under attack. Under these circumstances, the public often turns to online media as a more reliable source of information. Therefore, due to the important role they play and the major public impact they can have, independent online media can become targeted as well, when reporting on assemblies. In December 2020, massive protests were held nationwide in Albania, as a reaction to the murder of a young man, K.R., by a police officer, while he was walking home past curfew hours. Citizens Channel, an independent online media outlet promoting citizen journalism as described above, was livestreaming and reporting on these protests for several days in a row, including reporting on police violence and abuse, when their website experienced a DDoS attack and was down for a few days as a result. The apparent aim of the attack was to delete all the existing content from their

116 Authors; interview with a human rights expert, 3 February 2022.

117 Authors' interview with a human rights lawyer, 14 April 2022.

118 Taylor, Alice, *Albanian Government Considered Buying Hacking Group from NSO Group Competitor in 2014*, Exit News, 23 July 2021.

119 Ibid.

120 Ibid.

121 European Center for Not-for-Profit Law, *Safeguarding online assemblies*, 2020.

website. Even though the source of the attack to date remains unknown, some experts saw this as an attack related to the reporting by Citizens Channel of the protests.[122]

In conclusion, the digital revolution seems to be changing how assemblies look, how they are organized and held, but also how they are surveilled and repressed. This requires increased awareness of the new challenges arising, and a prepared response by all relevant stakeholders to address them, as well as a more enabling and contemporary legislation that goes beyond the classic means of guaranteeing the exercise of freedom of assembly.

WAYS FORWARD

RECOMMENDATIONS FOR PUBLIC ACTORS: GOVERNMENT, PARLIAMENT, AND LAW ENFORCEMENT AUTHORITIES

On legal framework:

- Amendments to the Criminal Code should be adopted regarding crimes motivated by discrimination or hate to ensure protection in cyberspace.
- Amendments to the Criminal Code should be adopted to address online stalking.
- Anti-SLAPP legislation should be adopted to strengthen legal guarantees for the protection of freedom of expression, addressing both online and offline contexts.
- Amendments to the Law on Protection from Discrimination should be adopted to adequately address forms of discrimination occurring in cyberspace, including discriminatory automatic decision-making.
- Amendments to the Law on Assemblies should be adopted to provide adequate guarantees for online assemblies.
- Amendments to the laws on media and electronic communications should be adopted to provide a unified legal definition of harmful and illegal content and indicate the entitled authorities that may request the removal of online content.

122 Authors' interview with a human rights expert, 3 February 2022.

On policy framework:

- An intersectional approach to policymaking in the area of cybersecurity and human rights should be adopted in order for cybersecurity documents to include a human rights approach, and strategic human rights documents to incorporate the human dimensions of cybersecurity.
- Inclusive consultation processes between public and non-public actors should be carried out when strategic documents are being developed.
- Human rights risk assessment tools should be developed to mitigate discrimination risks and ensure evidence-based decision-making related to the digitalization of public services.
- A unified and comprehensive data collection system on discrimination/hate-motivated crimes should be established addressing both online and offline contexts.
- A stewardship approach should be adopted, enabling public and non-public actors to share the responsibility of upholding privacy principles on cyberspace and shaping inclusive policymaking.
- Urgent measures must be taken to strengthen data protection safeguards and compliance of inter-agency agreements and agreements with private subjects.
- Increased transparency is needed regarding the modalities of data storage of personal identifiable information and its transfer to third parties.
- Appropriate measures are needed to enable public authorities to extend the monitoring of minimal security measures of any subcontracted parties in relation to administrative operators of key information infrastructure, to increase private sector accountability.

On institutional capacities and cooperation:

- Increased cooperation is needed between cybersecurity institutions and independent human rights institutions in exchanging information and expertise when addressing human rights violations occurring in cyberspace.
- Increased coordination efforts are needed between cybersecurity institutions, to ensure adequate oversight and accountability both on technical and policy matters.
- Capacities of police officers, judges, and prosecutors should be raised on international standards on guaranteeing human rights in cyberspace.
- The state police and prosecution should be provided with adequate human and technical resources to address cybercrime both at the central and local levels.
- Independent human rights institutions should be provided with adequate human and technical resources to be able to conduct thorough administrative investigations on violations occurring in cyberspace.
- Cybercrime police officers and prosecutors should be provided with adequate training on conducting effective criminal investigations of crimes motivated by discrimination or hate occurring in cyberspace.

Trust-building measures between them and the discriminated groups that are targeted online should be undertaken, to tackle the underreporting of violations.

- The online reporting mechanism of the state police for cybercrime should be made functional and accessible for citizens nationwide to facilitate the reporting of violations in a timely manner.

RECOMMENDATIONS FOR NON-PUBLIC ACTORS: CSOS, ACADEMIA, MEDIA, INTERNATIONAL DONORS

On public awareness and accountability:

- Human rights violations occurring in cyberspace should be actively monitored to enable thorough research and assessment of the situation, which is currently insufficient.
- Non-public actors should actively contribute to consultation processes on legislative amendments and strategic policy documents related to cybersecurity and human rights.
- Public awareness should be raised about forms of discrimination occurring in cyberspace to encourage citizen reporting and for institutional practice to be developed in this regard.
- Public awareness should be raised on privacy threats occurring in cyberspace to encourage citizens to effectively identify and report any violations.

On capacity building and support for civil society and media:

- A self-regulation approach to online media should be promoted, in accordance with best practices, to ensure proportionality between accountability for violations and freedom from censure.
- Capacities of journalists should be increased with regard to ethical reporting and human rights issues.
- Capacities of CSOs and activists should be increased regarding the challenges posed to exercising freedom of assembly in cyberspace and mechanisms for protection.
- Digital security training and technical support for journalists and activists should be enhanced.
- Legal services for journalists and activists facing cyberthreats should be supported.

CHAPTER 2

BOSNIA AND HERZEGOVINA

Navigating the Legal System and Promoting Good Practice

By Aida Mahmutović and Aida Trepanić | Balkan Investigative Reporting Network Bosnia and Herzegovina (BIRN BiH)

CHAPTER 2

BOSNIA AND HERZEGOVINA – NAVIGATING THE LEGAL SYSTEM AND PROMOTING GOOD PRACTICE

THE CYBERSECURITY CONTEXT IN BOSNIA AND HERZEGOVINA

Cybersecurity is an area of vital concern for any country and encompasses the detection and prevention of cyber attacks, responses to such attacks, and the protection of data and information of all kinds against the risk of being stolen or compromised, which poses threats to national security and to the security of organizations, communities, and individuals. This includes personal and health-related information, sensitive data of all kinds, intellectual property, and information held in government, business, and industry computer systems. A cybersecurity strategy is one of the most essential tools for keeping a country, its businesses, and ultimately its people safe.

National computer emergency response teams (CERTs) play an essential role in critical information infrastructures protection (CIIP) and are a crucial part of any cybersecurity strategy.[123] According to the *National Cybersecurity Strategies Repository* of the International Telecommunication Union (ITU), 116 countries have a national cybersecurity strategy either already in place or in draft form.[124] Worldwide, as of March 2019 there were *118 national computer incident response teams (CIRTs)* in existence.[125]

The frequency of cyber attacks is *increasing globally*;[126] however, in 2022 Bosnia and Herzegovina (BiH) remains the only country in the Western Balkans (WB) not to have a state-level cybersecurity strategy or an operational network of CERTs and CIRTs at the national and regional levels. Given the country's current political landscape, it is not likely either that these will exist any time soon.

In the 21st century cybersecurity is closely bound up with the functioning of the state, as demonstrated in the United States in May 2021 when *the Colonial Pipeline suffered a ransomware cyber attack* targeting computerized equipment managing the pipeline, which carries gasoline to the eastern part of the country.[127] The consequences of cyber attacks can be just as damaging as the impacts of attacks from

123 https://www.ncsc.gov.uk/collection/incident-management/creating-incident-response-team

124 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

125 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

126 https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=2ce3ed1c7864

127 https://edition.cnn.com/2021/05/10/politics/colonial-pipeline-white-house-reaction/index.html

other sources, and this is why the establishment of a national-level CERT is so important, especially at the present time. In May 2022, for instance, Mircea Geoană, Deputy Secretary-General of NATO, warned about potentially massive cyber attacks by Russia on the critical digital infrastructure of Georgia and BiH, pointing out: 'Cyber attacks are, next to disinformation and digital espionage, a part of a new kind of warfare.'[128]

While NATO pledges to support countries' defensive capabilities, including against cyber warfare, it is unclear in the case of BiH to what extent relevant institutions and organizations consider cyber threats to be of critical importance, whether formal state-level cyber attack drills are carried out, and what kinds of coordination are in place, if any. This includes security efforts by the BiH government to prevent cyber attacks, mitigate damage, and protect critical infrastructure, businesses, and citizens and their rights.

BiH does not have a CERT at the national level. The European Union Agency for Cybersecurity (ENISA) lists the CERT of Republika Srpska (CERT RS) as a national governmental CERT,[129] but this gives a misleading impression as this CERT functions in only one part of the country.

In June 2022 the Criminal Policy Research Centre (CPRC) in Sarajevo, in cooperation with the University of Sarajevo, established an academic CERT whose goal is to provide services primarily to the academic community, independent media organizations, and civil society organizations (CSOs) across the country.[130] It is important to note that an academic CERT of this type could become a national-level organization if the state were to establish a legal framework for this to happen.

Predrag Puharić, Chief Information Security Officer at the Faculty for Criminal Justice, Criminology and Security studies at the University of Sarajevo and CEO of the academic CERT, told BIRN that slowness to adopt a state-level cybersecurity strategy was leaving BiH extremely vulnerable to cyber attacks. He said: 'I think that Bosnia and Herzegovina has not set up adequate mechanisms for prevention and reaction to even remotely serious attacks against state institutions or citizens themselves.'[131]

In 2017, the Ministry of Security of BiH (MoS) was tasked with drafting a national cybersecurity strategy, which was to be implemented after approval by the government, but to date none of this has happened. So far, and with the help of the Organization for Security and Co-operation in Europe (OSCE), only guidelines for a cybersecurity strategy have been adopted.[132]

For the purpose of this research, BIRN BiH contacted the MoS on several occasions in an attempt to obtain first-hand information on the challenges involved in formulating the national cybersecurity strategy and any successes – what has been done so far and what activities are currently ongoing. However, the ministry did not respond to requests for an interview. For a previous analysis by BIRN, the *MoS stated* that it had been unable to adopt a comprehensive strategy "because of the non-conformity of bylaws, but that the issue would be included in the country's 2021-2025 Strategy for Preventing and Countering Terrorism".[133]

The Ministry of Defence (MoD) has its own cybersecurity strategy, the Cybersecurity Strategy of the Ministry of Defense and the Armed Forces of Bosnia and Herzegovina. In response to a freedom of information (FOI) request from the Balkan Investigative Reporting Network in BiH (BIRN BiH) in February

128 https://tvpworld.com/60226190/russia-may-target-georgia-bosnia-and-herzegovina-nato-deputy-secretarygeneral

129 https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

130 https://detektor.ba/2022/06/01/osnivanje-drzavnog-tima-za-racunarske-incidente-potrebno-za-sigurnije-koristenje-interneta/

131 https://detektor.ba/2021/03/10/cyber-attacks-a-growing-threat-to-unprepared-balkan-states/?lang=en

132 https://www.osce.org/bs/mission-to-bosnia-and-herzegovina/438386

133 https://detektor.ba/2021/03/10/cyber-attacks-a-growing-threat-to-unprepared-balkan-states/?lang=en

2021, the ministry stated that neither it nor the Armed Forces had experienced any significant cyber attacks on communication and information systems or on networks supporting essential business processes. However, it added that if a cybersecurity strategy were to be established at the state level along with certain other security measures, such as the creation of a CERT, this would certainly make it easier for all institutions to make their cyber environments more secure.

The MoD explained that the goal of its in-house strategy was to establish a functional and sustainable cybersecurity system that would ensure a secure working environment for communication and information systems and networks, and thus improve the country's overall security situation. It defined its goal as the following: 'certain security measures are established and implemented, which are of a normative, procedural or technical nature'. While the MoD does not envisage the establishment of new departments or structures to deal with cybersecurity within either its own operations or those of the Armed Forces, it does not exclude this from happening in the future.

In parallel, an informal working group of experts on cybersecurity, known as the Neretva Group, is operating in the country under the auspices of the OSCE Mission to BiH, with support from the Delegation of the European Union in BiH and the EU Special Representative (EUSR) in BiH. The Group includes practitioners and IT/cyber experts along with representatives from the private and public sectors and from all levels of government. It drew up guidelines for a strategic cybersecurity framework in BiH in 2018-2019.[134] According to Sanja Catibovic, National Programme Officer for Security Co-Operation at OSCE in BiH, 'these guidelines have a comprehensive concept and deal with the most important priority areas for improving cybersecurity in BiH in accordance with international standards'. However, given the lack of response from the MoS, it is unclear whether these guidelines will ultimately form part of a national cybersecurity strategy, even partially.

A national Internet Governance Forum … brought together actors from all sectors that played a significant role in governing the use of the Internet in the country

In 2015, BiH took a step towards joining the Internet governance landscape by forming a national Internet Governance Forum (IGF BiH), which for the first time brought together actors from all sectors that played a significant role in governing the use of the Internet in the country.[135] The IGF BiH was convened for three consecutive years from 2015 to 2018 but unfortunately, due to a lack of will by actors to engage in a multistakeholder, bottom-up, and open discussion, it has not existed for four years now, even though there is more need now than ever for a forum of this kind for discussion and policy in light of the ever growing impacts that cybersecurity has on human beings and their rights. This was the only bottom-up, multistakeholder model policy fora which existed for three consecutive years and was supported by both international and national actors, including the UN IGF Secretariat.

In line with its EU accession efforts,[136] BiH is determined to implement measures that will ensure a high level of security for its digital networks and information systems. It is obliged to amend its national legislation and implementation under the 2008 Stabilization and Association Agreement signed with the EC,[137] which for instance is directly linked to implementing the Council of Europe Convention on

134 https://www.osce.org/bs/mission-to-bosnia-and-herzegovina/438386
135 https://www.apc.org/es/node/21130
136 http://europa.ba
137 https://ec.europa.eu/commission/presscorner/detail/en/IP_15_5086

Cybercrime (the Budapest Convention)[138] and the EU's General Data Protection Regulation (GDPR).[139] The Budapest Convention offers a general template for countries that are developing their national legislation and cooperation in the fight against cybercrime. Considering the significant gaps that exist in national legislation and its slowness to harmonize legislation, as well as its limited capacities to tackle broader issues related to cybersecurity and in particular those related to human rights, implementing the convention represents an important step forward for BiH.

BiH has also committed to implementing OSCE commitments arising from the decision of the OSCE Ministerial Council to step up efforts to reduce the risk of conflict through the use of information and communication technologies (ICTs), including an agreed package of confidence-building measures (CBMs) to address ICT security in order to increase predictability and transparency and reduce misperceptions and conflicts in cyber domains.[140] However, existing legislation has yet to be fully aligned with the relevant EU acquis.

Domestic legislation in BiH reflects the complex and decentralized structure of the country. Existing legislation at the state level referring to cybersecurity rarely and only partially addresses the relevant issues. By signing up to international agreements and conventions, such as the Convention on Cybercrime and the Stabilization and Association Agreement, BiH is obliged to align its national legislation on information and cybersecurity with these instruments and to establish mechanisms for implementation. However, progress to date on harmonization in the cybersecurity field has been inadequate.

Constitutionally, BiH is composed of two autonomous entities, the Federation of BiH (FBiH) and Republika Srpska (RS), both of which are self-governing and have their own Criminal Codes and Criminal Procedural Codes. Brčko District is a separate self-governing administrative unit which also has its own criminal codes. The legal provisions of Brčko District relevant to cybersecurity and cybercrime are the same as those set out in the Criminal Code FBiH. Above these codes, at the state level, is the Criminal Code of BiH, though this does not address certain cyber-related issues, which have been devolved to the level of criminal legislation in the three smaller entities.

There are eight laws currently in force that contain provisions relevant to Internet or online security: the Law on Electronic Signature of BiH,[141] the Law on Electronic Legal and Business Transactions of BiH,[142] the Law on Prevention of Money Laundering and Terrorist Financing in BiH,[143] the Criminal Code of BiH (criminal offences related to violation of copyright; incitement of national, racial, and religious hatred, discord, and intolerance; corporate liability; attempting and aiding or abetting),[144] the Criminal Procedure Code of BiH (production orders; search and seizure of stored computer data; surveillance and technical recording of telecommunications),[145] the Law on Personal Data Protection of BiH (data security),[146] the Law on Protection of Confidential Data of BiH (protection of classified data),[147] and the Law on Communications of BiH (data security).[148]

---

138 https://www.coe.int/en/web/cybercrime/the-budapest-convention

139 https://eur-lex.europa.eu/eli/reg/2016/679/oj

140 https://www.osce.org/files/f/documents/d/a/227281.pdf

141 https://advokat-prnjavorac.com/zakoni/Zakon_o_elektronskom_potpisu_BiH.pdf

142 https://www.komorabih.ba/wp-content/uploads/2021/10/Zakon-o-elektronskom-pravnom-i-poslovnom-prometu_sluzbeni-glasnik-BiH_88-07.pdf

143 http://msb.gov.ba/PDF/130320191.pdf

144 https://advokat-prnjavorac.com/zakoni/Krivicni_zakon_BiH.pdf

145 https://advokat-prnjavorac.com/zakoni/Zakon_o_krivicnom_postupku_BiH_-_preciscena,_nezvanicna_verzija.pdf

146 http://azlp.ba/propisi/default.aspx?id=1331&langTag=bs-BA

147 http://www.msb.gov.ba/Zakoni/zakoni/default.aspx?id=3403&langTag=bs-BA

148 https://www.rak.ba/hr/legal-bylaws

In BiH, there is no comprehensive law on information security at the state level. Republika Srpska has adopted a Law on Information Security,[149] which sets measures and standards for ensuring information security, addresses the protection of data within the entity's government, and determines bodies for adaptation, implementation, and monitoring of relevant measures. For several years now, there have been efforts in FBiH to introduce a law on the security of networks and information systems. In July 2019, at the suggestion of the federal ministry of internal affairs at a session of the FBiH government, a working group was established to prepare a preliminary draft of the law. A final version of the text of the preliminary draft was published in June 2021.[150]

CYBERSECURITY AND THE HUMAN RIGHTS FRAMEWORK

While it is possible to identify relevant actors in various specific fields, there are still plenty of unknowns when it comes to jurisdiction on a case-by-case basis regarding human rights in the digital space. We are all now cyber-beings to some extent, and we need laws to be both more 'cyber' and more 'human'. In a broad sense, cybersecurity means ways in which individuals, organizations, and institutions are able to reduce the risk of cyber attack. The Computer Security Resource Center defines cybersecurity as 'prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation'.[151]

However, there is no universal definition of cybersecurity. The Association for Progressive Communications (APC) *refers to* the definition developed by the Internet Free and Secure working group of the Freedom Online Coalition (FOC), which was composed of technologists, human rights experts, and government representatives. Inspired by the ISO/IEC 27000 standard on information security,[152] the FOC working group defined cybersecurity as 'the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline'.[153]

In order to ensure that legal and policy frameworks in BiH respond to the needs of the national economy and the public and private sectors and that they protect individual rights, policymakers need to become better acquainted with the pace of global technological development and its effects on security on the one hand and on human rights on the other.

Due to its fragmented administrative structure, BiH faces additional challenges when it comes to how governments, the private sector, and civil society respond to challenges around cybersecurity governance. Legal frameworks need to better respect human rights norms, while at the same time needing to combat increasing levels of cybercrime, cyber attacks, and other activities that employ technology and the Internet as spaces to promote violence and extremism and spread disinformation that undermines the security of individuals, of the nation, and ultimately of democracy.

---

149 https://www.paragraf.rs/propisi/zakon_o_informacionoj_bezbednosti.html

150 http://fmpik.gov.ba/bh/dokumenti/prijedlozi-i-nacrti/finalna-verzija-prednacrt-zakona-o-informacionoj-sigurnosti-fbih-09-06-2021.html

151 https://csrc.nist.gov/glossary/term/cybersecurity

152 https://www.iso.org/isoiec-27001-information-security.html

153 https://freeandsecure.online/definition/

Due to its fragmented administrative structure, BiH faces additional challenges … around cybersecurity governance

Cybersecurity matters so much because being connected to the Internet via our smartphones, laptops, and other gadgets that we live with, work on, and use to shop is an integral part of human life nowadays. We share – knowingly or unknowingly – our personal information online every day. We fall in and out of love – and our devices and our social media accounts follow us every step of the way. We communicate valuable personal and work data, which in certain contexts can put people such as human rights defenders and journalists in great danger.

What happens when cyberspace becomes unsafe, a place of threat, where people feel that they have no protection when their rights are breached, due to a lack of governance? Massive data breaches violate people's right to privacy; and malware targets human rights defenders and journalists. With the COVID-19 pandemic, the world has seen cyber attacks on hospitals and public services. Often draconian cyber laws have been proposed, which can have a chilling effect on freedom of expression, political dissent, and democracy in general. In BiH, policymakers and governments need to start considering the value of a rights-based approach to cybersecurity and Internet governance.

Cybersecurity and the right to privacy

The right to privacy is a basic human right that applies to everyone (with certain exceptional restrictions) and is protected primarily by international instruments such as the Universal Declaration of Human Rights (Article 12)[154] and the European Convention on Human Rights (Article 8).[155] The first binding act passed by the Council of Europe on 28 January 1981 relating to the protection of the right to privacy was the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[156]

In addition to these international acts, all of which BiH has ratified, the right to privacy is protected by provisions in the legislation of the country's constituent entities, as follows:

- The Constitution of BiH[157] in Article II/3 prescribes 'that all persons in the territory of BiH enjoy human rights and freedoms', and under point (f) states the right to a private life, home, and correspondence.
- The Constitution of the Federation of BiH[158] in Article II/A2 describes the rights enjoyed by all persons in the territory of the Federation under item (g), which prescribes the right to privacy.
- Article 13 of the Constitution of the Republika Srpsk[159]a reads: 'Human dignity, physical and spiritual integrity, human privacy, personal and family life are inviolable.'

154 https://www.ohchr.org/en/universal-declaration-of-human-rights
155 https://www.echr.coe.int/documents/convention_eng.pdf
156 https://rm.coe.int/1680078b37
157 https://www.ustavnisud.ba/public/down/USTAV_BOSNE_I_HERCEGOVINE_bos.pdf
158 https://parlamentfbih.gov.ba/dom_naroda/bos/parlament/o_parlamentu/ustavfbih.html
159 https://www.narodnaskupstinars.net/sites/default/files/upload/dokumenti/ustav/lat/ustav_republike_srpske.pdf

Legal theory[160] holds that the right to privacy protects the individual from excessive interference by the state, the public, or other individuals in the realms of spatial, information, and communication privacy.[161]

Spatial privacy refers to the home and other spaces in which a person leads a life separate from others. This is recognized as a constitutional right that guarantees the right to personal and family life, dignity, and physical and spiritual integrity. It allows an individual the right to have their own space in the family home or in the workplace to an extent that provides conditions for the development of their own personality.

Information privacy refers to privacy that relates to the collection of personal data, the management of those data, and their use. This right applies to data that require authorization to be used by third parties. The very act of data breach is an entry into the sphere of privacy, but the damage caused by it concerns the person. In this case, the value that needs to be protected is privacy, because it was not violation of data, but a violation of personality.

Communication privacy refers to personal records, correspondence, or any other form of communication. This is recognized as an inviolable right guaranteed by the Constitution of BiH, with limitations only in specific cases.

The case law of the European Court of Human Rights in Strasbourg has extended the concept of private life to physical and moral integrity, including sexual life (*Judgement in the Case of X and Y v. The Netherlands*[162]). The Constitutional Court of BiH, in *case number Ap-965/17 of 12 March 2019*, has also found that the right to prestige is part of the right to private life.[163]

At the end of 2021 a private video containing what was described as 'pornographic gay content' was published was publicly released and shared widely on different platforms. I.B., a young councilor from the Party of Democratic Progress (PDP) and a member of the Banja Luka City Assembly, endured months of financial blackmail, psychological harassment, and threats to share his private video more widely. The video was sent to journalists and public figures and also circulated in private messages over Viber, Messenger, and other chat applications. I.B. *claimed* that it had been disseminated to the public by political opponents of his party.[164]

While acknowledging that public figures are often more exposed to public attack and that in this case the video was used as a means of cyber-bullying for the purpose of political gain, I.B.'s right to privacy was also breached. He had not spoken publicly about his sexual orientation nor had it previously been publicly discussed in the media. In particular, the video was also sent to his parents whose health, he said, was 'seriously impaired', which ultimately had a negative effect on his own health.

He posted on his private Facebook account (the original post is no longer available): 'Although I believe that everyone has the right to a private life, I am aware of the responsibility I have as a public figure, [and] that is why I am withdrawing from politics, handing over the councillor mandate and leaving the PDP.'

---

160 *https://www.pravobih.com/sudska-zastita-prava-na-privatnost-u-bosni-i-hercegovini-t1159.html*

161 Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu, dr. sci. Marija Boban, Zbornik radova Pravnog fakulteta u Splitu, str. 584., https://hrcak.srce.hr/file/129212

162 *https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57603%22*

163 *https://www.ustavnisud.ba/uploads/documents/praksa-sudova-bih-sloboda-licnosti-i-sloboda-izrazavanja-sl-izrazavanja_1613343807.pdf*

164 *https://www.jutarnji.hr/vijesti/svijet/procurila-porno-snimka-politicara-iz-banja-luke-trazili-su-me-pola-milijuna-maraka-povlacim-se-15131680*

Banja Luka Police Department *confirmed* that I.B. had reported a case of attempted blackmail in relation to this private video in September 2021, before it was widely released, and that a report on the case had been submitted to the Prosecutor's Office in the city.[165] Lejla Huremović, an activist and a member of the Pride organizing committee, told BIRN BiH in an interview for this research that she considers the quick reaction of the police and the judiciary a positive example in this case. However, legally it has not yet been resolved.

The Human Rights Ombudsman of BiH is *of the opinion*[166] that violations of human rights by high-tech means is a challenge for all professionals involved in protecting and promoting human rights and also for every individual, bearing in mind that nowadays such technologies are a normal part of everyday life. Technology is not neutral, especially when it is used specifically to affect people's lives and to erode their rights. Technology as a tool is often used to breach the sphere of private life and it 'become[s] an object through which the right to privacy is violated or a person's safety is threatened'. In such instances, according to international human rights standards, the state is required to provide mechanisms of protection.

Cybersecurity and freedom of expression

Due to BiH's tragic past, involving incitement to war crimes and violence against people based on their nationality and/or religion, it is difficult to discuss freedom of expression without talking about hate speech. Such narratives still exist in BiH society today and divide people on a daily basis, though they often come under the guise of freedom of expression.

> Technical is not neutral, especially when it is used specifically to affect people's lives and to erode their rights

According to the Annual Report on results of the activities of the Institution of the Human Rights Ombudsman of BiH for 2021, in every modern democratic society freedom of access to information is a part of freedom of expression, provides a basis for building a democratic society, and is an inseparable part of the rule of law.[167] In BiH, freedom of access to information is regulated by laws in the country as a whole,[168] in the Federation of BiH,[169] and in Republika Srpska.[170] Freedom of expression meanwhile is regulated in national legislation by the Constitution of BiH,[171] the Constitution of FBiH,[172] and the Constitution of Republika Srpska,[173] as well as by the Law on protection against defamation of the

165 https://www.bl-portal.com/novosti/policija-reagovala-predmet-kod-tuzioca-begic-prije-tri-mjeseca-prijavio-ucjene/
166 https://www.ombudsmen.gov.ba/documents/obmudsmen_doc2021111511252845bos.pdf
167 https://www.ombudsmen.gov.ba/documents/obmudsmen_doc2022041413104027eng.pdf
168 https://advokat-prnjavorac.com/zakoni/ZAKON_O_SLOBODI_PRISTUPA_INFORMACIJAMA.pdf
169 http://www.pufbih.ba/v1/public/upload/zakoni/1e78c-zakon-o-slobodi-pristupa-informacijama-ispravan-tekst.pdf
170 https://advokat-prnjavorac.com/zakoni/Zakon_o_slobodi_pristupa_informacijama_RS.pdf
171 https://www.ustavnisud.ba/public/down/USTAV_BOSNE_I_HERCEGOVINE_engl.pdf
172 https://www.paragraf.ba/propisi/fbih/ustav-federacije-bosne-i-hercegovine.html
173 https://www.narodnaskupstinars.net/sites/default/files/upload/dokumenti/ustav/lat/ustav_republike_srpske.pdf

Federation of BiH[174] and similar laws in Republika Srpska[175] and Brčko District.[176]
The Council of Europe (CoE) defines the term 'hate speech' as 'covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism and other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin'.

The most commonly used form of hate speech in BiH is denial of genocide (in particular events at Srebrenica) and other war crimes determined by the courts. Most of those who express such opinions, both in the mainstream media and on social media, cite their right to freedom to expression. This was the main reason why in July 2021 Valentin Inzko, the outgoing High Representative of BiH, in one of his last official acts used his powers to impose amendments to the country's criminal code that banned the denial of genocide and the glorification of war criminals.[177] This decision was met with anger from some officials from the Republika Srpska entity, such as Dušica Šolaja, representative in the National Assembly, who *claimed* that the establishment of such a legal norm would restrict basic human rights to freedom of thought and expression.[178]

Among the most important international documents regulating freedom of expression are the Universal Declaration of Human Rights,[179] specifically Article 19, and the European Convention on Human Rights, Article 10.[180] BiH has ratified all major international acts directly and indirectly related to freedom of expression and the prohibition of hate speech.

The country's legal framework does not include regulations directly related to the prohibition of hate speech on the Internet, but this issue can be seen in the context of provisions in the criminal codes of BiH, the Federation of BiH, Brčko District, and Republika Srpska that prohibit incitement to national, racial, and religious hatred, discord, and intolerance.

The line between freedom of expression and hate speech is frequently blurred. This poses a threat to freedoms such as freedom of expression when there is no proper consideration of (all) human rights or consideration of the Internet in all its complexity.

In March 2020 lawmaker Damir Marjanović of Sarajevo Canton put forward a *draft law* aimed at sanctioning hate speech in public, including via 'computer system or network', specifically in that canton.[181] Marjanović noted that people were 'currently being insulted with impunity'. The argument that it would help prevent radicalization and violence that might pose a threat to national security was also *put forward* in justification of such a law.[182]

The law proposed to ban hate speech and punish offenders with terms of between six months and five years in prison. It stated, for example, that '[w]hoever organizes or leads a group of three or more

---

174 https://advokat-prnjavorac.com/legislation/Law-on-protection-against-defamation-of-the-Federation-Bosnia-and-Herzegovina.pdf

175 https://advokat-prnjavorac.com/zakoni/Zakon-o-zastiti-od-klevete-Republike-Srpske.pdf

176 https://advokat-prnjavorac.com/zakoni/Zakon-o-zastiti-od-klevete-Brcko-distrikta-BiH.pdf

177 https://detektor.ba/2021/07/23/inzko-nametnuo-izmjene-i-dopune-krivicnog-zakona-kojima-se-zabranjuje-negiranje-genocida/?lang=en

178 https://zastone.ba/da-li-zabrana-negiranja-genocida-ugrozava-osnovna-ljudska-prava/

179 https://www.un.org/en/about-us/universal-declaration-of-human-rights

180 https://www.echr.coe.int/documents/convention_eng.pdf

181 https://skupstina.ks.gov.ba/sites/skupstina.ks.gov.ba/files/zakon_kaznjavanje_govora_mrznje.pdf?utm_source=Klix.ba&utm_medium=Clanak

182 https://balkaninsight.com/2019/09/20/sarajevo-politician-champions-legislation-to-outlaw-hate-speech/

persons for the purpose of committing the act referred to in paragraph 1 of this Article shall be punished by imprisonment for a term between six months and five years', and also '[w]hoever participates in the association referred to in paragraph 2 of this Article shall be punished by imprisonment for a term not exceeding one year'.

During a *public debate* on this draft law and the issue of hate speech masquerading as freedom of expression, Irfan Čengić, a member of the House of Representatives in the Parliament of FBiH, said that hate speech on the Internet should be included in the Law on Public Order and Peace. 'It should be added that the Internet is a public space,' he remarked, noting that this was already the practice in Republika Srpska.[183] During the same debate, the Minister of Internal Affairs of the Sarajevo Canton, Admir Katica, said that "Sarajevo Canton is moving towards declaring the Internet a public space, and that they are already considering hate speech as a security threat".

However, in September 2021 *the draft was withdrawn* by the Assembly of Sarajevo Canton, with a unanimous decision to pursue a joint initiative at a higher, federal level.

As one of its larger initiatives in tracking the widespread phenomenon of hate speech, discriminatory speech, and, specifically in the context of BiH, the denial of genocide and other war crimes, in December 2021 BIRN BiH launched the Mapping Hate database.[184] The database maps incidents involving different types of hate speech and focuses on public officials or public figures who, due to their position, have large platforms at their disposal, either via mainstream media or online through social media accounts, and are using these channels to spread discriminatory and/or hate speech, deny court-determined war crimes including genocide, or provoke controversy in BiH.

The database contains examples of both 'lawful' and 'unlawful' hate speech,[185] which are mostly the words of politicians and/or public officials that are then further disseminated by their supporters and by online bots, ultimately influencing citizens to take polarized 'left or right' stances on their own social media accounts.

The cases described below are all examples that involve freedom of speech closely bound up with discrimination and/or hate speech. All of these cases have provoked action by the state apparatus, in particular the Prosecutor's Office; in some of them the courts have already delivered a verdict, which enables us to examine the process and the logic behind it.

First, in March 2022, at a time when the national public broadcaster Radio and Television of Bosnia and Herzegovina (BHRT) was facing a difficult financial situation and much political pressure, Rajko Vasić, a politician from the Alliance of Independent Social Democrats (SNSD), a political party in Republika Srpska, sent a tweet which read: 'BHRT – survival or ruin? Vasić. If you are uncomfortable, I will come and blow it up with a mine.'[186] Following a public outcry and numerous complaints to Twitter, the platform deleted the post, ruling that it violated its guidelines.

Meanwhile Damir Arnaut, a member of the House of the Representatives in the BiH Parliament, filed a criminal complaint against Vasić, alleging terrorism on the grounds of making a threat against the media

183 https://detektor.ba/2021/11/23/digitalni-svijet-izmedju-slobode-izrazavanja-i-govora-mrznje-proglasiti-internet-javnim-prostorom/

184 https://mapiranjemrznje.detektor.ba/

185 https://www.article19.org/resources/hate-speech-explained-a-summary/

186 https://mapiranjemrznje.detektor.ba/articles/hate/33-rajko-vasi%25C4%2587-na-twitteru-prijetio-miniranjem-bhrt-a

via Twitter.[187] In his criminal complaint, Arnaut, a lawyer by profession, invoked the country's criminal law and specifically the criminal offence of terrorism. He pointed out that, with the tweet, Vasić had posted a photo clearly showing the building of the public broadcaster and leaving no doubt as to what place, object, media, and ultimately people he was referring to when making the public threat. The complaint stated: "[...] the BHRT building is clearly [an] object belonging to Bosnia and Herzegovina therefore without a doubt [it] is a public object, as well as an infrastructural object including an informational system, therefore blowing up with a mine such [an] object – which Rajko Vasić threatened [to do] – would cause great damage and is very likely to endanger human life or cause economic damage."

Arnaut confirmed that he was invited to give a statement to the Federal Police Administration regarding the criminal charges, adding: "I have no doubt that this constitutes a criminal offence of terrorism, as prescribed by the BiH Criminal Code. Namely, under the Code, that offence involves not only blowing up a significant government or public target, with the goal of intimidation, but threatening to do so as well. The fact that the threat was made online, where the intimidation effect is exponentially greater, makes it that much more serious."

"Due to the fact that a small number of domestic laws explicitly mention cyber space as such, a general feeling is that the offences committed in the digital space or through technological means are unregulated or insufficiently regulated. However, unlawful activities remain unlawful, regardless of the manner, venue or tools used to commit them."

As a result, this solely means that it is necessary to approach such cases with a broader interpretation of regulations, and to accept the fact that all illegal activities should be sanctioned, regardless of where they are committed, said Arnaut for the purpose of this research.

A similar criminal complaint has been filed by BHRT's management. BIRN BiH also contacted the Prosecutor's Office, which confirmed that it had opened a file on the case. Meanwhile, Vasić deleted his tweet, though it is archived on BIRN BiH's Mapping Hate database.[188]

Another case which caused a stir and which combines these two issues – freedom of expression and anti-discrimination online – involves a web portal called 'antimigrant.ba'. During the migration crisis of recent years, BiH became a hotspot on the so-called Western Balkan route as it borders Croatia, an EU country. When the crisis began, the Internet became the place of choice in BiH – and also a relatively safe space – for those spreading hatred towards the migrant population and people on the move. Numerous websites engaged in unprofessional reporting and the spread of hatred. One of these was the antimigrant.ba portal, which was set up by journalist Fatmir Alispahić.

An indictment was brought against Alispahić in the Court of of BiH in September 2021 after the antimigrant.ba portal and its social media accounts had published a constant stream of articles and videos in 2019 and 2020 that encouraged the spread of hatred against migrants and the migrant population in general, as well as against the constituent peoples of BiH. In November 2021, however, announcing its first instance verdict, the State Court acquitted Alispahić of charges of inciting national, religious, and racial hatred, discord, and intolerance through the content published on the portal.[189] It considered that all the statements and claims made fell within the scope of freedom of thought and of speech, and ruled that migrants were not an object of criminal protection at the state level and that state law did not proscribe all forms of hate speech (unlike the Criminal Code of Republika Srpska).

---

187 https://radiosarajevo.ba/vijesti/bosna-i-hercegovina/arnaut-podnio-krivicnu-prijavu-protiv-clana-snsd-a-koji-moze-da-minira-bhrt/451729

188 https://mapiranjemrznje.detektor.ba/articles/hate/33-rajko-vasi%C4%87-na-twitteru-prijetio-miniranjem-bhrt-a

189 https://detektor.ba/2021/11/19/fatmir-alispahic-oslobodjen-optuzbe-za-izazivanje-mrznje/

The judge stated that Alispahić had been acquitted because the prosecution had not proved that he had incited hatred against constituent peoples of BiH and migrants and because the indictment erroneously referred to the application of international mechanisms. Neither, he said, had the prosecution determined exactly which allegations he should be charged with, with the indictment containing 180 allegations. The duty of the Court was to analyse all allegations involving constituent people and migrants, in order to identify statements that arguably constituted hate speech.

In March 2022, the State Prosecutor's Office lodged an appeal against the acquittal before the Appellate Chamber, arguing that the verdict should be revoked or amended and that Alispahić should be found guilty.[190] The prosecutor stated: 'We still believe and claim that the first instance court passed a verdict that is contrary to the facts, i.e. the evidence presented, [...] These [articles] that have been published really point to more than hate speech. We also referred to certain conventions for the protection of human rights, which we mentioned during our closing arguments.' He added that the prosecution believed that with this verdict the Court had set a precedent for future cases of this nature. Finally, however, in April 2022 the Appellate Chamber also acquitted Alispahić of the charges of inciting national, religious, and racial hatred, discord, and intolerance by means of the articles he published.[191]

The court did not discuss the issue of the domain name 'antimigrant' being registered on the national top-level domain (TLD) '.ba'. The University Tele-Informatics Centre (UTIC) administers the .ba domain, which was awarded to BiH in 1996 by the Internet Assigned Numbers Authority (IANA), which is now managed by the International Corporation for Assigned Names and Numbers (ICANN). Regulations on the use of the .ba domain name are set out in the Rulebook on General Conditions for Registration and Use of Domain Names under the Bosnian-Herzegovinian Internet Domain .ba.[192] Article 30 of the Rulebook ('Rights and obligations') clearly states under point (b) that 'the registrant is obliged to use the domain name in a way that does not violate the laws and other regulations of the state of Bosnia and Herzegovina, does not violate the rights of third parties, and respects the principle of prohibition of discrimination on any grounds'.

The antimigrant.ba website is hosted by US-based company, domain name registrar Namecheap, Inc. Theoretically, and in general terms, it would be possible to make a complaint to the hosting provider, as well as to the registry, to establish 'evidence of harm' done by the website. However, domain name professionals warn that this can be a lengthy process.

Another case where the courts decided that the actions of a defendant were covered by the principle of freedom of speech was that of *Jasmin Mulahusić*, who was investigated by the Prosecutor's Office after posting messages deemed to be insulting on national and religious grounds on his social media profiles and on the Internet over a long period of time. Some media reports referred to him as the 'Internet warrior' or 'Internet raider'.[193]

According to the Prosecutor's Office, Mulahusić had made and posted various photo and video montages that spread national and religious hatred and intolerance against the people of BiH on a number of Facebook profiles in 2020 and 2021. It also alleged that he was linked to people who had connections with terrorist organizations. It requested that he be taken into custody due to the danger of him absconding and the risk that, by remaining at large, he could obstruct the investigation, conceal evidence,

190 *https://detektor.ba/2022/03/31/tuzilastvo-u-zalbi-trazi-ukidanje-oslobadjajuce-presude-fatmiru-alispahicu/*

191 *https://detektor.ba/2022/04/15/fatmir-alispahic-pravosnazno-oslobodjen-optuzbi-za-izazivanje-mrznje/*

192 *https://nic.ba/doc/Pravilnik_o_opstim_uslovima.pdf*

193 *https://detektor.ba/2021/09/06/predlozen-pritvor-za-jasmina-mulahusica-osumnjicenog-za-izazivanje-nacionalne-i-vjerske-mrznje-i-netrpeljivosti/*

and influence witnesses or accomplices, as well as continue to post offensive material. However, the Court rejected this because it was not convinced of 'the existence of the criminal offence for which Mulahusić is charged from the submitted motion and evidence of the Prosecution'.[194] The prosecutor confirmed to BIRN BiH that the Court believed that this was 'a matter of freedom of speech'.

This issue can also be looked at from a different angle. According to Vanja Stokić, an activist, journalist, and editor-in-chief at independent news website eTrafika, one of the main challenges for people who speak out publicly on controversial topics is that they face organized witch hunts, 'especially on social networks where the entire campaign is aimed at discrediting them so that no one takes them seriously anymore'. She herself received threats from an unknown man, who said he would 'cut off my head'. The Prosecutor's Office, however, judged that there were no grounds for criminal prosecution in this case and described it as an expression of personal attitudes and dissatisfaction with her work.

Cybersecurity and freedom of peaceful assembly and association

Freedom of peaceful assembly and association is guaranteed by numerous international and European conventions, including the Universal Declaration of Human Rights and the European Convention on Human Rights. The right to freedom of peaceful assembly is also guaranteed by the constitutions of the state entities in BiH, the Brčko District Statute, and the legal regulations of numerous cantons and other entities. The Constitution of FBiH does not directly regulate this right but states that the federal government and the cantons are responsible for guaranteeing and enforcing human rights,[195] while the Constitution of Republika Srpska states that 'citizens have the right to peaceful assembly and public protest'.[196] Relevant laws on assembly also exist at the cantonal level. The Statute of the Brčko District of BiH states that 'everyone has the right to freedom of peaceful assembly and association',[197] and in July 2020 the Brčko District Assembly adopted the Law on Peaceful Assembly.[198]

The easiest way nowadays for citizens to learn about and be invited to a peaceful assembly or association is through social networks, since notifications shared online are the quickest way to reach large numbers of people. However, technology also makes it easier for police officers to identify and target participants in gatherings, who frequently are detained for no good reason or because they have attempted to express an opinion. It is important to point out here that freedom of assembly is often associated with freedom of expression.

The Sarajevo Pride march, first held in 2019, can be characterized as a high-risk gathering. Lejla Huremović, an activist and a member of the Pride organizing committee, reported that challenges around freedom of assembly include digital attacks online. She said: 'The biggest challenge is to keep the website, social profiles related to Pride, and the private profiles of members safe and protected from hacking.' There have been (unsuccessful) attempts to hack into the organization's website as well as into the private profiles of members. The main challenge is to protect members from exposure to hacking and identity theft and to safeguard their personal information. As Huremović explained: 'Disclosure of personal information is especially important for LGBTIQA+ people who have not come out publicly as LGBTIQA+.

194 https://detektor.ba/2021/09/07/jasmin-mulahusic-pusten-na-slobodu/

195 https://www.paragraf.ba/propisi/fbih/ustav-federacije-bosne-i-hercegovine.html

196 https://www.narodnaskupstinars.net/sites/default/files/upload/dokumenti/ustav/lat/ustav_republike_srpske.pdf

197 https://advokat-prnjavorac.com/legislation/Statute-of-the-Brcko-Distrikt-of-Bosnia-and-Herzegovina.pdf

198 https://skupstinabd.ba/3-zakon/ba/Zakon%20o%20mirnom%20okupljanju/01B29-20%20Zakon%20o%20mirnom%20okupljanju.pdf

Identity blackmail is also common.'

The death in March 2018 of David Dragičević, a 21-year-old student from Banja Luka, sparked some of the largest protests in BiH's history, and the case highlights concerns about surveillance affecting people's right to association and to protest. David had been reported missing after a night out; his body was found six days later in a stream, and the police investigation declared that his death was an accident. However, his family believe that he was murdered and that the Republika Srpska police and prosecutor's office are covering up what really happened. A Facebook group, *'Pravda za Davida'* ('Justice for David') has over 225,000 followers.[199] The group publishes updates on legal developments in the case, and also invites people to take part in public protests. However, during a rally in 2018 in Rogatica those taking part *noticed concealed cameras* in the windows of the town hall.[200]

In 2019 the Initiative for Monitoring the EU Integration of BiH[201] published a report entitled *Alternative Report on the Application of Bosnia and Herzegovina for Membership in the European Union 2019: Political Criteria*,[202] which dedicated a whole section to the Pravda za Davida protests. It noted that cameras were set up at protests and that recordings were used to identify protesters, who were then subject to surveillance and wiretapping. Personal details about some of the protesters were also publicly shared in the media. The report said: 'Members of the group and those who supported the protests witnessed pressures such as surveillance, wiretapping, identification from wearing clothing with protest slogans in various cities in the RS, etc. In July, on the eve of the second large gathering, cameras were set up on Krajina Square to record all events at the site that day, and there are reasonable suspicions that the footage was used to identify and to put pressure on protesters. Thus, for example, RTRS [Radio Television of Republika Srpska] published a list with the names, surnames, personal numbers, and residential addresses of about thirty people who participated in the protests. The list undoubtedly came from police sources, especially since some of the people whose data were published had criminal or misdemeanor police "files", which was then used to present the protests as "criminal". After public condemnation of such a call for lynching, RTRS removed the article from its website, but it remained available on the portal of the news agency Srna and on other media that transmitted it, with illegally published personal data.'

In August 2018 Slobodan Vasković, a columnist who had followed the case of David Dragičević from the very beginning, often revealing details that no other outlets had published, wrote a column claiming that the head of the Prevention Unit in the Anti-Terrorism Directorate, Dejan Mitrić, had continued to authorize illegal wiretapping: 'Mitrić's unit monitors phones, and in order to do so, he labelled the most important people from the "Justice for David" group as "terrorists". Some inspectors rebelled against Mitrić, because he illegally monitored phone numbers of people from the "Justice for David" group. Some of them wrote official notes on those circumstances, but that did not stop Mitrić from continuing his dirty work [...]'.[203]

In October 2018, Radio Slobodna Evropa *published an article* about the presence of cameras during a gathering of activists, reporting that 'Armoured police combat vehicles are present in Banja Luka, and police officers are also hidden in the facilities around Krajina Square, where they are filming with cameras and monitoring the situation.'[204] Activist Daniela Ratešić Došen *claimed* that during the rally in Banja Luka the police illegally followed members of the group, and described how they monitored their movements by

199 https://www.facebook.com/pravdazadavidadragicevica

200 https://infomediabalkan.com/ko-je-spijunirao-pravdu-za-davida-skrivene-kamere-u-rogatici-banja-luci-video

201 https://eu-monitoring.ba/en/

202 https://eu-monitoring.ba/site/wp-content/uploads/2019/04/alternativni_bhs-1.pdf

203 https://slobodanvaskovic.blogspot.com/2018/08/mitric-visoki-funkcioner-mup-rs-vodece.html

204 https://www.slobodnaevropa.org/a/29527766.html

sending fake text messages via mobile phone.[205]

The alleged murder of David Dragičević has still not been examined in a court. The pressure put on protestors through digital survaillance, in particular on those organizing protests, with the aim of intimidating them, has never been subject to any legal procedures either.

Cybersecurity and anti-discrimination

The prohibition of discrimination in BiH is regulated by numerous legal acts, from international to domestic legal frameworks. The country is a signatory to numerous international documents in the field of human rights and is obliged to carry out activities to fulfil its commitments. The following international United Nations agreements, to which BiH is a signatory, contain provisions on non-discrimination:

- *Convention on the Elimination of All Forms of Racial Discrimination* (CERD)[206]
- *Convention on the Elimination of All Forms of Discrimination against Women* (CEDAW)[207]
- *Convention for the Protection of the Rights of All Migrant Workers and Members of Their Families*[208]
- *Convention on the Rights of the Child* (CRC)[209]
- *Convention on the Rights of Persons with Disabilities* (CRPD)[210]
- *International Covenant on Civil and Political Rights* (ICCPR)[211]
- *International Covenant on Economic, Social and Cultural Rights* (ICESCR)[212]
- *Universal Declaration of Human Rights* (UDHR)[213]
- *UNESCO Convention against Discrimination in Education.*[214]

Fourteen UN Committees have been established under specific provisions of these conventions as mechanisms for monitoring their implementation. Other bodies within the UN system with responsibility for monitoring human rights and discrimination include the Human Rights Council, through Universal Periodic Reviews (UPRs) and Special Procedures.

---

205 https://www.klix.ba/vijesti/bih/danijela-ratesic-dosen-policija-je-nelegalno-pratila-clanove-grupe-pravda-za-davida/181108124

206 https://legal.un.org/avl/pdf/ha/cerd/cerd_e.pdf

207 https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women

208 https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-protection-rights-all-migrant-workers

209 https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

210 https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities

211 https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

212 https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights

213 https://www.ohchr.org/en/universal-declaration-of-human-rights

214 http://portal.unesco.org/en/ev.php-URL_ID=12949&URL_DO=DO_TOPIC&URL_SECTION=201.html

Mechanisms for the protection of human rights and non-discrimination under the Council of Europe include the European Convention on Human Rights and its Protocols and other agreements to which BiH is a signatory, such as Protocol 12 to the Convention, which calls for the prohibition of discrimination.

Domestically, laws which define discrimination are the *Law on Prohibition of Discrimination*[215] and the *Law on Gender Equality in BiH*.[216] The Law on Gender Equality of BiH regulates, promotes, and protects gender equality, guarantees equal opportunities and equal treatment of all persons, regardless of their gender, in the public and private spheres, and regulates protection against discrimination. Article 2, paragraph 3 clearly prohibits discrimination based on gender and sexual orientation. The Law on Prohibition of Discrimination provides for special protection mechanisms and outlines activities aimed at combating and eliminating discrimination, primarily procedures for bringing complaints before the Ombudsman, as well as appropriate judicial and administrative procedures. The Law on Gender Equality explicitly prohibits direct and indirect discrimination on the grounds of sex or sexual orientation and prohibits harassment, sexual harassment, and incitement to discrimination. It also prohibits gender-based violence (GBV) in the public and private spheres of life, as well as victimization.

Under the Law on Prohibition of Discrimination, the main institution for protection against discrimination, or de facto equality body, is the *Institution of the Human Rights Ombudsman of BiH*.[217] The law also sets out the role of the Ministry of Human Rights and Refugees in preventing and combating discrimination. Mechanisms for protection against gender discrimination under the Law on Gender Equality are the *BiH Agency for Gender Equality*,[218] the *RS Gender Center*,[219] and the *FBiH Gender Center*.[220] Both laws determine the possibility of judicial protection, for which special procedures are prescribed.

The domestic legal framework in BiH still does not recognize discrimination on the Internet per se. However, on 26 April 2022, for the first time a (first instance) judgement for discrimination against LGBTIQA+ persons was confirmed by the Municipal Court in Sarajevo.[221] A former member of the Sarajevo Canton Assembly, Samra Ćosović Hajdarević, had written a public statement on her Facebook page, in reaction to the announcement of the first Pride March in BiH in 2019. She said: 'State! You have no right to complain until you improve the situation of the people. A small group of 15 activists from Prijedor, Banja Luka, Sarajevo, Bijeljina, Tuzla, and other parts of BiH earned prominence and significance. Fifteen of them are sufficient to launch an initiative and organize so-called Pride marches aimed at destroying the state and its people.

'Everyone has the right to live their lives as they like**,** but we also have the right to choose who we want to live with. I want people like these to be isolated and put away from our children and society. Let them go somewhere else and make a city, a state, and a law for themselves, and their own rights that no one will dispute. But NOT here!'

In a public statement immediately after the judgment was announced, Lejla Huremović of the Pride March organizing committee, said: 'This verdict is very important because it has been proven that spreading hate speech and calling for violence against LGBTIQ+ persons in the online sphere (social networks) can also [more widely] affect the quality of life of LGBTIQ+ persons, or lead to physical violence. This is a confirmation that hate speech and incitement to violence on social networks, especially by public figures

215 https://advokat-prnjavorac.com/zakoni/Zakon-o-zabrani-diskriminacije-u-BiH.pdf
216 https://www.gcfbih.gov.ba/wp-content/uploads/2014/01/ZoRS_32_10_H.pdf
217 https://www.ombudsmen.gov.ba/Default.aspx?id=0&lang=EN
218 https://arsbih.gov.ba/
219 https://www.ravnopravnors.com/
220 https://www.gcfbih.gov.ba/
221 https://soc.ba/en/the-first-judgement-for-discrimination-against-lgbti-persons/

and politicians, are not permissible and can be sanctioned. In the spirit of this year's BiH Pride March, which is on June 25, let this verdict be a warning to everyone that every [instance of] hate speech and call for violence will be reported and that we will expect the same verdict.'

For this research, and before the verdict was announced, we spoke with Huremović about the discrimination and hate speech that she and others involved in Pride were facing, as well as about issues of freedom of assembly related to the first BiH Pride march. She said that the threats they had encountered online included incitement to violence and that they all constituted hate speech – and they had all been reported. She added: 'We know that the police invited certain people for interviews during the organization of the Pride parade, but we do not have much information about the outcome of these cases.'

WAYS FORWARD

Due to the complex legal and judicial system of BiH, citizens face barriers in seeking redress through the formal justice system. Their rights are often not fully realized, which leads to a lack of trust in the legal system and the rule of law. Based on the challenges faced during the preparation of this policy paper and the findings of the research, we make the following recommendations for action by various stakeholders in order to improve the realization of human rights in cyberspace, and for BiH to be better prepared for cyber attacks which affect the country as a whole, its institutions and its economy, all the way down t individual lives.

Legislators and public policymakers:

- Legislators and public policymakers need to raise the profile of cybersecurity and issues relating to human rights in public policy debates. They need to gather relevant information and gain a better understanding of the correlations between cybersecurity and human rights in order to inform policy discussions and enable them to propose laws and policies which better fit current needs.
- Laws and policies need to be formulated to take account of cyber and human rights norms at all levels in BiH, including at the national level.
- Legislators must work cooperatively to adopt a national cybersecurity strategy, in order to avoid BiH lagging behind in a challenging environment in which cyber attacks are on the rise.

Government agencies and institutions:

- Institutions need to be more open to collaborating and communicating with the public and with the media, with the aim of better serving the public.
- They should also collaborate to a greater extent with other institutions in the region and elsewhere in Europe in order to learn from good practice and be better equipped to develop the processes that are needed.
- Better coordination with other relevant organizations throughout the country, at all levels and in all areas, is of key importance. This includes seeking information from and working in coordination with

NGOs, human rights groups, journalists, and intergovernmental organizations in BiH that work in the fields of human rights and freedoms, security, and cybersecurity.

- A national CERT needs to be set up as soon as possible.

Prosecutors and the judiciary:

- Prosecutors and judges need to undergo specialized training (if possible to be provided by the international community and based, for example, on EU practice) in order to better understand the challenges involved in regulating cyberspace and the importance of upholding people's rights when they are breached.
- Training topics should include human rights, especially gender and minority rights, as well as general information on the functioning of the Internet and cyber norms – since policy discussions and media coverage often apply the term "cyber norm" to policy instruments that are not in fact norms. BiH needs governance measures to better regulate cyberspace.

Nonprofit organizations, civil society, and the media:

- Civil society and the media, and individuals who work at the intersection of human rights and digital and cybersecurity, need to form alliances to work on strengthening the awareness and capacities of other organizations.
- More public campaigns by civil society and media are needed on the importance of cybersecurity and how it affects people's lives. Partners in this alliance need to work hand in hand to put pressure on policymakers and legislators, by providing them with information from the field, to get more involved in advocating for proposing laws which have both human and state security in cyberspace in mind.
- BiH currently lacks a database of breaches of human rights in the digital sphere. This could be one of the first steps for such an alliance to work on, in order to provide substantive data on cases of breaches in BiH.

As a general conclusion and recommendation, BiH needs a space for dialogue where all relevant actors are able to come together, connect and share their challenges, set goals, and work together to find solutions that work best for everyone. Such space could be provided either by relaunching the dormant Internet Governance Forum or by creating a new space such as an open forum, with annual meetings and activities to be conducted throughout the year.

CHAPTER 3

KOSOVO

Strengthening New Foundations and Institutions

By Lulzim Peci and Valdrin Ukshini | Kosovar Institute for Research and Development (KIPRED)

CHAPTER 3

KOSOVO – STRENGTHENING NEW FOUNDATIONS AND INSTITUTIONS

INTRODUCTION

This paper maps the key human rights challenges in relation to cybersecurity in Kosovo to identify the critical issues that require intervention and possible improvements. For this purpose, this study focuses on cybersecurity dimensions in relation to specific human rights.

The paper is divided into three main parts: the cybersecurity context in Kosovo; cybersecurity and human rights, with a particular focus on the right to privacy, freedom of expression, freedom of assembly and association, and anti-discrimination; and recommendations. The first section provides a brief overview of relevant legislation, policies, and stakeholders. The second section explores the extent to which cybersecurity in Kosovo conforms with international human rights standards and the level of coordination between different institutions involved in safeguarding these rights in practice. The paper concludes by offering recommendations and specific suggestions for improving the legal and policy frameworks related to cybersecurity and human rights in Kosovo.

This research endeavour is heavily based on the following primary sources: the legal framework of Kosovo, opinions of the Venice Commission, and documents of the Council of Europe; official reports of the European Union (EU) and the US State Department; and interviews with representatives of the Ministry of Interior Affairs, Ministry of Justice, Ministry of Defence, Ministry of Economy, Kosovo Police, Ombudsperson Institution of Kosovo (OIK), Agency for Information and Privacy, and the National Computer Security Unit (KOS-CERT), as well as with one expert from academia and two experts from civil society. This study has also used a number of secondary sources such as research reports and media reporting.

CYBERSECURITY CONTEXT IN KOSOVO

This section provides an overview of laws, policies, strategies, and stakeholders related to cybersecurity in Koso vo. It examines the main institutions responsible for cybersecurity, their roles, and the level of cooperation among different actors – including both state and non-state stakeholders.

Prior to the Declaration of Independence in February 2008, a cybersecurity legal and policy framework essentially did not exist in Kosovo. The framework began to be developed during the first few years of independence and is still evolving. In this regard, the first legal act adopted by the Assembly of Kosovo,

on 10 June 2010, was the Law on Prevention and Fight Against Cybercrime.[222] This law provides the legal basis for preventing and combating cybercrime and sanctioning violations, by adhering to human rights and safeguarding personal data.[223] It defines cybercrime as a criminal activity carried out in a network, that has as an objective, or which involves in the way in which it is carried out, the misuse of computer systems and computer data.[224]

The Assembly of Kosovo adopted two cybersecurity-related laws in 2012. The Law on Information Society Services, adopted on 15 March 2012,[225] regulates electronic services (e-commerce, e-payment, e-banking, e-government, and e-procurement) and the use of electronic signatures by the Kosovo government, businesses, and citizens. The law aims to reduce potential problems and abuses pertaining to electronic transactions, as well as to protect the security of information systems.[226] In addition, the Law on Electronic Communications, adopted on 4 October 2012,[227] provides legal norms for the use of electronic communications, and ensures the protection of personal data and the right to privacy in this area.[228]

Another legal act promulgated in 2012 by the Assembly of Kosovo pertaining to cybersecurity is the Law on Interception of Electronic Communications, which was enacted on 28 May 2015.[229] This law filled an important gap in cybersecurity governance and human rights in Kosovo by regulating the procedures and conditions for the interception of electronic communications related to criminal procedure, national security, and the safety of its citizens. The law defines the obligations and responsibilities of the respective state institutions in relation to lawful interception – including procedures for overseeing its implementation – and safeguarding human rights and freedoms.[230]

Furthermore, the Law on Critical Infrastructure, adopted by the Assembly of Kosovo on 30 March 2018,[231] provides legal provisions for the regulation of critical infrastructure in Kosovo. It identifies relevant sectors, provides guidance on how to manage them, and defines penalties for non-compliance.[232] In this regard, the law identifies information and communication technology (ICT) as a critical infrastructure sector, among others.[233] The Law on the Protection of Personal Data, enacted by the Assembly of Kosovo on 30 January 2019,[234] was the last legal act adopted in relation to cybersecurity governance in Kosovo. The law defines legal protection, institutional responsibilities for monitoring the legality of data processing and access to public documents, and sanctions related to the protection of personal data and privacy of

222 Official Gazette of the Republic of Kosovo, Law on Prevention and Fight Against Cyber Crime (Law No. 03/L –166), 20 July 2010.

223 Ibid., art. 1.

224 Ibid., art. 3.1.

225 Official Gazette of the Republic of Kosovo, Law on Information Society Services (Law No. 04/L-094), 11 April 2012.

226 Ibid., art 1.

227 Official Gazette of the Republic of Kosovo, Law on Electronic Communications (Law No. 04/L-109), 9 November 2012.

228 Ibid., art. 2.

229 Official Gazette of the Republic of Kosovo, Law on Interception of Electronic Communications (Law No. 05/L-030), 13 July 2015.

230 Ibid., art. 1.

231 Official Gazette of the Republic of Kosovo, Law on Critical Infrastructure (Law No. 06/L – 014), 27 April 2018.

232 Ibid., art. 2.

233 Ibid., art. 5.2.7.

234 Official Gazette of the Republic of Kosovo, Law on Protection of Personal Data (Law No. 06/L – 082), 25 February 2019.

individuals.[235] This law also complies with the EU Commission's Directive 95/46/EC on the General Data Protection Regulation.[236]

The previous Kosovo government had prepared the new Draft Law on Cybersecurity in 2020;[237] however, owing to the extraordinary elections of February 2021, the law has not yet been adopted by the Kosovo Assembly.

The first policy related to cybersecurity in Kosovo – the Electronic and Communication Sector Policy – Digital Agenda for Kosova 2013-2020 – was drafted in March 2013 by the then Ministry of Economy[238] and had the following objectives: to develop ICT; to develop electronic content and services, and promote its use; and to enable Kosovo residents to use ICTs.[239] The key outcome of this document concerning cybersecurity was the establishment of the national Computer Emergency Response Team (CERT) responsible for investigating security incidents related to electronic communications networks and services.[240]

The National Cybersecurity Strategy and Action Plan … underlines that public and private authorities must guarantee basic rights and liberties in cyberspace

Against this background, the National Cybersecurity Strategy and Action Plan 2016-2019 is the most important policy document adopted by the Kosovo Government to date. It aims to ensure a safe cyberspace environment by minimizing and preventing cyber threats in cooperation with national and international partners.[241] The strategy underlines that public and private authorities must guarantee basic rights and liberties in cyberspace and that government measures to protect and guarantee national cybersecurity should respect fundamental rights and liberties, including rights to privacy, free access to information, and 'other democratic principles'.[242] Furthermore, one of the strategy's key principles is to ensure human rights and freedoms and assure cybersecurity by 'respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information, and identity regardless of ethnicity, gender, age, religion throughout all stages'.[243] As far as practical implementation is concerned, however, the strategy's action plan does not envisage any activity related to this dimension of cybersecurity. Although, according to public information provided by the Ministry of Internal Affairs on 4 February 2019, more than 70 per cent of the activities envisaged by the action plan were implemented,[244] there is no information about evaluating implementation of the strategy after this date.

The National Cyber Security Strategy laid the foundations for cybersecurity governance in Kosovo. First and foremost, it envisaged the creation of the post of National Cybersecurity Coordinator, as well as the National Cyber Security Council (NCSC), to strengthen multi-stakeholder involvement and coordination in relation to 'cyberspace' security. The NCSC aims to strengthen cooperation both within

235 Ibid., art. 1.

236 Ibid., art. 2.

237 Government of Kosovo, *Draft Law on Cybersecurity*, 17 July 2020..

238 Ministry of Economy, Electronic and Communication Sector Policy: Digital Agenda for Kosovo 2013-2020, March 2013.

239 Ibid., pp. 3-4.

240 Ibid., p. 33.

241 Ministry of Internal Affairs, National Cybersecurity Strategy and Action Plan 2016-2019, December 2015, p. 2.

242 Ibid., p. 12.

243 Ibid. p. 13.

244 Ministry of Internal Affairs, *Këshillit Shtetëror për Siguri Kibernetike ka vlerësuar zbatimin e strategjisë shtetërore për siguri kibernetike*, 4 February 2019.

the government and with the private sector, and to provide recommendations on strategic issues to 'high political levels'. According to the strategy, the 'permanent' NCSC members – the key stakeholders – are representatives of the following institutions: the Ministry of Internal Affairs; the Kosovo Police; the Kosovo Forensics Agency; the Ministry of Kosovo Security Forces (now the Ministry of Defence); the Kosovo Intelligence Agency; the Agency of Information Society; the Kosovo Security Council; the Ministry of Justice; the Ministry of Economy; the Kosovo Prosecutorial Council; the Kosovo Judicial Council; the Ministry of Finance; Kosovo Customs; the Ministry of Education, Science and Technology; the Ministry of Foreign Affairs; the Regulatory Authority of Electronic and Postal Communications; and the Central Bank of Kosovo. According to the strategy, however, other ministries and agencies may also be included occasionally, whereas private sector representatives are invited as associate members of the council.[245] The council used to convene every three months,[246] but its last meeting, chaired by the National Cybersecurity Coordinator, took place in March 2021 and the body has been virtually dysfunctional ever since.[247]

Nevertheless, it should be stressed that the NCSC's membership does not reflect human rights and freedoms principles since it does not include – on a permanent or occasional basis – the respective stakeholders, such as the OIK or civil society organizations specializing in human rights. Furthermore, according to an OIK representative – with the exception of rare roundtables, workshops, or webinars where cybersecurity issues were briefly discussed as secondary topics – the OIK has not been asked to cooperate with the NCSC in any specific way, nor to provide its opinion on the interconnectedness of human rights with cybersecurity.[248]

Regarding emergency responses, the strategy envisages the operationalization of the national CERT (KOS-CERT) and the establishment of other CERTs that are predominantly responsible for preventing and responding to serious network and information security breaches.[249] The KOS-CERT, which is part of the Regulatory Authority of Electronic and Postal Communications (ARKEP), became operational in June 2016[250] and, until 2020, more than 50 CERTs were operating in Kosovo, including within the executive government, government agencies, the private sector, and academic institutions. Nevertheless, these CERTs are generally understaffed and in many cases lack expertise.[251] The new Draft Law on Cybersecurity[252] will, however, repeal the Law on Prevention and Fight of the Cybercrime.[253] It envisages the establishment of the National Authority for Cybersecurity within the Ministry of Internal Affairs and the operationalization of the CERT within this structure. The adoption of the new Draft law on Cybersecurity may pave the way for strengthening the currently limited capacities of the CERT.

Furthermore, in 2016 the former Ministry of Kosovo Security Force (MKSF)[254] adopted the Cybersecurity Strategy in MKSF/KSF (2017-2020) with the following key objectives: to address threats to the MKSF; to increase awareness among personnel of the risks posed by cybercrime; to strengthen the reliability

245 Ministry of Internal Affairs, National Cybersecurity Strategy and Action Plan 2016-2019, December 2015, p. 19.

246 Global Cyber Security Capacity Centre, Cybersecurity Capacity Review, Republic of Kosovo, March 2020, p. 30.

247 Ministry of Internal Affairs, *Mbahet takimi i Këshillit Shtetëror për Siguri Kibernetike*, 1 March 2021.

248 Interview with a representative of the Ombudsperson Institution of Kosovo, May 2022.

249 Ministry of Internal Affairs, National Cybersecurity Strategy and Action Plan 2016-2019, December 2015, p. 23.

250 Global Cyber Security Capacity Centre, Cybersecurity Capacity Review, Republic of Kosovo, March 2020, p. 10.

251 Ibid., p. 35.

252 Government of Kosovo, *Draft Law on Cyber Security*, 21 July 2020.

253 Official Gazette of the Republic of Kosovo, Law on Prevention and Fight Against Cybercrime (Law No. 03/L –166), 20 July 2010.

254 The Ministry of Kosovo Security Force was transformed into the Ministry of Defence under Law No. 06/L-122 on the Ministry of Defence, adopted by the Assembly of Kosovo on 14 December 2018 (Official Gazette of the Republic of Kosovo, Law No. 06/L-122, 4 January 2019).

and safety of communication information systems within the MKSF/KSF; and to draft and revise existing policies, instructions, and procedures.[255] Regarding cybersecurity incidents, the strategy also envisaged the operationalization of the CERT within the ministry,[256] although the CERT had been formally established in 2015.[257]

The National Cybersecurity Strategy and Action Plan 2016-2019 and the Cybersecurity Strategy in MKSF/KSF (2017-2020) expired three and two years ago, respectively, and are therefore no longer implementable. The new Cybersecurity Strategy (2022-2026) has, however, been drafted but not yet approved by the Kosovo Government.[258] Furthermore, the Draft Security Strategy of Kosovo (2021-2030)[259] and the Draft Strategy of Defence of Kosovo[260] were prepared by the previous Kosovo government in November and December 2020, respectively, as superior national security policy documents, including to provide strategic guidance related to cybersecurity 2020; however, owing to the extraordinary elections of February 2021, they could not be adopted by the assembly. It is therefore possible to conclude that since 2019/2020 cybersecurity in Kosovo has effectively been governed without respective policy guidance.

Furthermore, representatives of both academia and the Ministry of Economy feel that efforts to advance the legal infrastructure related to cybersecurity should include the transposition of the Network Information Systems (NIS) Directive of the EU and derivative bylaws, as well as the drafting and issuance of the new National Cybersecurity Strategy.[261] Representatives of the Kosovo Police/Ministry of Internal Affairs also stressed that, in terms of legislation, the adoption of the new Law on Cybersecurity would have the most direct impact on strengthening cybersecurity in Kosovo,[262] since the draft law envisages the transposition of the NIS Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 on security measures for network and information systems.[263]

According to a KOS-CERT representative, the main institutional mechanisms responsible for the implementation of cybersecurity measures in Kosovo are the Information Society Agency (ISA), the Sector for Combating Cybercrime of the Kosovo Police, the National Cyber Security Unit KOS-CERT, and the highest justice bodies – such as the prosecution, courts, and specific companies specializing in cybersecurity and providing related services. In this regard, the ISA is, among others, responsible for communication technology infrastructure of Kosovo's institutions – including the accumulation, administration, dissemination, and storage of data through the establishment of the State Data Electronic Centre – and for the security and protection of electronic communication infrastructure and data.[264] The Sector for Combating Cybercrime of the Kosovo Police is responsible for dealing with crimes related to computer system access, the provision of pornographic material to those under the age of 16, and the violation of the secrecy of correspondence.[265] The KOS-CERT is currently responsible for coordinating

255 Ministry of Kosovo Security Force/KSF, Cybersecurity Strategy in Ministry of Kosovo Security Force/KSF (2017-2020); 2016.

256 Ibid.

257 Global Cyber Security Capacity Centre, Cybersecurity Capacity Review, Republic of Kosovo, March 2020, p. 41.

258 Interview with a representative of the Ministry of Internal Affairs, Interview, 19 May 2022.

259 Government of Kosovo, Draft Security Strategy of Kosovo (2021-2030), November 2020.

260 Government of Kosovo, Draft Strategy of Defence of Kosovo, December 2020.

261 Interview with Blerim Rexha, 26 May 2022, and a representative of the Ministry of Economy, 23 May 2022.

262 Interview with a representative of the Kosovo Police and the Ministry of Internal Affairs, 24 May 2022.

263 Government of Kosovo, *Draft Law on Cyber Security*, 17 July 2020.

264 ISA, *Functions of the Agency*; 2022.

265 Ministry of Internal Affairs, *Investigation Department*, 2022.

and responding to reported cybersecurity incidents, and acts as a contact point for responses at the regional and international level.[266]

In this respect, a representative of the Ministry of Internal Affairs stressed that Kosovo's lack of country code top-level domains (TLDs) is a major cybersecurity risk since the Internet Protocol (IP) addresses of devices connected to the internet in Kosovo are either directed to Albania or Serbia, making it very difficult to manage incident reports. They also underlined the need to appoint officials who specialize in information system security in all governmental ministries and agencies, given the important role it plays in ensuring not only cybersecurity but also national security.[267] In this vein, a representative of the Ministry of Defence highlighted the ministry's aim to establish the National Cybersecurity Training Centre to increase cybersecurity capacities in Kosovo's security institutions.[268]

The KOS-CERT has an online platform for the reporting of cyber incidents committed against private or public legal entities and citizens, but it is unfortunately not being used by victims as they are unaware that it exists. Instead, victims of cybercrimes usually report incidents to the Kosovo Police, which directs cases to its Investigation Department, namely the Section for the Investigation of Cybercrimes.[269] In this regard, a representative of OIK stated that the level of interaction concerning cybercrimes is limited, and that only a few cases referred to the OIK were related to possible computer interference, such as the violation of privacy or personal data. They also underlined that the OIK staff responsible for investigating and handling these cases are not familiar with the complexity of the cyber environment and the wider implications of cybersecurity breaches.[270]

Opinions differed … regarding the level of involvement and cooperation with private sector, academia, and citizens in the area of cybersecurity

Opinions differed among representatives of governmental institutions and academia regarding the level of involvement and cooperation with private sector, academia, and citizens in the area of cybersecurity. A representative of the Ministry of Economy underlined that the private sector is involved in all the working groups for drafting strategies, primary and secondary legislation, and other strategic documents, and that there is genuine cooperation with electronic communications operators. The implementation of security measures set by the Electronic Communications Law and their contribution to Cyber Security Maturity Assessments (CSMAs) were provided as examples.[271] According to a representative of the Ministry of Justice, although the ministry does not have a direct role in cybersecurity, it does allow for inputs from the entire academic community and civil society, particularly in the drafting of laws related to cybersecurity.[272] Furthermore, a representative of the Ministry of Internal Affairs observed that government cooperates with the private sector, namely with banks, within the framework of the NCSC,[273] whereas a representative of KOS-CERT claimed that, due to insufficient capacities, its cooperation with academia was limited to a few study visits of several hours within each institution.[274] In addition, a representative of the Ministry of Defence said they worked with the academic community but

266 Interview with a representative of KOS-CERT, 26 May 2022.
267 Interview with a representative of the Ministry of Internal Affairs, 19 May 2022.
268 Interview with a representative of the Ministry of Defence, 1 June 2022.
269 Global Cyber Security Capacity Centre, Cybersecurity Capacity Review, Republic of Kosovo, March 2020, p. 53.
270 Interview with a representative of the OIK, 27 May 2022.
271 Interview with a representative of the Ministry of Economy, 23 May 2022.
272 Interview with a representative of the Ministry of Justice, 19 May 2022.
273 Interview with a representative of the Ministry of Internal Affairs, 19 May 2022.
274 Interview with a representative of KOS-CERT, 26 May 2022.

only on an occasional basis, such as through joint exercises involving academic institutions of Kosovo, the Kosovo Security Force, and the Iowa National Guard.[275]

It is notable that the University of Prishtina's team 'Runtime Terror' came first in the 'International Cybersecurity Exercise 2022' – organized in conjunction with Iowa State University (USA), the Kosovo Security Force, and the Iowa National Guard – which took place at the end of May 2022,[276] thus proving the potential of the academic community in Kosovo to develop cybersecurity expertise. Nevertheless, the representative claimed that academia and civil society are not represented at all in Kosovo's cybersecurity institutions, and that KOS-CERT is the only institution to interact with citizens, since it is responsible for keeping them informed of potential cybersecurity threats. According to him however, even these efforts are virtually non-existent.[277]

It is therefore possible to conclude that governmental institutions and the private sector – namely, banks and electronic communications operators – work together on cybersecurity-related issues. Cooperation with academia is, however, limited to occasional exercises and study visits, and lacking almost entirely with citizens – owing to the limited capacities of cybersecurity institutions.

CYBERSECURITY AND HUMAN RIGHTS FRAMEWORKS

This section considers whether cybersecurity measures in Kosovo conform to its human right standards, including the application of domestic human rights protection. It also scrutinizes the extent to which different institutions coordinate to safeguard these rights in practice, as well as issues affecting different gender groups.

The Constitution of the Republic of Kosovo provides for the safeguarding of human rights and fundamental freedoms. In terms of cybersecurity, the most important provisions are those related to the right to personal integrity, liberty and security, privacy, freedom of belief, conscience and religion, freedom of expression, freedom of gathering, and freedom of association, as well as the rights of children. Furthermore, the Constitution of Kosovo envisages the protection of human rights and fundamental freedoms that are also guaranteed by the Universal Declaration of Human Rights, the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocols, and the International Covenant on Civil and Political Rights and its Protocols, which, according to its provisions, are directly applicable in Kosovo. In addition, they have precedence over the provisions of national laws and other acts of public institutions. Most importantly, the Constitution envisages that the rights and fundamental freedoms shall be interpreted according to the decisions of the European Court of Human Rights.[278]

Although Kosovo is not a member of the Council of Europe and, as such, has neither signed nor ratified the Budapest Convention on Cybercrime,[279] according to a profile prepared by the Cybercrime Programme Office of the Council of Europe (C-PROC) on assessing the current state of implementation of the convention under national legislation, it has implemented the convention through the following pieces of legislation: Law No. 03/L–166 on Prevention and Fight Against Cybercrime; Code No. 06/L-074; Criminal

275 Interview with a representative of the Ministry of Defence, 1 June 2022.

276 For further details, see: *Reserve & National Guard Magazine*, *First international cyber-defense competition links Iowa, Kosovo campuses*; 19 May 2022; and IScorE, *International Cyber Security Exercise*; 22 May 2022.

277 Interview with Blerim Rexha, 26 May 2022.

278 Constitute, *Kosovo's Constitution of 2008 with Amendments through 2016*, 27 April 2022.

279 Council of Europe, Budapest Convention on Cyber Crimes, 23 November 2001.

Code of the Republic of Kosovo (2019); Law No. 04/L-109 on Electronic Communications (2012); and Law No. 04/L-213 on International Legal Cooperation in Criminal Matters.[280] Furthermore, according to the EU Commission's Kosovo 2021 Report, Kosovo's legislation on cybercrime is generally in line with the EU acquis.[281]

It should be noted, however, that the Criminal Code does not specify all the offences related to cybercrime, which are defined by the Law on Prevention and Fight of the Cyber Crime.[282] This law covers penal acts related to the confidentiality, integrity, and availability of computer systems data; the unauthorized interception of data; the unauthorized transfer of data; the hindrance of computer system operations; the unauthorized production of data; possession and attempt to commit a penal act; computer-related penal acts; the loss of assets; and child pornography through computer systems. The Criminal Code also, however, covers the abuse of children in pornography; the issuing of uncovered or false cheques and the misuse of bank or credit cards; identity and access device theft; intrusion into computer systems; and the violation of patent rights and copyrights. Finally, the Law on Interception of Electronic Communications,[283] as mentioned above, specifies the respective state institutions' obligations and responsibilities related to ensuring respect for human rights and freedoms with regards to lawful interception, including procedures for overseeing its implementation.

However, according to the EU Commission's Kosovo 2021 Report, while Kosovo's legal framework guarantees the protection of fundamental rights and is in line with European standards, implementing human rights legislation – as well as overseeing and coordinating existing human rights mechanisms – remains a challenge. The report also underlines that while Kosovo is still in the process of developing a well-functioning judicial system, the institutions are currently rather slow, inefficient, and prone to political influence.[284]

The EU Commission finds that efforts to investigate and prosecute cybercrime have progressed, with 53 cases initiated in Kosovo in 2020, but there is insufficient knowledge and limited cybercrime training available for newly appointed judges and prosecutors.[285] Furthermore, within Kosovo's judiciary system, no single specialized unit deals with cybercrime investigations, which are usually conducted by the Sector for Cybercrime Investigation of the Kosovo Police. Against this background, the report highlights that incidents involving offensive and hate speech in online and social media often lack effective judicial follow-up.[286]

In terms of discrimination, while a number of hate speech and hate crime incidents against the lesbian, gay, bisexual, transgender, intersex, queer, and asexual (LGBTIQA+) community have been reported, especially on social media, these cases are not always properly investigated or brought to justice.[287] Furthermore, according to a policy report published by the Kosovar Institute for Policy Research and Development (KIPRED) in December 2018, these shortcomings are mainly due to the following factors: a lack of institutionalized training for police, prosecution, and judges; the outdated standard operating procedures of the Kosovo Police, adopted in 2007, which do not comply with the laws on gender equality

---

280 Council of Europe, *Kosovo Cyber Crime Legislation: Domestic Equivalent to the Provisions of the Budapest Convention*.

281 European Commission, *Kosovo Report 2021*, 19 October 2021, p. 40.

282 Official Gazette of the Republic of Kosovo, Law on Prevention and Fight Against Cybercrime (Law No. 03/L –166), 20 July 2010.

283 Official Gazette of the Republic of Kosovo, Law on Interception of Electronic Communications (Law No. 05/L-030), 13 July 2015.

284 European Commission, *Kosovo Report 2021*, 19 October 2021.

285 Ibid., p. 42.

286 Ibid. p. 31.

287 Ibid. p. 35.

and discrimination; homophobia and prejudice among certain officials within rule of law institutions; and the fact that the police have often failed to handle offences against the LGBTIQA+ community sufficiently seriously or to ensure confidentiality.[288]

Cybersecurity and the right to privacy

This section briefly analyses cybersecurity legislation in Kosovo regulating the right to privacy, including in online spaces, as well as the institutions responsible for responding to cybersecurity-related issues.

The right to privacy in Kosovo is guaranteed by Article 36 of the Constitution, which stipulates that 'everyone enjoys the right to have her/his private and family life respected, the inviolability of residence, and the confidentiality of correspondence, telecommunication and other communication', and that 'every person enjoys the right of protection of personal data', which should be regulated by law.[289]

Kosovo adopted the Law on Interception of Communications[290] in 2015 to regulate the right to privacy. Article 4 of this law lays out the following basic principles: respect for human rights and fundamental freedoms safeguarded and guaranteed by the Constitution; compliance with the European Convention on Human Rights and Freedoms, including the case-law of the European Court of Human Rights; and the prohibition of interception without a respective decision by the court. Article 6 stipulates that lawful interceptions should include three phases: (1) the submission of requests for interception from the institutions authorized by the law; (2) the review, approval, and submission of requests for interception; and (3) the court order for interception. The Commissioner for Oversight of Interception of Communications, established by the Law on Interception of Communications, functions within the Kosovo Judicial Council (KJC). The commissioner controls the lawfulness of communication interceptions on an annual basis and reports possible violations to the KJC and the State Prosecutor, as well as the respective parliamentary committees of the Assembly of Kosovo. Prior to the adoption of this law, the lack of a legal framework for cooperation between national and international security and justice institutions in Kosovo made interceptions challenging and resulted in independent agreements between these institutions and telecommunication operators.[291]

The Law on Protection of Personal Data[292] determines possible sanctions for the violation of personal data, including violations of the provisions on security of personal data; on direct marketing; on video surveillance, such as surveillance in apartment buildings and work areas; and on biometrics, in the public and private sector.[293] The law complies with the EU Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data.[294] A representative of the Agency for Information and Privacy, however, claims that there are

---

288 Qosaj-Mustafa, Ariana and Morina Donjeta, *Accessing Justice for Victims of Gender Based Violence in Kosovo: Ending Impunity for Perpetrators*, Policy Report, KIPRED, December 2018.

289 Ibid.

290 Official Gazette of the Republic of Kosovo, Law on Interception of Electronic Communications (Law No. 05/L-030), 13 July 2015.

291 Kursani, Shpend, *Lawful Interception of Telecommunications in Kosovo: Security Implications*, 27 October 2011.

292 Official Gazette of the Republic of Kosovo, Law on Protection of Personal Data (Law No. 06/L – 082), 25 February 2019.

293 Ibid., arts. 91-107.

294 Ibid., art. 1.2.

gaps in this law and that it should include specific measures on the regulation of data protection given evolving technological developments.[295]

The Criminal Code does not specify all criminal acts related to cybercrimes and the right to privacy. It stipulates only that 'whoever, without authorization, photographs, films, or videos or in any other way records another person in his or her personal premises or in any other place where a person has a reasonable expectation of privacy, and in that way fundamentally violates another's privacy, shall be punished by a fine or by imprisonment of one (1) to three (3) years', and that 'whoever, without authorization, passes on, displays or grants access to a third person to a photograph, film, videotape or any other recording obtained in violation of paragraph 1. of the Article 202, shall be punished by imprisonment of one (1) to three (3) years'.[296]

Nevertheless, according to KKJC data, over the last six years the courts in Kosovo have made 18 judgments on cases related to the violation of the right of privacy.[297] Nine of these cases were categorized as unauthorized photography or recordings, four as intrusions into computer systems, four as harassment, and one as coercion. Twelve of them were related to cyber harassment and non-consensual intimate images, terms that are not referred to in the Criminal Code.

All the victims in these cases were women, indicating that they are the main targets of these criminal acts. An analysis of these cases shows that male perpetrators committed these criminal acts to denigrate the personal integrity and dignity of female victims, through the distribution of photos and videos to the victim's family or friends or via different online social medias and pornographic platforms.

According to the Council of Europe, cyber harassment often targets women and girls – referred to as 'cyber violence against women and girls' – and involves the following: unwanted sexually explicit emails or other messages, offensive advances on social media or other platforms, the threat of physical or sexual violence, cyberbullying, and non-consensual intimate images.[298] Whereas according to the European Institute for Gender Equality, the term non-consensual intimate images refers to the online distribution of sexually graphic photographs or videos without the consent of the individual in the images.[299]

The KJC data shows that the majority of the perpetrators in Kosovo were punished by fines. In some cases, prison sentences were replaced by fines, with the consent of the convicted persons, and in others the court suspended sentences. It is important to stress, however, that credible international media organizations have reported that EU privacy laws have also failed the victims of non-consensual pornography. This has pushed a number of EU member states to take this issue into their own hands by providing national legislation that criminalizes these acts. For example, in December 2020, Ireland adopted a stringent legislation on online offenders, which meant they could face up to ten years in prison and unlimited fines[300] Although Kosovo's Criminal Code considers these cases as criminal deeds, despite not using the correct terminology, the government should follow the best practices of EU states and provide legislation that sanctions cyber harassment and revenge porn and imposes severe punishments to effectively protect its citizens' right to privacy – especially that of women, who are the main victims of these criminal acts.

---

295 Interview with a representative of the Agency for Information and Privacy, 19 May 2022.

296 Official Gazette of the Republic of Kosovo, Criminal Code of the Republic of Kosovo (Code No. 06/L-074), 14 January 2019.

297 Kosovo Judicial Council, *Judgements*.

298 Council of Europe, *Types of cyberviolence*.

299 European Institute for Gender Equality, Definition of '*revenge porn*'.

300 Pogatchnik, Shawn, *Ireland brings in tough laws on revenge porn and online bullying*, Politiko, 17 December 2020.

The Ombudsperson Institution of Kosovo's report on the installation of security cameras in some cells of prisoners in the Women's Correctional Center in Lipjan describes another interesting case related to privacy rights.[301] According to the report, the centre has had a number of security cameras installed in order to protect prisoners who suffer from serious mental health problems related to self-harm or suicide attempts. It concludes that while there was a legitimate purpose for the measure, such an action constitutes a violation of the right to privacy; installing security cameras in certain cells should be regulated by legal acts and procedures which provide the necessary guarantees and procedures related to the protection of human rights, particularly the right to privacy.[302]

Against this backdrop, a civil society activist states that there have been numerous cases of members of the LGBTIQA+ community being victims of cybercrime involving breaches of privacy in the online space – usually through fake social media profiles. Many of these cases have been reported to the police, who have so far failed to identify any of the perpetrators. Owing to the lack of effective investigation, the activist observed that although such incidents continue to occur, they are no longer being reported to the police.[303] Regarding non-majority communities, in 2019 a Roma woman was attacked after a group of young people photographed her at a bus station in Malisheva and shared her photo online with the caption: 'Be careful at your home'.[304] As a result of these false allegations, which led to digital media reports and online cyberbullying, the woman was attacked twice – once in Lipjan, and again in Ferizaj.[305]

These cases illustrate the risks posed by cybercrime incidents that affect the right to privacy, which may have grave consequences for victims if they are not effectively protected by legislation, or the cases are not properly investigated by the Kosovo Police and other respective institutions.

Cybersecurity and freedom of expression

This section considers key issues related to online censorship and legislation addressing cybersecurity and freedom of expression in Kosovo. The right to freedom of expression in Kosovo is guaranteed by Article 40 of its Constitution, which defines it as the right 'to express oneself, to disseminate and receive information, opinions and other messages without impediment'.[306] The article stipulates that this freedom can be limited by law 'when it is necessary to prevent encouragement or provocation of violence and hostility on grounds of race, nationality, ethnicity or religion'.[307] Furthermore, the Constitution explicitly forbids censorship,[308] which in legal terms includes online censorship. The legislation of Kosovo does not treat disinformation through civil or criminal legal frameworks. In this context, according to a representative of OIK, all the guarantees provided by Kosovo's legal framework also apply to cybersecurity.[309] In addition, defamation and insult cases are treated by the Civil Law on Defamation

---

301 Ombudsperson Institution of Kosovo, *Raport me rekomandime, ex officio nr.95/2022 përkitazi me instalimin e kamerave të sigurisë në disa qeli të burgosurave në Qendrën Korrektuese për Femra në Lipjan*, 25 February 2022.

302 Ibid.

303 Interview with Arber Nuhiu, 2 June 2022.

304 Ombudsperson Institution of Kosovo, *Raport me rekomandime Ex-Officio 468-2019 përkitazi me detyrimet pozitive në rastin e znj. Z. S. të garantuara me Kushtetutën e Republikës së Kosovës, si dhe me nenin 3 të Konventës Europiane për Mbrojtjen e të drejtave dhe Lirive Themelore të Njeriut*, 9 December 2019.

305 Ibid.

306 Constitute, *Kosovo's Constitution of 2008 with Amendments through 2016*, 27 April 2022.

307 Ibid.

308 Ibid., art. 42.2.

309 Interview with a representative of the Ombudsperson Institution of Kosovo, 27 May 2022.

and Insult,[310] whereas the Criminal Code penalizes hate acts (art. 2.12) and those inciting discord and intolerance (art. 141).

It is notable in this context that the European Commission's Kosovo 2021 Report underlined that Kosovo's Constitution and legal framework guarantees freedom of expression and media freedom. The report stated that, in general, the media laws and those related to defamation and access to information are in accordance with standards of the Council of Europe and the case-law of the European Court on Human Rights. Nevertheless, it also expressed concern that the Law on Protection of Journalistic Sources does not comply with European standards and best practices, and that the government's administrative capacities to deal with issues related to freedom of expression are not sufficient.[311] Furthermore, it raised issues regarding public smear campaigns and threats, particularly physical attacks on journalists, and underlined that not all threats of this nature are reported to the relevant authorities. In addition, it stated that freedom of expression and self-censorship in the north of Kosovo is a matter of particular concern.[312]

In this vein, the US State Department's Kosovo 2021 Country Report on Human Rights Practices found that, in general, the Kosovo government has respected the right of freedom of expression, but underlined that there were credible reports of some public officials, politicians, businesses, and religious groups intimidating media representatives. This report also indicated that there were no cases of direct censorship of print or broadcast media, but that pressure and threats from politicians and organized criminal groups frequently resulted in self-censorship by journalists.[313] On the other hand, the report stressed that the government has neither restricted nor disrupted access to internet or censored online content, and that it has not conducted any surveillance of private online communications in the absence of an appropriate legal authority.[314]

One representative of civil society felt that over the last few years three major challenges had emerged related to freedom of expression and cybersecurity: cyberbullying or hate speech, misinformation, and online harassment.[315] Freedom of expression and human rights should, according to them, apply to all types of communication, including the internet. They also emphasized that while the UN had declared freedom of speech and expression in cyberspace a fundamental part of human rights, this comes at a price for millions of internet users, who are being bullied and exposed to hate speech and fraud every day. Furthermore, they claimed that cybersecurity laws have a direct impact on human rights, particularly the right to privacy and freedom of expression, which contributes to development, democracy, and dialogue. In their opinion, these laws are insufficient to tackle the issues raised above, since the identification of hate speakers, bullies, or frauds is either slow or, in most cases, does not happen at all.[316]

---

310 Official Gazette of the Republic of Kosovo, Civil Law on Defamation and Insult (Law No. 02/L-65), 1 May 2008.

311 European Commission, *Kosovo Report 2021*, 19 October 2021.

312 Ibid., p. 30.

313 US State Department, *Kosovo 2021 Report on Human Rights Practices*, 2021, pp. 14-15.

314 Ibid., p. 16.

315 Interview with Adrian Zeqiri, 3 June 2022.

316 Ibid.

Cybersecurity and freedom of peaceful assembly

This section analyses Kosovo's legislation related to the right to freedom of peaceful assembly and possible cybersecurity infringements, as well as responses by the respective actors and institutions. Articles 43 and 44 of the Constitution guarantee the right to freedom of peaceful assembly and association. These rights are also provided for by the Law on Public Gathering[317] and the Law on the Freedom of Association in Non-Governmental Organizations.[318]

Legislation in Kosovo related to the right of peaceful assembly, however, is still outdated compared with that of freedom of association – despite a number of efforts to update it. The Concept Document on Public Gatherings, drafted in March 2018 by the Ministry of Internal Affairs of Kosovo, identified numerous issues in relation to the implementation of the Law on Public Gatherings of 2009, including legal gaps and discrepancies, vagueness, and some inconsistences with the Criminal Code of Kosovo.[319] The government consequently drafted a new Law on Public Gatherings and, on 21 August 2020, the then prime minister, Avdullah Hoti, requested an opinion of the Venice Commission on whether it adhered to best international practices, standards, and norms.[320]

The Venice Commission provided several comments and conclusions on this draft law and raised three key issues related to cybersecurity. The first concerned the requirement to identify an organizer for public gatherings, given that social media makes it possible to organize gatherings in an informal manner; in this case, according to the opinion of the Venice Commission, the absence of an identifiable organizer should not affect the right to freedom of assembly to all gatherings. In this vein, the Venice Commission stated that the draft law should establish a procedure on facilitating public gatherings that are not organized by an identifiable person or group.[321]

The second issue related to digital images and recordings by the authorities; Article 12(8) of the draft law states that 'recordings, filming and photographs are disposed of immediately after the gathering, in case they are not needed', which, according to the Venice Commission, does not refer to data protection legislation and fails to specify a maximum duration for data retention. The Venice Commission also found the clause 'in case they are not needed' to be too vague and to provide authorities with too much discretion, which raises serious concerns about the data protection of the attendees of public gatherings. Similarly, the opinion highlights the need to ensure that the draft law complies with the Joint Guidelines on Freedom of Peaceful Assembly of the Venice Commission – OSCE Office for Democratic Institutions and Human Rights, which requires that the digital images of organizers and participants in gatherings should not be recorded by authorities, with the exception of cases authorized by law. In addition, the opinion requires that legislation and respective policies pertaining to the collection and processing of information related to gatherings must integrate legality, necessity, and proportionality tests. The Venice Commission also requested that the law add a cross-reference to legislation on data protection – such as the Law on Minor Offences, the Code of Criminal Procedure, and the Law on Protection of Personal Data, and that the clause 'in case they are not needed' should not be used in the above mentioned article of the draft law.[322] Finally, it raised concerns about the absence of provisions on online gatherings in the draft

317 Official Gazette of the Republic of Kosovo, Law on Public Gathering (Law No. 03/L-118), 15 April 2009.

318 Official Gazette of the Republic of Kosovo, Law on the Freedom of Association in Non-Governmental Organizations (Law No.06/L – 043), 24 April 2009.

319 Ministry of Internal Affairs, Concept Document on Public Gathering, March 2018.

320 Venice Commission, *Kosovo: Opinion on the Draft Law on Public Gathering*, 9 October 2020.

321 Ibid., p. 11.

322 Ibid., p. 15.

law, which therefore fails to offer citizens the legal right to hold public gatherings online; the commission recommends including a legal provision to regulate this matter.[323]

According to an interpretation provided by the Report on the Freedom of Internet in the Western Balkans, however, citizens of Kosovo are free to use internet platforms, including social media, to organize peaceful gathering, since there are no legal restrictions to internet freedom.[324] Against this backdrop, a representative of the Agency for Information and Privacy has declared that the use of biometric surveillance, in principle, is not allowed, except in specific cases provided for by the Law on Protection of Personal Data.[325] Furthermore, the Kosovo 2021 Human Rights Practices Report of the State Department underlines that the Kosovo government has neither restricted nor disrupted internet access. Nor has it monitored private online communications without the appropriate legal authority.[326]

A civil society leader, however, said they had come across many events, whether carried out online or face-to-face, where participants had not been asked for their permission to be photographed or for the photos to be published on the official websites of the organizer. They expressed concern that this not only violates the participant's right to privacy but may also lead to the identification of many potential victims.[327] Furthermore, they knew of several cases where face recognition had led to violence against LGBTIQA+ activists. According to them, the spread of pictures with unconcealed faces on social media caused the victims to suffer severe hate speech, cyber threats, and even physical violence, or to be considered unacceptable by their families. In addition, they observed that while the police were involved in the cases reported, due to the lack of trust of government institutions, many of these cases were not reported at all. They highlighted that local civil society organizations are usually the first to report and react to these violations of rights, and often follow up on these cases.[328]

A civil society leader of the LGBTIQA+ community refers to cases related to the first and second pride parade in Kosovo, both of which were announced publicly, where organizers and members of the community were subjected to threats. During the first parade, the threat was considered imminent and, as a result, the police force was engaged, including by deploying snipers on the roof of the Grand Hotel located in the centre of Prishtina. The following year, organizers received another online threat, reported to the Kosovo Police, from someone with an IP address in Switzerland. Nevertheless, the police again engaged sniper officers to ensure the safety of participants, which included the prime minister and many members of the diplomatic corps accredited in Prishtina. Despite a number of threats over the last few years, the pride parades have been organized and taken place without any significant problems.[329]

---

323 Ibid., p. 17.

324 Civil Rights Defenders, *Report on the Freedom of Internet in the Western Balkans*, 2020, p. 14.

325 Radio Evrope e Lirë, *Qeveria e Kosoves analizon kontratat për kamerat kineze*, 4 February 2022.

326 US State Department, *Kosovo 2021 Report on Human Rights Practices*, 2021, p. 16.

327 Interview with Adrian Zeqiri, 3 June 2022.

328 Ibid.

329 Interview with Arber Nuhiu, 2 June 2022.

Cybersecurity and anti-discrimination

This section will analyse anti-discrimination awareness in cybersecurity within the legislative and institutional framework of Kosovo, as well as possible disparities in access to cybersecurity for vulnerable groups.

In this regard, Article 24 of the Constitution of Kosovo protects against discrimination, combined with applying specified international legal norms, particularly UN and European legislation on human rights and anti-discrimination (art. 22), and ensuring that human rights provisions conform to court decisions of the European Court of Human Rights (art. 53). Kosovo's anti-discriminatory legislation was further advanced in 2015, with the promulgation of Law No. 05/L-019 on Ombudsperson, Law No. 05/L-020 on Gender Equality, and Law No. 05/L-021 on Protection from Discrimination.
In terms of anti-discrimination and cybersecurity, according to a report on internet freedom in the Western Balkans, internet access is available at a reasonable price to all population groups, without discrimination. The report also found that the government is taking measures to ensure that low-income individuals have access to the internet, especially those in remote rural areas, and that, internet service providers, as a general rule, treat internet traffic equally and without discrimination.[330]

A civil society leader, however, claimed that one key area of concern is mental health issues related to hate speech, cyber bullying, and threats – particularly the online security of vulnerable groups such as women, Roma, and LGBTIQA+ communities. Experiences of online hate impact people's freedom to express feelings or opinions without fearing for their safety.[331] He also observed that a number of social networking sites share content that includes inappropriate hate speech related to the LGBTIQA+ community or prejudice towards non-minority communities, particularly the Roma community. Furthermore, they claimed that despite the submission of formal complaints by the discriminated groups, these issues were not addressed.[332] The most striking case in Kosovo in this regard was a social media campaign against the former US Special presidential envoy for Serbia and Kosovo peace negotiations, Mr Richard Grenell, who was insulted on the basis of his sexual orientation owing to his political stance; the major offences were committed by the Facebook group 'Me Kryeministrin' [With the Prime Minister], managed by Vetëvendosje militants.[333] According to a civil society leader, the former President Thaçi intended to establish a Consultative Council within the Office of the President for issues affecting the LGBTIQA+ community; however, the process was interrupted due to his resignation as a result of indictment by the Specialist Chambers of Kosovo.[334]

According to the civil society leader, lynching, misinformation, and fake news are only some of the issues related to the misuse of the freedom of expression in cyberspace by spreading discrimination, defamation, or disinformation – which, in certain cases, may affect the safety of individual citizens belonging to marginalized groups. They mentioned an incident that occurred in May 2019 when a trans Roma woman was described in the media as 'dangerous, violent, and a thief', despite having been interviewed by the police and found to be innocent. The case became national news and was accompanied by horrific hate speech spread through social media networks; many videos were circulated using violence against this Roma woman due to misinformation disseminated by unofficial and false portals. At the time, state actors, including the Kosovo Police and the Ministry for Communities and Return, responded but took too long to

330 Civil Rights Defenders, Report on the Freedom of Internet in the Western Balkans, 2020, p. 12.
331 Interview with Adrian Zeqiri, 3 June 2022.
332 Ibid.
333 Insajderi, Grupi *"Me Kryeministrin" bëjnë fushatë dhe e fyejnë Grenellin në baza të orientimit sekslual*, 27 March 2020.
334 Interview with Arber Nuhiu, 2 June 2022.

ensure the woman's safety. Local civil society organizations also sought to intervene until the woman was reported safe.[335]

The new Draft Law on Cybersecurity stipulates that the online distribution of pro-genocide materials or those related to crimes against humanity, including racist or xenophobic materials, is to be punishable as a criminal offence.[336] The online distribution of materials related to pro-genocide or crimes against humanity are defined as 'delivering or deliberately distributing to the public through computer systems, materials that substantially deny, sensitively minimize, approve or justify acts that constitute genocide or crimes against humanity'.[337] The draft law states that perpetrators shall be punished by imprisonment of three to six years.[338] The distribution of racist or xenophobic materials through computer system is defined separately as 'delivering or deliberately distributing to the public through computer systems, materials with racist or xenophobic content'; the draft law stipulates that perpetrators shall be fined or punished by imprisonment of up to two years.[339]

Despite significant progress … the legal framework remains incomplete [and] policies are out of date

WAYS FORWARD

The research findings presented in this paper show that legal and policy frameworks, as well as the protection of human rights, related to cybersecurity in Kosovo have evolved since the Declaration of Independence in 2008. Despite significant progress, however, the legal framework remains incomplete; since 2019, all the respective policies are out of date, thus implying that cybersecurity measures in Kosovo have been implemented without policy guidance over the last three years.

The research findings demonstrate a lack of capacity to address cybersecurity issues among government institutions and agencies, as well as a shortage of qualified cybersecurity personnel and specialized institutions to provide professional training in this field. Furthermore, the area of cybersecurity lacks a human rights dimension within the Kosovo government and the judiciary. Although cooperation exists, at least in principle, between state cybersecurity institutions, academia, and the private sector, interaction with citizens is virtually non-existent. The research does, however, show that internet access is available at a reasonable price to all groups of the population, without discrimination. Furthermore, the government is taking measures to ensure internet access for low-income individuals, especially in remote rural areas.

The research findings indicate that the main victims of cybercrimes in relation to human rights are women, the LGBTIQA+ community, and Roma – along with, to a lesser extent, other vulnerable groups. Furthermore, the findings show that the perpetrators of these crimes receive less sever punishments than those foreseen by the law for their crimes.

Based on the findings of this paper and suggestions from those who participated in the research, it is

335 Interview with Adrian Zeqiri, 3 June 2022.
336 Government of Kosovo, *Draft Law on Cyber Security*, 21 July 2020.
337 Ibid. art. 15
338 Ibid.
339 Ibid., art. 17.

possible to propose the following recommendations to governmental and non-governmental stakeholders in Kosovo:

Kosovo government:

- A representative of the Institution of Ombudsperson in Kosovo should be made a permanent member of the NCSC; representatives of human rights organizations and civil society organizations representing women, LGBTIQA+ communities, and other vulnerable groups should be made associated members.
- The Kosovo government should adopt the new National Cybersecurity Strategy and Action Plan, which will provide policy guidance to cybersecurity institutions, including actions to take to improve human rights protection in relation to cybersecurity.
- Kosovo institutions, including the judiciary, should increase cybersecurity capacities in order to meet challenges related to rapidly developing information technology and the increasing number of cybercrimes that affect human rights.
- A National Cybersecurity Training Centre should be established to increase cybersecurity capacities in all of Kosovo's security institutions.
- The Kosovo government should improve the Law on Protection of Personal Data and introduce strong legislation to sanction incidents involving cyber harassment and non-consensual intimate images by following the best practices of EU states in this field, in order to protect its citizens' right to privacy – particularly that of women who are the main victims of these criminal acts.
- The Draft Law on Public Gatherings should conform to the Opinion of the Venice Commission of 9 October 2020.
- The Kosovo government should implement the NIS Directive of the EU, as well as its derivative bylaws, and adopt the new Law on Cybersecurity as soon as possible.
- Efforts should be made to improve inter-governmental coordination and cooperation in legislative and policy initiatives related to cybersecurity and responses to cyber incidents and crimes, as well as to provide a clear definition of the duties and responsibilities of all cybersecurity institutions.
- The KOS-CERT and other CERTs should be given a clear legal mandate that specifies in detail their duties and responsibilities; they should be supported by professional staff to ensure they have the necessary capacities to accomplish their responsibilities.

Academia and civil society:

- Digital training should be introduced at all levels of education to ensure the educational system adapts to respond to technological developments.
- Cybersecurity awareness should be increased through extra-curricular programs provided by academia to civil society groups and students.
- Efforts should be made to increase civil society's capacity and awareness of cybersecurity and the protection of human rights and vulnerable groups, such as women, LGBTIQA+ and non-majority communities in cyberspace.

Private sector:

- Possible private-public partnerships should be explored to increase governmental and non-governmental capacities in the area of cybersecurity.

International community:

- Legal, policy, and technical expertise should be provided to Kosovo institutions in the field of cybersecurity.
- Efforts to increase cybersecurity awareness should be supported, especially those targeting vulnerable and marginalized groups.

CHAPTER 4

MONTENEGRO
Improving Awareness as a Foundation for Tailoring the Approach

By Milica Kovačević and Tijana Velimirovic | Centre for Democratic Transition (CDT)

CHAPTER 4:

MONTENEGRO – IMPROVING AWARENESS AS A FOUNDATION FOR TAILORING THE APPROACH

THE GENERAL CONTEXT OF CYBERSECURITY

Cybersecurity and data protection in Montenegro are regulated by the Law on Information Security[340] and the Regulation on Information Security Measures, which were adopted in December 2021. The digital transformation of society has led to a significant increase in the incidence of **cyber attacks**. This has further underlined the importance of having in place adequate protection for critical infrastructure and of taking decisive steps in the field of cybersecurity, which means strengthening national capacities for cyber defence and for responding to cybercrime.[341]

In recent years, Montenegro has introduced a number of strategic frameworks and organizational structures in the field of cybersecurity. The National Security Strategy and the Defence Strategy of Montenegro were adopted in February 2020.[342] Newly adopted Cybersecurity Strategy covers the period 2022-2026, and follows two similar strategies implemented in the periods 2013-2017 and 2018-2021. The most recent cybersecurity strategy of the Army of Montenegro covers the period 2019-2022. The National Team for Response to Computer Security Incidents in the Cyberspace of Montenegro (CIRT.ME) was formed in 2012 and is a member of the global Forum of Incident Response and Security Teams (FIRST); a network of CIRTs has also been established at the local level. An organizational unit for cyber defence and response to computer technology incidents has been established at the Ministry of Defence; the capacities of the National Security Agency (NSA) and the Police Directorate have been strengthened; and a Council for Information Security has been established.[343]

The state administration bodies recognized under the national cybersecurity strategy are the NSA, the Ministry of Defence, the Ministry of Interior, the Police Directorate, the Directorate for Protection of Classified Information, CIRT.ME, the Ministry of Education, Science, Culture and Sports, the Ministry of Public Administration, Digital Society and Media, and the Ministry of Foreign Affairs. Amendments to the Law on Information Security and additional harmonization with the European Union's Directive on Security of Network and Information Systems (NIS Directive) are planned, along with the establishment of a new Cybersecurity Agency.

340 https://www.gov.me/dokumenta/fbb730c5-8c62-47e3-863f-cfaae9631b8d

341 https://wapi.gov.me/download-preview/97751303-14b4-49f3-b428-911f09728b46?version=1.0

342 https://www.gov.me/dokumenta/08cb12b5-395e-4047-a1cd-ff884683b9e3

343 https://wapi.gov.me/download-preview/97751303-14b4-49f3-b428-911f09728b46?version=1.0

The NSA is recognized in strategic documents as one of the key institutions responsible for policing the cyberspace realm in Montenegro, in line with its primary focus on the protection of national interests and security. The law governing the NSA defines the agency's competencies, which primarily involve the collection and processing of data with significance for national security, as well as its work in counter-intelligence and the protection of important facilities and persons.

The CIRT team is responsible for dealing with security incidents involving computer technology in Montenegro's cyberspace realm. It was formed in 2012 as part of a joint project between the Government of Montenegro and the International Telecommunication Union (ITU). Until November 2020 CIRT was part of the Ministry of Public Administration but since then, following amendments to the Law on Data Secrecy, it has come under the Directorate for the Protection of Classified Data. The national CIRT's function is to protect national networks against computer security incidents stemming from the Internet and other risks related to information security. It is also the central point of contact at the national and international levels for all computer security incidents where at least one of the parties involved is based in Montenegro. CIRT works on incident handling, response, and coordination, prepares safety warnings and advice to users, and works to raise awareness and to educate users.

> The Council for Information Security [has the] aim of monitoring and coordinating activities in the field of cybersecurity and proposing regulations

In 2019, the Government of Montenegro adopted a Decision that mandated the formation of the Council for Information Security, with the aim of monitoring and coordinating activities in the field of cybersecurity and proposing measures to improve policies, regulations, and practice in this area.[344] Analysis carried out at the level of the Council, with the assistance of strategic partners, indicated the need for a thorough reorganization of the national CIRT in order to centralize cyber expertise, reduce the outflow of experts, and enable a more effective response to cyber attacks and the protection of critical information infrastructure.[345]

Since Montenegro's accession to NATO in 2017, the Ministry of Defence and the Montenegrin army have made significant efforts to improve information security, in particular building capacity in cyber defence, in line with national and NATO strategic objectives. In this context, changes have been made to organizational structures within both the army and the ministry, in clear recognition of the need to strengthen cyber capacity in the defence arena.

Among other duties, the Ministry of Public Administration, Digital Society and Media administers the proposal and implementation of policy aimed at the development of an information society; prepares draft laws and other regulations in the field of information security; and provides professional assistance for the application of information and communication technologies (ICT) in state administration and other state bodies. It is currently establishing a framework for the management of information systems within such bodies, in accordance with international standards; is setting up technological and security information infrastructure for these state bodies; and is determining technical and other rules governing their use of ICT.

Montenegro has ratified a number of internationally binding conventions, has joined the UN, the Organization for Security and Co-operation in Europe (OSCE), NATO, and FIRST, and has participated in initiatives and platforms aimed at strengthening capacities for cyber defence. It is also a member of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) and of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) based in Estonia, and has participated in numerous

344 https://www.gov.me/dokumenta/5b254c61-683f-45fa-8925-30d2df8ecb63

345 https://wapi.gov.me/download-preview/97751303-14b4-49f3-b428-911f09728b46?version=1.0

international joint exercises, trainings, meetings, forums, and conferences. Its membership of these conventions and organizations has been a significant factor in shaping its approach to cybersecurity. NATO's first anti-hybrid threat support team visited Montenegro in November 2020 to help strengthen the country's capabilities and deter hybrid challenges.[346] Montenegro has also engaged in the EU's hybrid risk survey, with the objective of identifying systemic vulnerabilities and further focusing EU assistance provided in this field.[347]

The state does not yet have a strategy on combating hybrid threats, however. It announced in 2019 that one would be introduced, but after a change of government in 2020 work on this strategic document was suspended. Meanwhile, our interlocutors reported that, given the high prevalence of hybrid threats and therefore of cyber threats, current levels of protection are definitely not sufficient. Individuals do not have a high level of awareness of cyber threats, and are most vulnerable to social engineering. They emphasized the need to educate citizens in order to increase Internet security in general, but also pointed out that all owners of information systems must implement security measures to prevent attacks.

There is an obvious need for close cooperation between government and the private sector in the field of cybersecurity, and the coordination of all segments of society is necessary in order to respond in a timely and efficient manner to the challenges that exist in the cyber domain. The government's cybersecurity strategy and action plan acknowledge that more cooperation and improved measures for prevention and education about cybersecurity are needed in the public and private sectors. The strategy underlines that existing platforms where the private and public sectors come together (such as Science and Technology Park Montenegro) should be further strengthened to provide training, exchange expertise, and encourage cooperation in research and development in the field of cybersecurity.

Despite the established institutional and strategic framework, a number of challenges have been identified in implementation and in achieving results. What has been recognized as a key challenge is the lack of financial resources to implement the strategy; this is a consequence of decision-makers being insufficiently aware of the importance of investing in cybersecurity. Another problem is a shortage of experts and professional staff in this area, an issue that is particularly apparent in Montenegro as a country with extremely limited human resources. The strategic documents state openly that Montenegro lacks adequate mechanisms for detecting cyber threats and mechanisms for a sufficiently rapid response or recovery following an attack.

It is often difficult to identify and prosecute the perpetrators of cybercrime. Consequently, state authorities often appear powerless in their failure to find out where attacks come from and explain to the public who is behind them. For example, in April 2022 Montenegro was flooded with false reports that bombs had been planted in public buildings, which led to the evacuation of all schools in the country and caused great public concern. Apart from words of general reassurance from the authorities, the public were told only that 'emails were sent from domains whose servers are abroad, and that the authorities are working on identifying the senders'.[348]

Nor does Montenegro have the legal framework or mechanisms required to block content from the Internet, even when online activity appears to be unequivocally criminal in nature, such as hate speech, threats, the promotion of terrorism, the spreading of religious or ethnic hatred and disinformation, child pornography, and the like. This problem is recognized in the new strategy and solutions to it should be prioritized, especially given a marked increase in the dissemination of hatred, discrimination, xenophobia, and misinformation on the Internet, aimed at undermining security and social cohesion.

346 *https://balkans.aljazeera.net/news/balkan/2020/1/17/tim-nato-u-crnoj-gori-zbog-prijetnje-od-ruskih-hibridnih-napada*

347 Montenegro 2021 Report.

348 *https://www.slobodnaevropa.org/a/crna-gora-skole-dojava-bomba-evakuacija/31823151.html*

CYBERSECURITY AND HUMAN RIGHTS FRAMEWORKS

Montenegro has begun the process of establishing a legislative framework to … investigate cases of high-tech computer and cybercrime and to sanction perpetrators

Montenegro has begun the process of establishing a legislative framework to prevent the disruption of information and communication technologies, to investigate cases of high-tech computer and cybercrime, and to sanction perpetrators by reforming its criminal legislation. In addition, the country's Constitution, specifically Article 9, specifies that ratified and published international treaties and generally accepted rules of international law form an integral part of the internal legal order, have supremacy over domestic legislation, and are directly applicable when they regulate relations differently from domestic legislation.

In 2009, Montenegro passed the Law on Ratification of the Council of Europe's Cyber Crime Convention (the Budapest Convention), at the same time ratifying the Additional Protocol on Racism and Xenophobia (CETS 189) and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201). In addition, it began to harmonize its national legal framework with the provisions contained in these conventions.

The competent authority for establishing the legal framework and cybersecurity policy in Montenegro is the Ministry of Public Administration, Digital Society and Media. Legal acts that form the basis of the modern concept of cybersecurity and the way it works in the country are the:

- Law on Information Security[349]
- Data Secrecy Act[350]
- Decree on Information Security Measures[351]
- Code of Criminal Procedure[352]
- Law on Ratification of the Convention on Computer Crime[353]
- Law on the National Security Agency[354]
- Criminal Code[355]
- Electronic Signature Act[356]
- Electronic Communications Act[357]

---

349 https://www.gov.me/dokumenta/fbb730c5-8c62-47e3-863f-cfaae9631b8d
350 https://www.gov.me/dokumenta/c1ac4c4d-e914-47f7-8f61-49d1bf85560e
351 https://www.gov.me/dokumenta/c3b1ba84-8d7b-4baf-914c-3913b358bb2d
352 https://www.paragraf.me/propisi-crnegore/zakonik-o-krivicnom-postupku.html
353 https://wapi.gov.me/download/fe845b44-f208-444b-9ff1-3a96b6ce0983?version=1.0
354 http://www.anb.gov.me/ResourceManager/FileDownload.aspx?rid=194322&rType=2&file=ZAKON%20O%20ANB.pdf
355 https://www.gov.me/dokumenta/5bd66a1b-ad2a-4801-ae8a-e025016691f0
356 https://www.gov.me/dokumenta/040e9f79-f385-49bd-9773-6a77cb7e8f40
357 https://www.gov.me/dokumenta/207dd619-58fc-4d2e-a033-e31642675807

- Electronic Commerce Act[358]
- Cyber Security Strategy of Montenegro 2013-2017, 2018-2021, and 2022-2026[359]

The national CIRT receives daily reports of incidents of various kinds (attacks on websites, Internet fraud, abuse of profiles on social networks, etc.), but it believes that the true number of cyber incidents is much greater than what is reported, as users tend not to report disturbing incidents online to official bodies.

CIRT encourages citizens to report incidents via its own website, and issues notices and warnings about Internet scams and cyber attacks. In 2021 it ran public campaigns warning about phishing, data protection and security of devices, and the need for caution when shopping online. It also ran earlier campaigns aimed at protecting children and youth. However, it is clear from publicly available sources that there have been very few (if any) special campaigns focused specifically on human rights, discrimination, or violence.

The various challenges have yet to be addressed and solutions found that would meet EU and international standards. One example is that in the EU rules on the protection of personal data are very strict; while cyberspace is an ideal arena for the misuse of personal data, in the EU such misuse is very punishable. However, Montenegro has not harmonized its legislation with the EU's General Data Protection Regulation for personal data (GDPR 2016/679), which is why Montenegrins cannot be considered to have the same level of personal data protection or ability to exercise the right to privacy as citizens of EU countries.[360]

Furthermore, human rights have not yet been adequately considered in the development of the regulatory framework for cybersecurity. Even the newly adopted strategy does not acknowledge that cybersecurity is essentially a human rights issue and should be treated as such. In relation to identified problems, hate speech and the spread of ethnic and religious hatred are mentioned in a few places in its pages, but conceptually the strategy does not demonstrate any ambition to apply human rights-based approaches to cybersecurity laws, policies, and practices.

Cybersecurity and the right to privacy

The protection of personal data in Montenegro is guaranteed by the Constitution, ratified international treaties, and national legislation, primarily the provisions contained in the Law on Personal Data Protection and the Law on Free Access to Information.

The intention is that the new Law on Personal Data Protection will be harmonized with the GDPR and the personal data of Montenegrin citizens will be protected in the same way as in the EU. However, Montenegro has not yet signed the 2018 Council of Europe Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[361]

358 https://www.gov.me/dokumenta/c46f2c6b-a0bc-459c-8086-00c618d3a4be
359 https://www.gov.me/dokumenta/8a2de214-c58e-4524-9196-c08886f5829b
360 https://wapi.gov.me/download-preview/97751303-14b4-49f3-b428-911f09728b46?version=1.0
361 Montenegro 2021 Report.

The supervisory role in the field of personal data protection is the remit of the Agency for Personal Data Protection and Free Access to Information[362], whose administrative capacity needs to be further strengthened.[363]

In one illustration of the challenges facing the sector, in March 2020 the government itself violated the right to privacy and the protection of personal data by publishing lists of persons in self-isolation during the COVID-19 pandemic. According to the non-governmental organization (NGO) Human Rights Action (HRA), the personal details of at least 2,000 people were released.[364] After the Government published the names and addresses of people under health supervision, an application (https://crnagorakorona.com/home) of unknown authors appeared, through which it was possible to locate the position of people in self-isolation. Lists of people in self-isolation were also published by some print and electronic media. The system of personal data protection clearly failed in this case, with the Agency for Personal Data Protection endorsing the government's actions. When the lists were published, the ombudsman, the Protector of Human Rights and Freedoms of Montenegro, reacted by saying that 'there [was] no possibility to react' and that 'he [could] not interfere in the work of other independent and autonomous bodies'. However, only two months later he asked the Ministry of Public Administration to conduct a detailed investigation.[365] In October 2021, the High Court in Bijelo Polje issued the first legally binding verdict that the state, by publishing lists of people in self-isolation, violated the right to privacy and protection of personal data.

At the beginning of April 2021 a list of 62 people in Podgorica suffering from coronavirus became public, along with their ID numbers. As a consequence, a single employee of the Podgorica Health Center was prosecuted, but was released in the first instance. During the criminal proceedings, it was proven that special categories of personal data had been sent outside the health information system via email, without any protection through encryption, contrary to regulations.[366]

The NSA has also been accused of unjustifiably violating the right to privacy. In 2021 criminal charges were filed against the agency's former director Dejan Peruničić alleging abuse of office, illegal wiretapping, and surveillance conducted between January and September 2020 of several then opposition leaders, the Serbian Orthodox metropolitan, and two journalists critical of the former government.[367]

The Law on Data Secrecy sets out a system for determining the confidentiality of data, along with access to classified data, the storage, protection, and use of such data, and record-keeping. Classified information is defined as information that, if disclosed to an unauthorised person, could have harmful consequences for the security and defence or the foreign, monetary, or economic policy of Montenegro. This law sets out the conditions and determines what is considered to be classified information. Also considered to be confidential is the secret information of a foreign state or of an international organization, which is marked as such and submitted to the competent authorities in Montenegro.[368]

Civil society organizations (CSOs) have been warning for years that 'restricted' labels of secrecy are used unjustifiably in Montenegro to limit access to public information. In addition, amendments to the 2017 Law on Free Access to Information have degraded the public's right to access information. The NSA and the

---

362 *https://www.azlp.me/me/agencija*

363 Montenegro 2021 Report.

364 *https://www.vijesti.me/vijesti/drustvo/574937/drzava-krsila-pravo-na-privatnost*

365 *https://www.vijesti.me/vijesti/drustvo/543643/bivsa-vlada-masovno-krsila-pravo-na-privatnost*

366 *https://www.vijesti.me/vijesti/drustvo/543643/bivsa-vlada-masovno-krsila-pravo-na-privatnost*

367 U.S. Department of State, *2021 Country Reports on Human Rights Practices: Montenegro* (Bureau of Democracy, Human Rights, and Labor: 2021).

368 *https://www.gov.me/dokumenta/c1ac4c4d-e914-47f7-8f61-49d1bf85560e*

Ministry of Defence can have information of public importance declared secret without any judicial control. The NGO MANS has urged the new government to lift these restrictions and return to previous, more open solutions.[369]

Cybersecurity and freedom of expression

The new cybersecurity strategy prioritizes amendments to the Criminal Code and the Criminal Procedure Code of Montenegro. Amendments to the Criminal Code will help towards sanctioning the criminal offence of spreading and transmitting false news and misinformation, while amendments to the Criminal Procedure Code should improve and facilitate investigative procedures.

Montenegro has no authority that is able to analyse and shut down websites from which crimes are committed, in particular crimes involving child pornography, xenophobia, terrorism, and spreading religious and national hatred, and crimes related to the grey economy. Nor are Montenegrin ISPs able to shut down subdomains or to disable access to sites from which criminal acts are committed.

The new strategy envisages amendments to the existing Law on Electronic Communications, in order to identify technical possibilities for shutting down or blocking subdomains, that is, preventing access to websites from which criminal acts are committed or which violate the provisions of the Criminal Code. However, this is not only a technical but also a legal issue, and special attention should be paid to defining the legal basis for these actions and carefully determining the authority whose decisions will enable content to be blocked on the Internet.

The strategy also envisages amendments to the Criminal Code in order to recognize and sanction a criminal offence of creating and disseminating false news and misinformation via the Internet. In recent years a number of journalists and other individuals have been arrested for allegedly publishing fake news, and charged with 'causing panic and disorder'. However, proceedings have been selective and not all creators of fake news have been treated in the same way. In 2020 the NGO HRA submitted to the Constitutional Court of Montenegro an initiative to review the constitutionality of this article of the Criminal Code, claiming that it was imprecise and allowed arbitrary interpretation, to the detriment of human rights and freedom of expression.[370] Although it is this very lack of precision that makes it necessary to consider making this criminal offence, in this case too special care should be taken to ensure that individuals are not prosecuted for inaccurate statements that do not call for violence and do not constitute hate speech, as this is an excessive restriction on freedom of expression contrary to European human rights standards.

Cybersecurity and freedom of assembly

Cyber attacks on media portals are common, and almost all of the more widely used portals have been targeted in recent years. In addition to the media, the latest Serious and Organized Crime Threat Assessment (SOCTA 2022) from Europol estimates that distributed denial-of-service (DDoS) attacks are

369 https://www.vijesti.me/vijesti/politika/608778/mans-pozvao-vladu-da-hitno-usvoji-izmjene-zakona-o-slobodnom-pristupu-informacijama

370 https://www.pobjeda.me/clanak/hra-trazi-ocjenu-ustavnosti-krivicnog-djela-kojim-se-sankcionisu-lazne-vijesti

common against the information systems of state bodies and legal entities, government websites and portals, and the websites of political parties.[371]

Our interlocutors told us about two recent incidents when hackers interfered with events organized by the media. Hackers broke into two hybrid events and played music, screened inappropriate illustrations and obstructed work. It turned out that both these events had a common feature in that the invitations to them were published online through social networks. Organizers reacted and solved the problems, but omitted to report these incidents as they were caught unprepared.

Our interlocutors pointed out that the digital security of journalists is rarely discussed and that few resources are invested in educating journalists and other media workers; it is clear that technical assistance and support for education are needed in this area. However, because of the importance of journalism to democracy and human rights, and the fact that the media are recognized as a group that is particularly vulnerable to cyber threats, strategic and policy documents should also consider state intervention in the form of special support for the media to help them resist these threats.

During the 2016 parliamentary elections, several important websites were the target of cyber attacks, including news portals and the websites of political parties and NGOs. The website of the Center for Democratic Transition (CDT), an NGO that had accredited election observers deployed around the country, suffered constant DDoS attacks for days in the lead-up to polling day. Monitoring systems established that the attacks came from a large number of different IP addresses and from multiple countries.

On election day itself the Agency for Electronic Communications and Postal Services (EKIP) ordered all operators to temporarily suspend the messaging applications Viber and WhatsApp; the official reason it gave was that these services were sending spam or unlawful marketing material. This decision was criticized by CSOs as being contrary to the right to freedom of expression and to the Constitution. In 2019, the Constitutional Court ruled that the article in the Law on Electronic Communications that allowed EKIP to order operators to suspend Internet and telephone communications to an unlimited extent if it found this to be 'justified in cases of fraud or abuse' was unconstitutional, and ordered that provision to be repealed.

Various pro-fascist groups in Montenegro have spread hate speech on extreme right-wing portals, in comments below the line on articles, and on social networks, criticizing activists, citizens, and entire nations for anything that they perceive not to fit with their own value systems. Typically, these extremist groups launch waves of stigmatization and abuse aimed at individuals and groups of people, with posts encouraging ethnic and religious hatred, racial and other discrimination, and violence against their targets.[372]

Cyber 'lynch mobs' of this kind often target a specific person, and thus expose them to the threat of violence in real life. Furthermore, there are no effective, proportionate, or dissuasive sanctions available to combat hate speech and hate crimes. Prosecutors often classify such cases as the lesser offence of a misdemeanour against public order, which ignores – either accidentally or intentionally – the motives behind such attacks and thus hides the problem 'under the carpet' in statistics on misdemeanours, which do not recognize ethnic or religious hatred as a motive.

According to data from the Judicial Council, in the period 2017-2020 one last-instance judgement was passed for the crime of inciting national, racial, and religious hatred and the convict got a suspended

371 https://www.vijesti.me/vijesti/crna-hronika/603933/socta-2022-raste-sajber-kriminal-sve-vise-prisutno-dijeljenje-snimaka-seksualnog-zlostavljanja-djece

372 https://www.cdtmn.org/wp-content/uploads/2021/03/Rast-desnicarskog-ekstremizma-u-Crnoj-Gori_WEB-Preview-3.pdf

sentence. The offence was committed using social media networks. In 2021 a total of 15 cases were brought before the courts involving people accused of inciting national, religious, and racial hatred, six of which were received in 2021. By the end of 2021, proceedings were conducted in 11 cases, and eight of them were completely concluded; of these, the procedure was suspended in four cases and convictions were secured in the other four.[373]

Although online media and Internet communications have for years been recognized as channels used to spread hate speech, misinformation, and propaganda, the realm of online media was not regulated in Montenegro until the recent adoption of the Law on Media. The amendments to the law define an online publication (a news portal) as being a media outlet whose content is disseminated via the Internet and which is entered in the media records kept by the Ministry of Culture. Portals are obliged to report their legal information and data on ownership, set rules for comments made by readers and remove illegal content, and so on. However, there are still no sanctions if a portal is not registered, and no solutions have been found in cases where portals share illegal content.[374] [375]

Cybersecurity and anti-discrimination

Montenegrin legislation rarely treats cybersecurity and discrimination as related topics. The Law on Prohibition of Discrimination stipulates that harassment via audio and video surveillance, mobile devices, social networks, and the Internet, which aims at or results in the violation of personal dignity, causing fear, feelings of humiliation, or insult or creating a hostile, degrading, or offensive environment, is considered to be discrimination.[376] The Criminal Code provides for penalties for discrimination and violation of equality in several of its articles.

The definition of the crime of 'inciting national, racial, and religious hatred' includes the prohibition of public incitement to violence or hatred against a group or a member of a group based on race, colour, religion, origin, or nationality. The same article includes a ban on public approval, denial of the existence of, or significant mitigation of crimes of genocide, crimes against humanity, and war crimes in a manner that may lead to violence or incite hatred against a group of persons or a member of a group, if these crimes are established by a final judgment of a court in Montenegro or an international criminal court.

Hate speech is defined by the Law on Prohibition of Discrimination as 'any form of expression of ideas, claims, information and opinions that spreads, incites or justifies discrimination, hatred or violence against a person or group of persons because of their personal characteristics, xenophobia, racial hatred, anti-Semitism or other forms of hatred based on intolerance, including intolerance expressed in the form of nationalism, discrimination, and hostility against minorities'. Such offences are classed as misdemeanours, punishable by a fine.

The Roma are the most disadvantaged minority community in Montenegro and Roma people face enormous risks of discrimination. A large percentage of Roma households do not have the basic household conditions for a decent family life. For example, in a recent research report (*Socio-economic position of Roma and Egyptians in Montenegro*, by the Ministry of Justice, Human and Minority Rights,

373 https://www.cdtmn.org/2022/04/20/na-zataskavati-slucajeve-izazivanja-mrznje/

374 https://seenpm.org/wp-content/uploads/2021/01/Resilience-research-publication-2-Montenegro_Nationall-language.pdf

375 Law on Media (*Official Gazette of Montenegro*, No. 46/2010, 40/2011 – other law, 53/2011, 6/2013, 55/2016, 92/2017 and 82/2020 – dr. law).

376 https://www.ombudsman.co.me/docs/1612165541_zakon-o-zabrani-diskriminacije.pdf

2020),[377] 9.8% of Roma respondents said that their household had no electricity and 11.6% had no water (13.8% had no running water). Eighty per cent of households did not have a computer, which was needed for distance learning during the COVID-19 pandemic. Only 65.5% of households had some form of access to the Internet (via a mobile phone, Wi-Fi router, or in some other way), while only 55.1% of respondents used the Internet every day.

Interviewees from the Roma youth organization Phiren Amenca (Walk With Us) told us that there was much unethical reporting and extreme hate speech against Roma and Egyptian communities online, but they did not have any specific data on breaches of cybersecurity when it came to their communities.

At the beginning of the coronavirus pandemic, discrimination against Roma people was very visible. Hate speech by social media users commonly included claims that Roma people were the first to catch coronavirus because they had poor lifestyles and poor hygiene. Since the pandemic many Roma people have been left without income or access to education and social and health care. However, some Roma settlements have not had access to running water for years prior to that.

In cases brought before the ombudsman in 2020, there were 19 pending that involved discrimination on the grounds of ethnicity and a connection with a minority people or a minority national community.[378]

Hate speech aimed at the LGBTIQA+ population is also common in media and information spaces. There have been nine Montenegro Pride marches to date since 2013, but there is still widespread discrimination in society. LGBTIQA+ people face abusive attacks on social media networks, often accompanied by threats of violence. The LGBTIQA+ community has been dealing with hate speech and public threats for years, especially on social media platforms such as Facebook and Instagram. The organization Queer Montenegro says that the attacks are most acute around the time of the Montenegro Pride march, when LGBTIQA+ people face the worst kinds of comments and threats, either on their public profiles or on private ones. They are often confronted with graphic descriptions of violence directed at them or their families, accompanied by words such as ‘I know where to find you’, and are forced into a situation where they have to delete their profiles, as it is hard to endure these kinds of threats.

The Law on Life Partnership of Persons of the Same Sex, which was passed in parliament on 1 July 2020,[379] has also been a target of attacks and hate speech. Dating applications, which are widely used in Montenegro, also carry the danger of attacks for this community. As Queer Montenegro explained, abusers often register on such sites simply in order to find an individual and threaten them, in some cases making a screenshot of the conversation and threatening to publish it and publicly ’out’ the person. It is also quite common for people to push their way into the organization’s offices and make direct threats against people there.

One-third of citizens in Montenegro do not want to live in the same country as LGBTIQA+ people, and almost 43 per cent believe that LGBTIQA+ people should not have the same rights as other citizens, according to an EU and Council of Europe survey conducted by the Centre for Democracy and Human Rights (CEDEM) in 2020.[380]

Reporting about migrants in the Montenegrin media is mostly in the form of articles and reports copied and pasted from regional media; very little of it involves original research. This means that in the local context reports about migrants are mostly related to a specific event. An analysis of narratives that

377 https://www.gov.me/dokumenta/ac3e91ce-6f24-4aad-b648-70d51de2559e

378 https://www.ombudsman.co.me/docs/1619074992_izvjestaj_01042021.pdf

379 https://www.slobodnaevropa.org/a/30701060.html

380 https://www.portalanalitika.me/clanak/trecina-crnogorskih-gradana-ne-zeli-da-zivi-u-istoj-drzavi-sa-lgbti-osobama

contained hate speech and misinformation, published jointly by the Media Institute of Montenegro (Podgorica), SEENPM (Tirana), and the Peace Institute, Ljubljana,[381] found that comments by readers, which have been identified as a problematic segment of online media, included calls for physical violence against migrants, content ridiculing their situation, and broader conspiracy theories such as the goal of refugee movements being the 'Islamization of Europe'.

Online violence against women is not an isolated phenomenon; rather it is located in a broader social context of gender inequality and discrimination against women and girls. Because of this, in order to understand digital violence it is crucial for us first to pause in order to examine what gender-based violence (GBV) is, because the aggression and attacks experienced by women in their online interactions are nothing other than an extension of the violence that has affected them in all spheres of their lives for many years.[382] In Montenegro, for example, women who dare to get involved in politics and to express their own opinions are frequently targeted with abuse and misogynistic attacks. A new kind of pattern has recently emerged: insulting, humiliating, abusive, and sexist comments targeting almost every woman who dares to think differently from the herd, including state officials.[383]

WAYS FORWARD

First and foremost in Montenegro, it is necessary to work actively to raise awareness of the fact that cybersecurity is a human rights issue. There is a need to promote an open, free, and stable cyberspace realm where the rule of law applies fully and human rights and fundamental freedoms are respected. This means protection from Internet shutdowns that deny people access to information and the ability to express opinions. But it also means taking responsibility for behaviour in cyberspace and protection from online violence, discrimination, and hate speech.

Accordingly, an expert review is required of existing laws and other regulations that govern issues at the intersection of cybersecurity and human rights, to measure them against best standards in this area and good practice and to make recommendations for improving the legislative framework. Ideas have already been put forward in strategic documents and public initiatives about how to improve criminal, media, electoral, and other legislation in the context of hybrid threats, misinformation, and attempts by foreign actors to interfere. All these initiatives should be viewed through the prism of human rights. It is also necessary to improve legislation that protects personal data, along with laws that guarantee access to information.

Sufficient financial resources need to be provided in order to implement existing strategic documents and laws; this has not been the case to date. It is especially important in light of the shortage of experts and professional staff in the field of cybersecurity. There will be a constant need to invest in the recruitment, education, and upgrading of skills of such personnel.

It is necessary to work on improving media literacy. As one interlocutor told us, 'People need to learn to behave in cyberspace as they do in physical spaces, only with much more attention to their surroundings.'

381 *https://seenpm.org/wp-content/uploads/2021/01/Resilience-research-publication-2-Montenegro_Nationall-language.pdf*

382 Organization of American States (OAS), *Online gender-based violence against women and girls: Guide of basic concepts, digital security tools, and response strategies* (OAS, 2021).

383 *https://docs.google.com/viewerng/viewer?url=https://www.cdtmn.org/wp-content/uploads/2022/05/WEB_Vidimo-li-slona-MNE-1.pdf&hl=en*

The state must create a legislative framework and strengthen the capacities of authorities in charge of this framework, as well as forging stronger public-private partnerships.

In addition, in order to achieve these goals, it is necessary to build an environment of trust. This is needed in particular to help build partnerships between the state and the private sector. It is a process that requires a lot of time and effort and an active approach to communication, coordination, and education.

CHAPTER 5

NORTH MACEDONIA

Driving Implementation to Strengthen Stakeholder Inclusion

By Bardhyl Jashari, Goce Arsovski and Elida Zylbeari | Metamorphosis Foundation

CHAPTER 5

NORTH MACEDONIA – DRIVING IMPLEMENTATION TO STRENGTHEN STAKEHOLDER INCLUSION

CYBERSECURITY CONTEXT IN NORTH MACEDONIA

Strategic documents

North Macedonia is slowly but steadily working towards developing a secure cyber environment. In 2018, the government made an important step forward in the field of cybersecurity by adopting the National Cybersecurity Strategy 2018-2022, including an Action Plan – both of which prioritized addressing cyber threats and improving cybersecurity. This paper aims to foster the development of a safe, secure, reliable, and resilient digital environment in the country. It defines the main stakeholders in this field, and identifies goals, measures, and activities to support the realization of the objectives outlined in the strategy's Action Plan.

The country's efforts to develop a cybersecurity legal and institutional framework also align with its efforts to ensure that its legislation conforms with European Union (EU) and NATO standards and protocols. Most notably, the government of North Macedonia is working to create a new piece of legislation[384] called the Law on Security of Networks and Information Systems, which is expected to comply with the EU Network and Information Systems (NIS) Directive. In addition, in February 2021, North Macedonia signed a memorandum of understanding[385] with NATO that aims to facilitate the exchange of information and best practices on cyber threats. The Global Cybersecurity Index for 2020[386] noted these efforts, as well as the country's progress, ranking North Macedonia in 38th place out of 182 countries.

Cybersecurity initiatives in North Macedonia are also in line with commitments made within the framework of the Digital Summit for the Western Balkans (26-28 October 2020) and the multi-annual Regional Economic Area Action Plan for the Western Balkans, which supports the region's digital integration. As

384 Consultations are still ongoing. For more information, visit: *https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=51471*

385 NATO, *NATO and North Macedonia strengthen responses to cyber threats*, 19 February 2021.

386 International Telecommunication Union (ITU), *Global Cybersecurity Index 2020*.

part of the Berlin Process,[387] the economy ministers pledged to strengthen cooperation with the business sector in various areas, including by establishing digital infrastructure and interconnection. On 6 October 2020, the European Commission's Economic and Investment Plan for the Western Balkans identified investing in digitalization a key priority.[388]

The Cyber Defence Strategy[389] is another key document in the field of cybersecurity; the strategy was developed by the Ministry of Defence in accordance with the National Cyber Security Strategy, the EU Cybersecurity Strategy and Policy, and NATOs' commitment to ensure a safe, reliable, and resilient digital environment. The Cyber Defence Strategy aims to develop and strengthen capacities and capabilities to actively monitor and reduce the impact of cyberspace threats and attacks in order to protect national interests.

Cybersecurity legal framework

Besides the National Cyber Security Strategy (2018-2022), which provides the strategic framework for the advancement of cybersecurity in North Macedonia, a number of legal acts are relevant to cybersecurity in the country. The Agency for Electronic Communications (AEC) provides regulations – developed in 2015 and updated in 2019 – to ensure the security and integrity of public electronic communication networks and services and to outline the steps that operators should take in the event of a security breach of personal data.[390]

The Law on Electronic Communications established the National Centre for Computer Incident Response (MKD-CIRT) as a separate unit of the AEC[391] to institutionalize the protection of network and information security, especially for entities with critical infrastructure. State institutions should harmonize their internal security measures in consultation with the CIRT. The CIRT website explains the procedures for requesting guidance and assistance,[392] which now need to be applied by institutions.

Other laws are also relevant to addressing cybersecurity issues and ensuring a secure cyberspace environment. The Criminal Code of North Macedonia deals particularly with cybercrime and crimes committed using computer systems, as well as with the collection of digital evidence by law enforcement authorities.

Furthermore, in 2018, reforms to the system in place for the interception of communications paved the way for the approval of a new Law on Interception of Communications and the amendment of the Law on Electronic Communications. As a result, the Administration for Security and Counterintelligence (UBK) was no longer able to directly access citizens' telecommunication traffic or play a mediatory role in the interception of communications – a request that formed part of the European Commission's 2015 Urgent Reform Priorities.[393] The Law on Interception of Communications allows for the interception

---

387 The Berlin Process, *https://www.berlinprocess.de/*

388 European Commission, *Western Balkans: An Economic and Investment Plan to support the economic recovery and convergence* (Brussels: EC; 6 October 2020).

389 Ministry of Defence, *Cyber Defence Strategy*, 2021.

390 Official Gazette of the Republic of North Macedonia, No. 92, 13 May 2019.

391 National Centre for Computer Incident Response (MKD-CIRT), *https://mkd-cirt.mk*.

392 Available at *https://mkd-cirt.mk/en/*.

393 European Commission, *Urgent Reform Priorities for the Former Yugoslav Republic of Macedonia*, June 2015. *http://www.merc.org.mk/Files/Write/KeyDocuments/01106/2015/sq/urgent_reform_priorities-june-2015.pdf*

of communications in order to detect and prosecute perpetrators of crimes, as well as to protect the country's defence and security interests – both justifications are in line with the Constitution and the Urgent Reform Priorities.

Regarding the fundamental right of citizens to personal data protection, the general framework for applying of this principle is defined by two provisions of the Constitution of the Republic of North Macedonia: Article 18 stipulates that '[t]he security and confidentiality of personal information are guaranteed. Citizens are guaranteed protection from any violation of their personal integrity deriving from the registration of personal information through data processing', and Article 25 prescribes that '[e]ach citizen is guaranteed the respect and protection of the privacy of his/her personal and family life and of his/her dignity and repute'.

The new regulation on personal data and privacy protection grants citizens more power by allowing them to exercise their right to control the processing of their data.

The Law on Personal Data Protection – the most important piece of legislation in the area of privacy – was initially enacted in 2005. The law established a new concept in North Macedonia: the right to privacy – for the first time – and specifically the protection of the personal data of citizens in the country's legal system. A new Law on Personal Data Protection in North Macedonia was adopted in February 2020 to comply with the EU General Data Protection Regulation (GDPR). Legal entitles were granted a transitional period of 18 months to comply with the new law and, as of 24 August 2021, it is in full effect. During the transitional period, the Agency for Personal Data Protection delivered generic training sessions for legal entities but did not campaign to raise citizens' awareness of their new rights. The new regulation on personal data and privacy protection grants citizens more power by allowing them to exercise their right to control the processing of their data. The new data protection law also applies to many entities that were not subject to the previous data protection legislation, especially online businesses that process individuals' personal data in North Macedonia.

The ratification of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the ratification of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and cross-border data flows, are also part of the legal framework for personal data protection in North Macedonia.

Another important law for the protection of human rights is the Law on Operational-Technical Agency, which enabled the establishment of the Operation-Technical Agency (OTA). Since November 2018, OTA has acted as mediator between authorized bodies for the interception of communications and telecom operators to avoid concentrating power in one authority and to ensure that the interception of communications is based only on laws and relevant court decisions.

Other relevant laws

Although most areas of information society development are regulated, the implementation of laws remains weak, often for objective reasons. This is an enduring challenge not only for the development of digital services but also for cybersecurity, as it requires coordination between institutions, along with the adaptation and harmonization of pertinent laws. An illustrative example of this issue is the inability of citizens to use electronically generated documents to exercise their rights. Printed documents obtained electronically are not accepted in legal transactions by certain banks, notaries, or universities. The use of electronic documents is, however, regulated by the Law on Electronic Documents, Electronic Identification

and Confidential Services, which stipulates that they have the same legal validity as paper documents. While they should therefore be accepted in legal transactions by all legal entities, the rules in this area are not harmonized and there is no clear guidance on how to address this issue and whether the stipulations will be applied in practice. Further research and consultations are needed in order to precisely ascertain what concrete actions need to be taken to spur the institutions to improve the situation. In practice, whether electronic documents are considered valid by a bank or notary largely depends on individual decisions.[394] The rejection of electronic documents often occurs for basic documents – such as a birth certificate or a certificate from the Cadastre – which must also be notarized, once printed, in order to be validated. The situation is contradictory: state institutions persuade citizens (who may lack the necessary digital skills or literacy) to use e-services but do not allow them to do so in practice,[395] which increases distrust towards institutions and creates a sense of individual powerlessness.[396]

Other important laws are the Law on Electronic Management and Electronic Services, which provides standards and norms for information systems security in the public sector, and the Law on Electronic Data Form and Electronic Signature. In 2019, the Republic of North Macedonia enacted the Law for Electronic Documents, Electronic Identification and Confidential Services, which is in line with Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market. The new law will replace the current law.

Relevant institutions

The Ministry of Information Society and Administration (MISA) has the mandate to create policies and laws in the area of cybersecurity and coordinates all initiatives related to information society development in North Macedonia.

The AEC was established under the Law on Electronic Communications in 2005 (Official Gazette no. 13/2005) as an independent regulatory body for the electronic communications market in North Macedonia. Besides regulating the electronic communications market and ensuring high-quality services and a competitive market in the telecommunication sector, the AEC is responsible for the security and integrity of public communication networks. The agency's rulebook – developed in 2015 and amended in 2019 – provides regulations for ensuring the security and integrity of public electronic communications networks. It also outlines the steps that operators should take in the event of a security breach of personal data.[397]

Established as an organizational unit of the AEC, MKD-CIRT prepares rulebooks, manuals, and other policies, and derives its mandate from the Law on Electronic Communications.[398] It serves as the official national point of contact and coordination in dealing with cybersecurity incidents in networks and information systems, and identifies and responds to cybersecurity incidents and risks.

---

394 Metamorphosis Foundation, *For Faculties, Banks and Some Notaries, the Electronic Certificate is an Unsolvable Enigma*, 5 January 2022.

395 Focus group with representatives of civil society organizations (CSOs), held on 5 April 2022.

396 Institute of Social Sciences and Humanities, *Digitalization as a Path of Real Citizen-oriented Administration: Decentralization of Processes as a Means of Accelerated and Effective Reform*, 2 September 2021.

397 Official Gazette of the Republic of North Macedonia, No. 92, 13 May 2019.

398 Law on Electronic Communications, *https://cutt.ly/1ntvcvz.*

The MKD-CIRT[399] website includes several warnings about phishing campaigns that pose a potential risk to citizens in North Macedonia. As well as safety tips, it includes detailed descriptions of the 'attacker' and clear guidelines on how users can recognize, avoid, and protect themselves from these types of threat. Awareness campaigns and alerts on potential risks – whether communicated through social media platforms or through an MKD-CIRT application – would make these warnings more accessible to citizens and allow them to be informed in a timely manner.

MKD-CIRT provides a service for verifying the security of web applications. The service is intended for organizations and constituents of MKD-CIRT from the public and governmental sector and bodies of state administration.[400] Moreover, MKD-CIRT plays an important role in affirming computer security by organizing hackathons on this topic.

The AEC's annual report does not provide any information on the activities of MKD-CIRT. It would therefore be helpful to have a more detailed overview of its activities, whether within or separate to the AEC report.

The Personal Data Protection Agency (DPA) is the national regulatory authority that oversees the implementation of the Law on Personal Data Protection – the principal legal instrument in the area of data protection.[401]

The Ministry of Defence is responsible for and has the capacities to ensure the effective functioning of the national defence system, including the following aspects: defence preparations; overall support provided by the Army of the Republic of North Macedonia; strategic defence planning; efficient defence resource management; the development of military capabilities for conducting defence missions; international defence cooperation; NATO integration; participation in European security and defence policy; and ongoing contributions to international operations. The ministry is also in charge of the implementation of the Cyber Defence Strategy. Pursuant to the Defence Law, cyber defence is considered part of the North Macedonia's defence strategy. The law defines the defence of the state as a system for defending the country's independence and territorial integrity, as well as for protecting the lives of citizens and their property from external attack. This includes the construction of an effective national defence system; training for and the deployment of relevant forces, as well as assets; and participation in NATO's collective defence system.

The Ministry of Interior is another important institution that is relevant to both the field of cybersecurity and the field of human rights. It performs functions and duties related to the national and public security system, including performing surveillance under its mandate and other security duties as stipulated by law. The Department for Cyber Crime and Digital Forensics at the Ministry of Interior is currently responsible for conducting national and international investigations into cybercrime, such as accessing a computer system without authorization, making and using a fake bank card for payment, producing and distributing child pornography, misusing personal data, and committing internet fraud. The department conducts forensic analysis of various types of devices containing electronic evidence and submits reports on the evidence found to the judicial authorities. It is also responsible for developing standard operating procedures for investigations in the field of computer crime, forms for the forensic analysis of electronic evidence, a methodology for computer crime investigations, and a strategy for computer crimes.

---

399 Available at *https://mkd-cirt.mk*.

400 National Center for Computer Incident Response (MKD-CIRT), web application checking service: *https://mkd-cirt.mk/usluga-za-proverka-na-veb-aplikacii/.*

401 See: *https://www.dzlp.mk/*

CYBERSECURITY AND HUMAN RIGHTS IN NORTH MACEDONIA

Cybersecurity and personal data protection

Privacy is a human right and guarantor of human dignity, and is key to maintaining personal security, protecting identity, and promoting freedom of expression in today's digital environment. In the past year, and particularly after the COVID-19 outbreak, state institutions in North Macedonia have moved towards providing more services online. There is, however, no common framework or standards for institutions to develop digital services, and they use a variety of different approaches to deploy new digital services. There is therefore a clear need – confirmed by relevant stakeholders during consultations for this study – to establish a model that includes policies, procedures, and technical specifications to ensure personal data protection and security. Most current e-services in North Macedonia lack Privacy Impact Assessments, which enable the design of new e-services that ensure privacy and transparency – usually linked to the publication of privacy policies that do not comply with the minimum GDPR and national law requirements for informing the data subjects (citizens – right holders). The European Commission Progress Report notes that most of the recommendations from the DPA are not fully implemented by the institutions concerned, and not all laws and by-laws regulating personal data processing are submitted to the directorate before adoption.

The country's efforts to comply with the GDPR requirements were delayed for several reasons and the new Law on Personal Data Protection was adopted in February 2020, instead of September 2019. As the COVID-19 outbreak began two weeks later, the planned activities for raising awareness among citizens and legal entities, as well as for ensuring compliance with other sectoral laws, changed. The transitional period for compliance expired in August 2021, although a number of activities have yet to be carried out by the agency, as well as institutions subject to the law (for example, to develop privacy impact assessment methodologies and adapt internal policies and documents according to the new law). No awareness campaign was carried out after the adoption of the new law and information was not made publicly available; instead, the DPA's activities focused solely on legal entities.

The Strategy on Personal Data Protection 2017-2022[402] calls for establishing a sustainable system for personal data protection, conducting ongoing public awareness-raising activities, and strengthening a culture of personal data protection. It also aims to enhance compliance among controllers and processors of personal data by improving risk assessment tools and developing privacy-by-design processes and solutions to support legal entities in building personal data protection systems.

Cybersecurity and freedom of expression

Several documents protect freedom of speech in North Macedonia, starting with the Constitution, which guarantees freedom of expression, freedom of speech, the right to access to information, and the establishment of institutions for public information. It also ensures the freedom to receive and transmit information, and bans censorship.

402 The strategy's objectives are outlined at https://dzlp.mk/sites/default/files/dzlp_strategija_mk.pdf.

The Criminal Code is in line with Article X of the Additional Protocol to the Council of Europe's Convention on Cybercrime,[403] and guarantees freedom of expression – unless used to promote hate, decimation, violence, threats, racism, or xenophobia. Freedom of expression, among other universal human rights, is also mentioned in the National Cyber Security Strategy and is universal and applicable to cyberspace.[404]

While the Constitution guarantees freedom of speech and bans censorship, the country lags behind in harmonizing media legislation with the standards of the EU

While the Constitution guarantees freedom of speech and bans censorship, the country lags behind in harmonizing media legislation with the standards of the EU – which it intends to join. The latest report[405] of the European Commission for North Macedonia emphasized that 'attention should be paid to the labour rights of journalists. The recommendation is to impose a zero-tolerance approach to intimidation, threats and violence against journalists in the course of their profession and to ensure that perpetrators are punished.'

Impunity for attacks on journalists, as well as the lack of a culture of public communication, also poses a challenge to freedom of expression and freedom of the media and leads to violence against journalists. The latest publication of the Association of Journalists of Macedonia (AJM), *Attacks on Journalists and Media Workers 2017-2021*, states that attacks on media workers are becoming an increasing problem and that in the last two years, there have been more attacks on female journalists than on male journalists. According to the AJM, the attacks often use sexist rhetoric, giving these attacks another dimension as they not only refer to the work of journalists, but also seem to be gender motivated. Furthermore, because of the pandemic, online threats against journalists have increased significantly. The attacks on journalists are often traced back to anonymous profiles on social networks or so-called 'bots' that use virtual private networks (VPNs) – i.e. they can easily hide their digital trace and it is hard for even the competent institutions to locate them. Experience has shown that the procedure for locating online attackers is difficult and slow. Cooperation between domestic law enforcements, as well as with international institutions and companies, is key, as is the use of international legal assistance instruments in gathering information during the pre-investigation procedure. It is important to underline that no official court case has been issued by the Public Prosecutor's Office or the Ministry of Interior, despite the fact that some of the threats were reported to the police.

Judicial abuse of the Law on Civil Responsibility for Defamation leads to self-censorship in the media. Lawsuits are used as a tool for intimidation and to put pressure on independent media. While the Code of Conduct and a media self-regulator both provide an ethical framework that encourages good journalistic practices, implementation remains poor.[406]

403 Council of Europe, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* (Strasbourg: Council of Europe; 2003), p. 2.

404 National Cyber Security Strategy 2018-2022, p. 15. *https://www.mioa.gov.mk/?q=en/node/2379*

405 European Commission, *North Macedonia 2021 Report* (Strasbourg: European Commission; 19 October 2021), p. 6 and p. 28.

406 Reporters Without Borders, *North Macedonia*, 2021.

Cybersecurity and hate speech

The consultations with civil society organizations (CSOs), the media, and government representatives confirmed that hate speech in North Macedonia, particularly online, has increased in the last two years (2020-2021). The Association of Journalists identified hate speech as a challenge; it was also cited by other CSO representatives several times during the course of the interviews. The lack of institutional awareness when combating online hate speech – which in turn affects the victim's level of digital security and may also compromise personal data (i.e. doxing[407]) – is discouraging to every party involved. As the president of the Association of Journalists noted, '[t]he current legal framework always requires an action by the citizens, from the citizen towards the system (i.e., the courts and prosecution). It should be the other way around; the system should protect the citizen by being proactive in this regard.' At the same time, although often criticized for the inefficient processing of cases related to hate speech, the Ministry of Interior briefly mentioned during the interview that all legal procedures are being followed, and that the right to privacy is being protected when using citizens' personal data. The Prosecutor's Office and the judiciary are also often criticized for being too slow and inefficient in processing cases related to online hate speech.[408]

The regulatory framework regarding hate speech is stipulated in several laws and, in general, conforms to the European Convention on Human Rights standards. The article of the Criminal Code related to 'endangering safety' includes sanctions for those who use computer systems to threaten or commit crimes against other people based on their race, skin colour, origin, national or ethnic background, gender, sexual orientation, language, social background, education, religious or political belief, disability, or age – or on any other ground (art. 144, para. 4). Hate speech is defined in the article as publicly spreading racist and xenophobic ideas or theories through a computer system, or by some other means of public information, to promote or incite hatred, discrimination, or violence against a person or a group (art. 394-g, paras. 1, 2). The code prohibits the approval or justification using a computer system of genocide, crimes against humanity, war crimes (art. 407-a), or racial or other forms of discrimination (art. 417, para. 3).

The Helsinki Committee for Human Rights monitors hate speech on social media networks and in traditional media through the online platform govornaomraza.mk. In March 2020, hate speech incidents increased by 100 per cent compared with the same period the previous year. Of these 773 reported cases, 108 were reported on grounds of political affiliation and 205 on ethnic grounds in 2019-2020.[409] In 2021, 338 cases had been reported on the platform by August, with most of the cases being filed on grounds of sexual orientation, gender identity, or ethnic or political affiliation.[410] There is, however, no unified data-collection process at the national level for online or real-life discrimination or hate-motivated crimes.

In addition, the Law on Audio and Audio-visual Media Services prohibits the broadcasting of media content that endangers national security; calls for the violent destruction of the constitutional order of the state, military aggression, or armed conflict; or incites or spreads discrimination, intolerance, or hatred based on any discriminatory ground (art. 48). The law does not, however, specifically cover online media. The regulator of the media sector – the Agency for Audio and Audiovisual Media Services (AAMS) – has been particularly engaged in the identification and prevention of hate speech and discrimination through

407 Wikipedia, definition of 'doxing': *https://en.wikipedia.org/wiki/Doxing*

408 Available at *https://bit.ly/3llRIxm*.

409 Available at *www.govornaomraza.mk*.

410 Ibid.

media.[411] The agency has also prepared guidelines for monitoring hate speech[412] and, since the end of 2018, has had legal remedies at its disposal to launch misdemeanour proceedings in cases where media outlets violate hate speech provisions. The AAMS can impose several measures when it identifies hate speech in audio-visual media content (art. 48), including the following: a public warning, a request for initiating a misdemeanour procedure, a proposal to revoke the licence, a decision to delete the media outlet from the registry (art. 23); or a fine of up to EUR 5,000 for the legal entity.

The Law on Prevention and Protection against Discrimination defines incidents of discrimination (art. 5) and stipulates protective mechanisms for discriminated persons. The law was passed in October 2020 and provides for the establishment of an independent and professional commission. The commission's objective is to make procedures to protect against discrimination more efficient and access to court/justice easier.

The Defamation Law remains problematic in terms of regulating hate speech as it does not treat online media as subjects of this law. As a result, some judges refuse to conduct cases because the law does not specifically regulate online media. Nor are they regulated through the Law on Media.

While hate speech is prevalent on social media, there are virtually no institutional measures to combat it. The Ministry of Interior and the Sector of Computer Crimes and Digital Forensics has no means of deleting or preventing access to public content placed on the internet or on social media.

Cybersecurity and freedom of peaceful assembly

The right of freedom of assembly guarantees that people can gather and meet – both publicly and privately. The Constitution of North Macedonia states that citizens have the right to assemble peacefully and to protest publicly without any prior announcement or special licence. The exercise of this right may be restricted only during a state of emergency or war. At the same time, North Macedonia is a member of the International Covenant on Civil and Political Rights, which governs the right of peaceful assembly and association. The protection of the right to peaceful assembly also extends to remote participation in, and the organization of, assemblies – including those conducted online. Associated activities that are carried out online or that otherwise rely on digital services are therefore also protected. There is, however, no dedicated national legislation regulating online or digitally mediated assemblies in North Macedonia.

Legitimate grounds for the restriction of the freedom of assembly are prescribed in the Law on Public Gatherings (art. 4). According to this article, the organizer is obliged to prevent an assembly from being held if it poses a risk to the life, health, security, or personal safety of people (or property). At the beginning of the COVID-19 pandemic, North Macedonia informed the Secretary-General of the Council of Europe on 1 April 2020 that it had restricted public assemblies and cancelled all public events, meetings, and gatherings. It stated that the application of these measures 'may influence the exercise of certain rights and freedoms under the Convention and in some instances give reason for the necessity to derogate from certain obligations of the Republic of North Macedonia' under Article 11 of the European Convention on Human Rights. In June 2020, it withdrew the derogation. Complaints to the Ombudsman can be filed by anyone who thinks that their right to assembly has been unlawfully restricted.

411 This is according to a report available at: *https://avmu.mk/wp-content/uploads/2017/05/Vodic-za-monitoring-za-govorot-na-omraza-Mak.pdf*

412 Safejournalists.net, *North Macedonia: Indicators for the Degree of Media Freedom and Journalists Safety in 2021*, p. 9.

In general, several reports – most notably the reports of Freedom House on North Macedonia for 2021 and 2022[413] – state that constitutional guarantees of freedom of assembly are well respected, despite concerns about the integrity of human rights activists when conducting their work. In the Universal Periodic Review of the UN Human Rights Council in 2019[414], the Special Rapporteur on Human Rights Defenders expressed his concern regarding the physical and psychological integrity of those advocating the rights of lesbian, gay, bisexual, transgender, and intersex persons and working to promote equality and non-discrimination, particularly in exercising their right to freedom of opinion and expression and freedom of peaceful assembly.

The media, and online media in particular, plays an important role in exercising the right to freedom of assembly. Besides documenting and reporting about specific gatherings, online media is used extensively to report from the ground in real time. The speed at which this type of reporting occurs often results in content being published without an editorial process. This is both an advantage and a challenge. On the one hand, live reporting on social media enables information to be made available in real time to a wide audience and allows authorities to be held to account for employing disproportionate force towards participants at gatherings or protests. On the other, publishing content with no fact-checking or formal editorial process can lead to the spread of disinformation.

Legislation should be updated to take into consideration the digital sphere and go beyond the traditional means of guaranteeing the right to freedom of assembly.

The digital transformation not only affects how assemblies of people are organized, but also how they are surveilled and potentially repressed. It is therefore important to be aware of the challenges that this new digital environment brings, as well as the appropriate response by all relevant stakeholders. Legislation should be updated to take into consideration the digital sphere and go beyond the traditional means of guaranteeing the right to freedom of assembly.

Cybersecurity and interception of communications

In 2018, the Assembly of North Macedonia passed a law limiting the secret police's surveillance activities. The following year, the Administration for Security and Counterintelligence (UBK) was replaced by the National Security Agency. A Council for Civil Supervision was created to provide additional security sector oversight in 2019 but never started work due to a lack of political will and resources.

The Law on Criminal Procedure defines special investigative measures for the interception of communications.[415] Article 19 specifies how they are regulated and stipulates that these measures – including the monitoring and recording of telephone and other electronic communications – are permitted when it is necessary to obtain data and evidence for criminal procedures, if this cannot be obtained by other means. For one of the special investigation measures,[416] for example, the law states that the

413 Freedom House, *Freedom in the World 2021: North Macedonia*, 2021 and Freedom House, *Freedom in the World 2022: North Macedonia*, 2022.

414 Kubovic, Roman, *UPR 32: Third Cycle of North Macedonia's Periodic Human Rights Review* (Geneva International Centre for Justice; 20 February 2019).

415 Official Gazette of the Republic of Macedonia, Nos. 150/2010, 100/2012, 142/2016, and 198/2018.

416 These measures include surveillance and recording in homes, enclosed or fenced-in areas that belong to home or office space designated as private, or vehicles, as well as the entrance of such facilities, in order to create the required conditions for monitoring communications.

recording shall be stopped if, during the recording, there are indications that statements may be recorded that belong in the basic sphere of private and family life. Any documentation related to such statements shall be destroyed immediately.

It is important to note that the new Law on Interception of Communications has increased the number of authorized bodies for the interception of communications, with the addition of the Military Security and Intelligence Administration in order to protect security and defence interests. The already tight deadline for court approval of requests for the interception of communications on this basis has been reduced from 24 to 12 hours, while the amount of time permitted for court rulings on requests for the interception of communications for the purpose of criminal prosecution has been increased. Communications intercepted on the basis of the protection of defence and security can be used as evidence for criminal prosecution[417] even if it is unrelated to defence and security, according to the Law on Interception of Communications. This is problematic not only because it does not comply with the scope of the court order for the interception of communications, but also because the data is not being used for its intended purpose.

Cybersecurity and anti-discrimination

The Constitution provides for protection against discrimination and states that all citizens are equal before the Constitution and law, and enjoy the same freedoms and rights – regardless of gender, race, colour, national and social origin, political and religious conviction, or property and social status. Until 2010, anti-discrimination provisions were scattered across various laws, including criminal and labour law. A comprehensive Law on Prevention and Protection against Discrimination was adopted in 2020, which introduced a more transparent way of choosing the members of the Commission for Prevention and Protection against Discrimination (CPPD). This law goes beyond the Constitution, with Article 5 offering an open-ended provision ending with 'any other ground' for discrimination.

Although legislation prohibits workplace sexual harassment, the issue persists and most instances go unreported. The Roma people face employment and other discrimination. Footage in September 2020 of a police officer attacking a Roma man in Bitola once again highlighted the routine violence faced by the Roma community in North Macedonia and their marginalized position.

According to Article 50 of the Constitution of North Macedonia, citizens may invoke the protection of fundamental freedoms and rights before the Constitutional Court of North Macedonia, through a procedure based upon the principles of priority and urgency. In practice, however, although these procedures have been invoked, the Constitutional Court has been very reluctant to act in such cases. There is also ambiguity when it comes to addressing discrimination complaints. Various laws specify different types of proceedings for similar cases.

The CPPD and Ombudsperson are only allowed to provide opinions and recommendations. While new methods are being developed to facilitate contact with the Ombudsman (such as an online complaint mechanism), their lack of authority and power to follow up on complaints remains an issue**.** The Ombudsman currently does not have a mandate to act, but only to initiate and request actions by other institutions, and to propose or bring forward recommendations.

The Association of Journalists notes that it has itself, along with individual journalists, been a target of discriminatory actions and threats, usually through social media platforms (such as Facebook and

417 See Article 28 of the law.

Twitter). As for the source of discrimination, they point out that most of the incidents have been gender motivated, but that some have been due to journalists' political views, ethnicity, or sexual orientation.

The government has taken no serious steps to respond to the inequalities that have arisen or worsened because of the COVID-19 pandemic, such as access to healthcare for people regardless of race and ethnicity (for example, for Roma communities – and particularly Roma women). No mechanism was introduced to ensure that the measures to prevent the spread of COVID-19 would not result in any form of discrimination. There are also other areas of concern, including that national legislation has still not been harmonized internally and that underfunding and understaffing prevents national human rights institutions from fully exercising their competences.

In conclusion, more efforts should be made to effectively address hate speech and discrimination in the digital environment, not only to build trust and awareness, but also to tackle prevailing impunity – particularly within the criminal justice system. Besides sporadic initiatives to collect data about hate speech and discrimination cases, such as the platform[418] developed by the Helsinki Committee for Human Rights, a more systemic and comprehensive data collection system for these types of incidents is needed. Such data would enable the identification of areas for intervention to tackle hate speech, harassment, and other forms of discrimination or criminal offences that take place in cyberspace. Finally, the relevant legal framework should be updated and the capacity of institutions strengthened to allow them to respond to emerging human rights challenges in cyberspace and provide equal protection online and offline.

REACTIONS AND RESPONSES TO RECENT CYBER ATTACKS

Several cyber attacks have occurred over the last three years and exposed the shortfalls and gaps in how North Macedonia's authorities are dealing with cybersecurity issues. They also continue to demonstrate a lack of transparency when communicating with the public about these types of attack. The consultations undertaken for this paper with various institutions, human rights activists, and media professionals show that institutions in North Macedonia have failed not only to communicate properly about cyber attacks, but also to fulfil promises made during public statements.

Most recently, the Bureau for Public Procurement has been one of the hardest-hit institutions of North Macedonia – it was still under a ransomware attack at the time of writing (late April 2022). While the institution has not disclosed any details, information available to the public through the media suggests that hackers successfully launched an attack by taking ownership of the public procurement database, including backups.

On the other hand, on 23 February 2022, the Central Bank of North Macedonia released a short statement saying that a hacking attempt had been prevented and that no data breach had occurred. They noted that a similar attempt had been aimed at several privately owned banks in the country. The statement concluded by stressing that 'the integrity and confidentiality of data [was] not compromised'. No further details were communicated to the public or media.

The investigation into the cyber-attack on the website of the State Electoral Commission, which coincided with election day on 15 July 2020, is also now being pursued. The Ministry of Interior stated that the case is under review and that the Sector for Computer Crime and Digital Forensics has taken several steps to clear up the case. Additionally, in a security breach that occurred two years ago, a Greek hacker group calling itself the 'Powerful Greek Army' leaked dozens of email addresses and passwords from staffers

418 Available at www.govornaomraza.mk.

in North Macedonia's ministries of finance and economy. Authorities have not yet determined how the attack happened. These illustrative cases highlight the lack of transparent communication strategies and protocols, as well as a lack of security that leaves North Macedonia vulnerable to possible cyber-attacks – especially from Russian hackers, now that Russia has declared North Macedonia a 'hostile country'.[419] Given that Russian hackers are seeking to target Western countries supporting Ukraine in its efforts to resist Moscow's invasion,[420] this event has raised concerns among institutions and NGOs about possible cyber attacks aimed at North Macedonian institutions and other companies.

In general, institutions do not systematically incorporate additional security measures and protocols after an attack has happened. Nor do they have communication protocols in place to effectively inform the public about these incidents. This failure to proactively provide information creates a vacuum in the public narrative, which is often filled with sensationalist content and conspiracy theories. Most importantly, it increases distrust in state institutions.

INTERVIEW AND CONSULTATION PROCESS

The project team interviewed stakeholders pertinent to cybersecurity and human rights in North Macedonia. Although the interview questions were sent to a larger number of CSOs and state institutions by post, as well as by email and phone, only the eight respondents listed below (in chronological order) had provided their input as of 26 April 2022:

- Agency for Personal Data Protection (APDP);
- Ministry of Justice;
- Macedonian Association of Journalists;
- Health Education and Research Association (HERA);
- Helsinki Committee for Human Rights;
- Roma Women's Rights Initiative;
- Ministry of Interior; and
- Ministry of Defence.

Each of the respondents covered aspects relevant to human rights and cybersecurity, starting with the Ministry of Justice, which has the mandate to propose changes or new regulations that can impact the legal and regulatory framework related to cybersecurity.

---

419 Following the Russian invasion of Ukraine, North Macedonia's parliament voted to condemn the Russian attack and backed EU sanctions against Moscow. The Defence Ministry stated that the country, as a NATO member, would join efforts to offer military aid to Ukraine. As a result, Russia put North Macedonia on its now expanded list of hostile countries. This list of hostile countries was published on 5 March 2022. EURACTIV, *Russia Adopts List of 'Enemy' Countries to Which It Will Pay Its Debts in Rubles*, 8 March 2022.

420 Sabbagh, Dan, *Russian hackers targeting opponents of Ukraine invasion, warns GCHQ chief*, *The Guardian*, 10 May 2022.

HERA and the Helsinki Committee for Human Rights are widely recognized as leading human rights CSOs in the country. Both organizations promote human rights and advocate for gender equality and fair treatment of the lesbian, gay, bisexual, transgender, intersex, queer, and asexual (LGBTIQA+) community. In the past, they have tackled important issues, threats, and challenges related to human rights in the country.

The Journalists Association is the largest body of journalists and media workers in North Macedonia: it advocates for freedom of the media and the safety of journalists, and strives to provide, promote, and protect professional journalistic standards and freedom of expression.

The APDP is instrumental in protecting citizens' personal data by conducting inspections and audits in businesses and other entities that gather, analyse, share, or use the personal data of citizens of North Macedonia. The agency (formerly directorate) is widely recognized as the 'go-to' institution among citizens if they suspect their privacy has been invaded.

All interviewees recognized the importance of cybersecurity and human rights. They not only demonstrated their interest in the subject, but also confirmed the need to mainstream human rights in the expert and public discourse on cybersecurity.

In addition to the interview respondents, the research team conducted several consultation processes during the second round of the data-gathering phase. Such consultations were made with Inkluziva – a prominent CSO advocating for an inclusive approach for people with disabilities – and Eko-svest – another established organization in North Macedonia that tackles issues such as active citizen participation, sustainable energy and transport, and climate change. The CSO Macedonian Platform Against Poverty – which tackles issues related to inequality and social justice, participative democracy, and citizen solidarity – was also consulted. The consultation process as a whole contributed towards a better understanding of the challenges faced by different stakeholders, especially target populations that are susceptive to discrimination, such as women, the Roma community, the LGBTIQA+ community, and people experiencing poverty, among others.

While the consultation process was informed by the interview questions, it followed a less formal and structured approach, focusing on specifics challenges experienced by CSOs and the communities they support.

The following conclusions do not present a complete picture of the cybersecurity landscape in the country, as only a few experts and institutions took part in the interviews and the consultation process. This lack of participation may be attributed to the insufficient openness and transparency of the institutions to discuss sensitive cybersecurity matters. Another, perhaps more relevant, reason is that at the same time as the interviews were conducted, several cybersecurity incidents occurred, directly targeting Macedonian institutions.

It is important to note that some interviewees chose not to answer all the questions posed. The respondents cited their lack of experience or expertise as the primary reason for not responding to questions on certain topics. Although most of the respondents recognized that the issue of cybersecurity and human rights is complex and sensitive, this did not prevent them from answering the questions during the interviews or consultation meetings. It is therefore possible to conclude that respondents did not answer all the questions either because they had not been exposed to or lacked familiarity with the subject matter or because they reflected the low level of awareness of the public on the subject matter.

RECOMMENDATIONS

Recommendations for public actors:

- The Criminal Code should be updated to clearly define the term 'hate speech' to prevent impunity owing to the lack of a definition, and to complete ongoing initiatives to better protect journalists from attacks and tackle online violence and stalking, which is crucial to ending impunity for gender-based violence against women.
- The Media Law should be updated to include online media – currently only broadcasting and print media are defined by the law – which would in turn enable the implementation of other laws pertinent to hate speech and discrimination.
- Amendments to the Law on Prevention and Protection against Discrimination should be adopted to adequately address forms of discrimination occurring in cyberspace and prevent discriminatory automated decision-making.
- Amendments to the Law on Assemblies should be adopted to provide adequate guarantees for online gatherings.
- National policies should be harmonized with international policies.
- A single comprehensive legal framework for cybercrime should be developed.
- Authorities in charge of cybercrime should be modernized.
- Formal procedures should be established for information exchange.
- The government should participate actively in the creation of international cybercrime regulations and standards, as well as their implementation at the national level.
- Continuous education and training should be provided for law enforcement entities in the field of cybersecurity, cybercrime, and electronic evidence.
- A unified and comprehensive data-collection system on discrimination/hate-motivated crimes should be established, addressing both online and offline cases.
- The knowledge and skills of police officers, judges, and prosecutors regarding international standards on human rights in cyberspace should be increased.
- Relevant and competent institutions, bodies, and agencies should implement the regulation related to hate speech in a proactive, nonselective, and impartial manner to improve the effectiveness of institutions and increase citizens' trust.
- The human and technical capacities and resources of the APDP and the CPPD should be increased to enable them to conduct proper systematic investigations into human rights violations in cyberspace.

- Independent regulatory bodies – such as the AEC, the Agency for AAMS, and the CPPD – should increase their level of cooperation and coordination, and establish regular inter-institutional channels of communication, including with the relevant sectors of the Ministry of Interior and Ministry of Defence.
- Public knowledge and awareness of the relevant regulatory bodies, including their role and competencies, should be increased.
- The Ministry of Interior should strengthen its technical and human capacity related to cybersecurity and human rights.
- MKD-CIRT should establish a prompt alert system to inform state institutions and citizens of current or potential risks from cyber-attacks.
- Relevant state institutions – particularly the AEC and MKD-CIRD – should conduct educational and awareness-raising campaigns on cybersecurity in cooperation with CSOs and the media.
- The government should invest in and provide resources to institutions in order to overcome the lack of IT staff, and outdated or lacking technical capabilities in the field of cybersecurity.
- The government, in cooperation with CSOs, should conduct a massive digital literacy campaign.
- The APDP should develop a methodology for performing Privacy Impact Assessments to be used by all state institutions willing to develop digital services.
- Data Protection Officers should be provided with training on challenges related to cybersecurity, artificial intelligence, and risk management and privacy protection.
- Efforts should be made to promote and affirm the role of the Ombudsman in North Macedonia.

Recommendations for NGOs, media, and academia:

- Awareness raising about human rights and cybersecurity awareness is the first necessary step towards sensitizing and engaging all relevant stakeholders in building a cyber-resilient environment that is mindful of human rights. While there are several institutions and organizations that tackle these issues separately (such as the Ombudsman, MISA, MKD-CIRT, and CSOs), these efforts should now work towards one common goal: the protection and promotion of human rights, especially those of vulnerable communities, in the digital world. CSOs and the media have an important role to play in this regard and should join their efforts with those of government institutions to reach all parts of society.
- A multi-stakeholder approach to creating a cyber-resilient society that is mindful of human rights should be used to engage CSOs, the media, and academia in consultations on legislative amendments and strategic policy documents related to cybersecurity and human rights.
- CSO should be provided with increased knowledge and capacities to allow them to competently navigate the digital environment and demand increased human rights protection, while supporting state institutions and other stakeholders as duty bearers responsible for protecting society and citizens.

- CSOs should be enabled to engage and competently voice their concerns about privacy and artificial intelligence – with government, law enforcement agencies, and judiciary institutions, as well as with businesses.
- Human rights violations occurring in cyberspace should be monitored systematically to not only help assess the current situation but also provide a basis for further research and allow activities to be adapted according to specific contexts and needs.
- Public awareness should be raised about forms of discrimination in cyberspace, as well as forms of discrimination recently protected by legislation, in order to encourage reporting and build institutional practices in this regard.
- An awareness-raising campaign should be carried out to inform citizens of their right to privacy and to assist them in effectively identifying and reporting any violations.
- A self-regulation approach to online media should be promoted, according to best practices, to ensure proportionality between accountability for violations and freedom from censure.
- The capacities of journalists and online media platforms with regards to ethical reporting and human rights issues should be strengthened.
- The capacities of CSOs and activists should be increased to allow them to respond to challenges in exercising the right to freedom of assembly in cyberspace.
- Digital security training and support for journalists and activists should be enhanced.
- Capacities of cybersecurity and human rights institutions should be supported to enable an effective response to human rights violations in cyberspace and conduct thorough investigations.

CHAPTER 6

SERBIA

Drawing the Links to Human Rights and Investing in People

By Maja Bjeloš and Marija Pavlović | Belgrade Centre for Security Policy (BCSP)

CHAPTER 6

SERBIA – DRAWING THE LINKS TO HUMAN RIGHTS AND INVESTING IN PEOPLE

INTRODUCTION

Official statistics indicate an increasing trend in the number of cyber attacks and cybercrime cases in Serbia. About 26 million significant cyber attacks on information and communication technology (ICT) systems occurred in 2020 – the most common of which involved attempted intrusions into ICT systems and unauthorized data collection. Serbian citizens also witnessed massive violations of their right to privacy and personal data during the pandemic, as well as an increase in the number of attacks against human rights defenders and political dissidents in the digital and physical space. In late 2021, the idea of using biometric surveillance to counter terrorism and organized crime was reintroduced. However, due to the rapid backsliding of democracy and the rule of law, citizens fear that the new face recognition technologies will be directed against them, rather than against criminals and potential terrorists. Since the beginning of 2022, there have been several attempts to commit internet fraud and steal the identities and data of users of the Raiffeisen Bank and the Post of Serbia. In the most recent incident, a hacker attacked the country's cadastre and shared electronic reports about bombs planted in various public and private institutions, causing widespread concern in society and temporarily disabling the day-to-day work of the institutions affected. Threats to journalists via social networks have also become more frequent.

Cyber attacks are now a part of daily life in Serbia, and threats posed by the internet and social networks are likely to intensify

Cyber attacks are now a part of daily life in Serbia, and threats posed by the internet and social networks are likely to intensify and become more complicated in the future. It is therefore important for state authorities to be prepared to respond to any challenge, risk, or threat quickly and effectively, while respecting human rights and the rule of law. The Belgrade Centre for Security Policy addresses the topic of cybercrime from the perspective of human rights and the rule of law. In this context, the centre conducted a baseline analysis and 22 interviews with governmental and non-governmental stakeholders in Serbia, from mid-January to end March 2022, to assess the level of legal and institutional development of the competent authorities in the area of information and cyber security, as well as the challenges facing cybersecurity and human rights in the country.

CYBERSECURITY CONTEXT IN SERBIA

Legislative and strategic framework

Over the past seven years, the Serbian government has worked intensively in cooperation with the private sector and civil society to define the legislative and strategic framework for the area of ICT security. The foundations and architecture of the ICT security system in Serbia were laid in 2016, while in the past three years the legal and strategic framework has been reviewed, taking into consideration practical experience, as well as European Union (EU) directives and guidelines.

The area of ICT security in Serbia is regulated by the umbrella Law on Information Security[421] from 2016, defining the rights, duties, and responsibilities of all legal entities and state authorities managing and using ICT systems. This law details the security safeguards for challenges, risks, and threats related to ICT systems. It also specifies the bodies responsible for protecting these systems, the forms of coordination among these actors, and the implementation of the prescribed measures. Three years after this law was promulgated, it was amended to improve its implementation and address issues identified in practice. In the area of cybersecurity, the by-laws enabling the implementation of this law are of particular importance, as well as other laws in Serbia's legal systems, such as the laws regulating personal data protection, critical infrastructure, electronic communication, and other relevant areas.[422] Experts describe the quality of the legal framework as solid, often emphasizing that Serbia is the most advanced in the region. However, implementation lags behind the threats that are evolving in cyberspace.

Although the normative framework regulates the area of ICT security, which is geared towards the protection of critical infrastructure, digital networks, and ICT systems, the phrase most commonly used in everyday speech is cybersecurity, implying not only ICT security, but also threats that are not formally part of ICT security.[423] Cybersecurity also includes the area of cybercrime, regulated by a separate legal and strategic framework. Lawmakers opted for the term 'ICT security' due to the need to align with the international standards in the field: the ISO 27000 standards.[424]

With the development of new technology, new forms of challenges, risks, and threats are emerging that are not covered by the current criminal legislation

The area of high-tech crime in Serbia is regulated by the Law on the Organisation and Competence of State Authorities in the Fight against High-Tech Crime and the transposition of the Council of Europe Convention on Cybercrime (the Budapest Convention) into the Criminal Code of the Republic of Serbia, defining the criminal offences that include

421 The Official Gazette of the RS, Nos. 6/16, 94/17, and 77/19, https://bit.ly/3bKjLtV.

422 The legal and strategic framework in the area of ICT security and high-tech crime in Serbia, annexe 1.

423 Bjelajac, Željko and Vesić Slavomir, *Bezbednost informacionih sistema*, *Pravo – teorija i* praksa, 2020, p. 66.

424 The ISO Standards Directory: https://www.27000.org/.

elements of high-tech crime.[425] Targeted changes were also made to the Criminal Procedure Code to introduce new terms related to cybercrime and a list of evidentiary actions to be applied in criminal proceedings for these offences.[426] With the development of new technology, new forms of challenges, risks, and threats are emerging that are not covered by the current criminal legislation. There is therefore a need to modify how the Criminal Code defines criminal offences in the area of high-tech crime, especially offences that do not directly stem from high-tech crime but can be perpetrated with the use of a computer or information systems – and that cannot be prosecuted ex officio but remain within the private lawsuit system.[427] For example, the criminal act of collecting personal data without authorization (art. 146) is charged through a private lawsuit; the citizen is therefore responsible for collecting evidence of the criminal offence and requesting data from private companies as an individual, which further complicates the process. To a certain extent, the legislator has inadvertently established inequity regarding age, since juvenile persons enjoy a higher degree of protection and in case of their rights being violated, national authorities are more likely to intervene ex officio, whereas adults must resort to a private lawsuit.[428] Experts propose a special legal definition of criminal offences to be prosecuted ex officio, for example in case of massive violations of the law.[429] Organizations dealing with human rights, especially those working with minority groups, suggest the need to introduce new criminal offences, such as the non-consensual sharing of intimate images targeting women.[430]

Strategic regulation of high-tech crime (Strategy for Combating High-Tech Crime for the period 2019-2023) entered into the legislative framework almost 10 years late (2018), reflecting a need for Serbia to become better aligned with the EU and to establish an efficient and sustainable system that consolidates the work of all institutions responsible for countering high-tech crime. Although the action plan for implementing the 2019-2020 strategy has now expired, the Ministry of Interior (MoI) has not yet drafted a new one. There is no information about the strategy's implementation available to the professional community working in this field, nor any means of effectively assessing its progress given the lack of a publicly available report from the MoI.

With regard to the strategic framework for ICT security, two strategies were in force until the end of 2020: the Strategy for ICT Security (2017-2020) and the Information Society Development Strategy in the Republic of Serbia (2010-2020). Since both strategies have expired, a new one was endorsed, titled the Information Society and Information Security Development Strategy of the Republic of Serbia Strategy for the period 2021-2026, which is aligned to the EU Network and Information Security Directive (NIS

---

425 Cybercrime acts include damaging computer data and programmes (art. 298); sabotaging a computer (art. 299); creating and introducing computer viruses (art. 300); committing computer fraud (art. 301); accessing a computer, computer network, or electronic data processing system without authorization (art. 302); preventing or restricting access to a public computer network (art. 303); using a computer or computer network without authorization (art. 304); and creating, obtaining, or providing another person with a means of committing criminal offences that result in a breach of computer data security (art. 304a). The second group of crimes is more diverse and includes crimes against intellectual property (arts. 198, 199, and 202), as well as individual crimes such as endangering security, most often through social networks (art. 138); publishing or presenting another person's texts, pictures, or recordings without authorization (art. 145); collecting personal data without authorization (art. 146); showing, procuring, or possessing pornographic material and pornography involving a minor (art. 185); abusing computer networks or other technical means of communication to commit criminal offences against the sexual freedom of a minor (art. 185b); offences involving forgery or the abuse of payment cards (art. 243); and any other criminal offence that involves the use of computers or computer networks.

426 Some of these terms include 'electronic record', 'electronic address', 'electronic document', and 'electronic signature'. In the case of cybercrime, special evidentiary actions may be applied to the following criminal offences: showing, procuring, or possessing pornographic material and pornography involving a minor; using copyrighted work or work protected by similar rights; damaging computer data or programmes; sabotaging a computer; committing computer fraud; and accessing a computer, computer network, or electronic data processing system without authorization.

427 Interview with Đorđe Krivokapić, 28 January 2022.

428 Interview with Lidija Komlen Nikolić, 7 February 2022.

429 Interview with Đorđe Krivokapić, 28 January 2022.

430 Interview with Vanja Macanović, 17 February 2022.

Directive). In the meantime, the Serbian government has endorsed the Strategy for the Development of Artificial Intelligence for the period 2020-2025 (73/2019), which reflects the state's tendency to incorporate advanced technologies into its work. By merging these two strategies, greater focus is placed on developing digital society, rather than ICT security. The Serbian government's strategic priority is to develop digital society[431] to enhance the effectiveness and efficiency of the work of public administration and local self-government and thus respond to the needs of citizens and the business sector. While digitalization offers certain advantages, it also entails a high risk for security and human rights, due to the high amount of personal data involved, especially sensitive data relating to citizens in the digital world. Representatives of civil society and the Cybersecurity Network Foundation underscore the problem that the processes of digitalization and the development of ICT security, although being carried out in parallel, are not being integrated, i.e. (cyber)security and human rights protection are not recognized as important joint components of the digitalization process.[432] On the other hand, from the perspective of the Ministry of Trade, Tourism and Telecommunications (MTTT), information security, digitalization, and e-commerce are processes that are linked.[433] The theory of change approach at the ministry is to share the responsibility of data protection with citizens, by enhancing their digital skills to enable them to protect themselves and fully exercise their rights.[434]

Cybersecurity is often understood in terms of national security and is embedded in policies related to national security and military doctrines. The main architects of the ICT security system did not, however, apply a national security approach when defining the policies and laws six years ago, which impacted the system's structure. Nevertheless, the second National Security Strategy of the Republic of Serbia (94/2019-13) recognizes that the development of modern technologies and their omnipresence in society increases the risk of high-tech crime and threats to ICT systems.[435] In the present security environment, particularly since the outbreak of war in Ukraine, cyber warfare and the protection of critical infrastructure is viewed as an integral part of national security at the international and European level. In the future, this could lead to changes in strategic thinking and/or institutional arrangements.

Information security actors

The main state institutions in the ICT security area are the MTTT, the Regulatory Agency for Electronic Communication and Postal Services (RATEL) and its computer emergency response team (CERT), as well as the Serbian government's Coordination Body for Information Security Affairs.

The MTTT proposes laws and strategies in this area and is the main institution responsible for implementing activities related to ICT security in Serbia. The ministry submits reports on its work to the National Assembly, which holds committee meetings and public hearings on information security. Members of parliament express their interest in projects implemented by the MTTT, such as online schooling and the installation of optical cables in rural areas.[436] Most members of parliament, however, lack specific knowledge about information security and are therefore unable to oversee government bodies effectively.

---

431 See RTV, *Digitalization is the Serbian Government's Priority* (Digitalizacija je prioritet Vlade Srbije), 5 September 2015.

432 Interviews with Novak Pešić, Vladimir Radunović, Irina Rizmal, and Bojan Perkov, February and March 2022.

433 Interview with state secretary Milan Dobrijević, 5 April 2022.

434 Ibid.

435 National Security Strategy of the Republic of Serbia, 2019. *https://www.mod.gov.rs/eng/4350/strategije-4350*

436 Interview with state secretary Milan Dobrijević, 5 April 2022.

RATEL[437] is an independent state agency within which the National Centre for the Prevention of Security Risks in ICT Systems of the Republic of Serbia (nCERT) also operates.[438] According to the Law on Information Security (art. 15), the nCERT is responsible for collecting and exchanging information about risks for ICT systems, as well informing, supporting, warning, and advising those in charge of ICT systems, as well as the wider public. A strategic decision was taken during the development of the law to place the nCERT within RATEL. This was done because the Regulatory Agency had sufficient resources to fulfil its legal obligations and because it is competent to handle electronic communication systems, from which the major risks for ICT security originate.[439]

Besides the nCERT, other authorities have their respective CERTs, such as the MoI, the Security Intelligence Agency (BIA), and the Serbian Army. The Centre for Security of the ICT System in Government Bodies (CERT of Government Bodies) was established only recently within the Office for Information Technologies and eGovernment, in accordance with the Law on Information Security.[440] The CERT of Government Bodies performs tasks related to the protection of ICT systems of government agencies – excluding those of independent operators – through eGovernment information and communication networks. Besides the national centres, 14 special CERTs have been established by companies and citizen associations.[441] The SHARE Foundation is the only civil society actor with its own CERT.[442] The SHARE-CERT was created to monitor violations of digital rights and freedoms in Serbia; it is mainly used by journalists, activists, and civil society organizations seeking legal and technical support.[443] The most active non-state actor is the Serbian Association of Banks, which has its own CERT, established with the idea of becoming a financial CERT.

Coordination among different government bodies and cooperation between the public and private sector is key to tackling cyber attacks and cybercrime more effectively. Inter-sectoral cooperation was formalized through the Coordination Body for Information Security Affairs.[444] This body is run by the MTTT and composed of members representing the state institutions responsible for ICT security, the academic community, civil society organizations, and the private sector. To improve certain aspects of ICT security, expert working groups are set up within the coordination body. According to the RATEL interlocutors and experts from the Cybersecurity Network, the body convenes regularly (twice a year),[445] but the recommendations of the meetings are not available to the public. Experts consider that the impact of the coordination body on decision-makers is limited, due to its advisory role and the need for political will at the government level to confer greater powers on this body.[446] In the absence of a fully functional government CERT, the existing coordination mechanism is not sufficient to respond to emerging threats and provide rapid, targeted solutions. According to the MTTT state secretary, the exchange of knowledge, information, and lessons learned about cyber incidents should take place through CERTs and not the coordination body.[447]

---

437 See the official web page of the RATEL: *https://www.ratel.rs/cyr/page/cyr-informaciona-bezbednost*

438 See the official web page of the National CERT: *https://www.cert.rs/rs*

439 Interview with Đorđe Krivokapić, 28 January 2022.

440 The Office for Information Technologies and eGovernment, Digitalizing Serbia, *CERT: Digitalizing public administration*.

441 The official records of all registered CERTs in Serbia are available at: *https://www.cert.rs/rs/evidencija-certova.html*

442 SHARE-CERT: *https://www.sharecert.rs/*

443 Interview Bojan Perkov, 25 January 2022.

444 The decision to set up the Coordination Body for Information Security Affairs is available at: *https://www.ratel.rs/uploads/documents/empire_plugin/5edde0a356c12.pdf.*

445 Interview with Novak Pešić, Adel Abusara, Irina Rizmal, and Jovan Milosavljević.

446 Interview with Novak Pešić, Adel Abusara, and Irina Rizmal.

447 Interview with state secretary Milan Dobrijević, 5 April 2022.

The key actors in the area of high-tech crime are the MoI and the Special Prosecutor's High-Tech Crime Department established within the Higher Public Prosecutor's Office in Belgrade, which has jurisdiction over the entire territory of Serbia.[448] The Law on the Organization and Competences of State Authorities in Combating High-Tech Crime[449] defines the roles and responsibilities of all authorities involved in countering high-tech crime. The Special Prosecutor's Office for High-Tech Crime, besides the head, has engaged four more deputy High Public Prosecutors specialized in this area, as well as four prosecutorial advisors with ancillary staff. This number of staff is insufficient, given that the Special Prosecutor's Office had 4,769 registered cases in 2020 – a 25 per cent increase compared with 2019.[450] Until 2009, the special department of the Higher Court in Belgrade was competent to try disputes in the field of high-tech crime, while the Appellate Court in Belgrade decided in the second instance; however, as the special department ceased to exist in 2009, the judges of this court now adjudicate in high-tech crime cases.

The cybersecurity network

Significant supporters in the area of cybersecurity include the international community – primarily the Organization for Security and Co-operation in Europe (OSCE) Mission to Serbia and the Geneva Centre for Security Sector Governance (DCAF) – and civil society, which was responsible for encouraging cooperation between state authorities, citizen associations, the academic community, and business operators, in 2014 and 2015. In mid-2015, the OSCE Mission to Serbia, DCAF, and the Diplo Foundation established a strategic partnership with the Petnica Research Station and created the so-called Petnica Group, which encompasses the key public and private stakeholders in cybersecurity. The informal cooperation facilitated through the Petnica Group has contributed to the development of strategic documents; the exchange of information, know-how, and experience; and greater networking between key stakeholders in the area of ICT security. According to several members of the group, the level of cooperation that exists between state and non-state actors relies on mutual trust, which is, at the same, time, the greatest asset of this public-private partnership. The cooperation between Petnica Group members was formalized in 2020, in the form of the Cybersecurity Network Foundation, which includes over 40 associations and entities.[451] The Cybersecurity Network facilitates the exchange of information, knowledge, and practices; acts as a support group in the event of cybersecurity incidents; and serves as a group of potential partners for cybersecurity projects and programmes. The network is recognized by the Information Society and ICT Security Development Strategy, and its representatives manage the working group of the Coordination Body for ICT Security Affairs, which has institutionalized its links with the state.[452] The task of the working group is to provide support to the state in implementing the strategy and to monitor cybersecurity projects at the national and regional level.[453] In the upcoming period, the network will focus on training and empowering young talents in Serbia in the area of cybersecurity, through the Cyber Hero programme.[454] This programme is implemented with the support of relevant state institutions, higher education institutions, associations, and businesses.

---

448 The official web page of the Special Prosecutor's Office for High-Tech Crime: *http://www.beograd.vtk.jt.rs/*

449 The Official Gazette of the RS, No. 104/2009.

450 *http://www.rjt.gov.rs/docs/rad_javnih_tuzilastava_2020_0421.pdf*

451 The official website of the Cybersecurity Network: *https://sajberbezbednost.rs/*

452 Interview with Adel Abusara, 11 February 2022.

453 Interview with Irina Rizmal, 25 February 2022.

454 Cyber Hero: *https://cyberhero.rs/about*

Challenges, constraints, and shortcomings

RATEL, and more precisely nCERT, has published a comprehensive yearly report on significant ICT system incidents that occurred in 2020. The report states that around 26 million incidents were recorded, the most common being attempts to hack the ICT system (17,332,830) and unauthorized data collection (8,470,838). In line with Article 11 of the Law on Information Security, all ICT system operators of particular importance (9,000 in total) are obliged to report incidents to the nCERT or other relevant authorities. The number of notifications on ICT system operators shared with the nCERT is low, not only because operators are unaware of their obligation to inform the nCERT of cyber incidents, but also because they are reluctant to impart such information due to reputational damage, omissions in their work or in case they initiate an inspection and have sanctions imposed. While the Law on Information Security envisages low fines for operators' failure to inform the competent authorities of incidents (425 to 4,250 euros), it is difficult for the MTTT to monitor its implementation owing to a shortage in staff – one inspector to several thousands of ICT operators. According to the MTTT state secretary, it is difficult to get permission from the government to hire new people. However, policymakers have never opted for a robust oversight body, but instead to enforce information security standards through compliance with the organic law and to ensure that incidents are reported to the Ministry and RATEL. Monitoring the ICT operators' work will be very difficult in the future because the MTTT foresees an increase in the number of ICT operators. This challenge could be mitigated by introducing specific criteria on the basis of which ICT operators would be considered essential.

Furthermore, lack of personnel with specific cybersecurity knowledge and experience in cybersecurity, particularly IT experts and chief information officers, hinders government efforts to protect ICT systems more effectively.[455] Out of all government bodies, the Ministry of Interior has the strongest capacities in the area, with 22 police officers working in the Department of Combating Cybercrime.[456]

Since digitalization is at the top of the political agenda, the government strategically allocates more funds for developing digital services development and investing in people who build and maintain these services. The Office for IT and eGovernment has thus recruited 200 people for the development of digital services using funds from the World Bank, but no cybersecurity experts.[457] Besides the existing lack of qualified experts on cybersecurity within the public administration and local self-government, the situation is compounded by the difficulty of attracting and retaining IT experts within state institutions – all the more because the IT labour market offers better remuneration and career development opportunities.

The abolition of the specialized court department has caused numerous problems in practice. The biggest obstacle in judicial proceedings is that judges who do not understand the technology or specifics of electronic evidence sufficiently are now adjudicating in cases involving cybercrime. For example, some judges do not know what an International Mobile Equipment Identity (IMEI) number is – a unique code that makes it possible to identify each individual mobile telephone. There are therefore situations where entire proceedings are rejected due to the insufficient digital literacy of judges and inadequate training for trying cybercrime cases. Consequently, efforts to recruit more staff and create special departments and CERTs should also be accompanied by more cybersecurity training. This is also relevant for police

455 According to the its response to a request for access to information of public importance on 6 April 2022, the Ministry of Foreign Affairs has one person responsible for ICT security but does not have its own CERT – despite being obliged to have one under the Law on Information Society. The Government Office for IT and eGovernment only recently appointed a new person tasked with ICT security. Following the retirement of the head of the MoI's CERT, this ministry recently appointed a new manager.

456 The Department of Combating Cybercrime is divided into four sections. The MoI can replenish its human resources by recruiting undergraduate students from the information and computing programme of the Criminalistics Police University.

457 Interview with Novak Pešić, 2 March 2022.

officers who need a better understanding of cybersecurity and knowledge of cybercrime regulations and procedures in order to obtain electronic evidence and ensure evidence admissibility in the court. In the previous practice of the courts and prosecutor's office, one of the major problems is inadmissible evidence as a result of ignorance of the procedures during the collection and handling of electronic evidence.[458]

One particular challenge is that many high-tech crime cases exceed the statute of limitation even before they reach court due to the untimely response of the injured parties, as well as the authorities during the evidence-collection phase.[459] The cybercrime penal policy is also lenient, and the criminal offence of having accessed a protected computer without unauthorized, for example, is liable to lead to a prison sentence of up to one year.

One of the missing links is stronger parliamentary oversight of cybersecurity actors and laws in Serbia. In the period 2019-2022, members of the National Assembly organized nine public hearings on cybersecurity, digitalization, the Data Centre in Kragujevac, artificial intelligence, and other topics.[460] Public discussions have, however, mostly focused on state or corporate cybersecurity instead of human security, while parliamentarians often used public hearings to praise the government rather than scrutinize it. It is worth noting that almost all public discussions on cybersecurity have been supported by foreign embassies and international development organizations, highlighting the lack of interest among lawmakers to address a topic that is in the public interest.

Finally, the initial architecture of the ICT security system is too complex and not adapted to the current environment, which is characterized by an increasing number of cybercrimes and incidents. Owing to its position within RATEL, the national CERT has a limited role, according to experts, and little potential to influence other state authorities and legal entities within the ICT system. It is problematic that not all ministries are aware of the existence or work of the CERT of Government Bodies, which is overshadowed by the RATEL nCERT. Experts are currently more in favour of creating a state CERT and a coordination body within the Serbian government – akin to the Coordination Body for Gender Equality – to strengthen the remit and improve communication between various government and non-government stakeholders.

CYBERSECURITY AND HUMAN RIGHTS FRAMEWORKS

Although the research conducted by civil society organizations indicates various forms of threats to the rights and freedoms of marginalized groups in Serbia involving the use of modern technologies, the strategic and legal framework in the area of ICT security does not recognize the impact of these technologies on various social groups, other than children and youth. Civil society organizations dealing with human rights and violence against women believe that this is a consequence of an insufficiently inclusive process in developing political documents and legal regulations – since the so-called women's organizations; lesbian, gay, bisexual, transgender, intersex, and queer (LGBTIQA+) groups; associations of Roma men and women in Serbia; and so forth were not consulted or included in the process.[461]

Organizations and institutions, such as the SHARE Foundation, the Association of Public Prosecutors, and the Data Protection Commissioner, consider that the human rights standards have been embedded

458 Interview with Lidija Komlen Nikolić, 7 February 2022.

459 Ibid.

460 Public hearings on cybersecurity in parliament: http://www.parlament.rs/prenosi/arhiva.3703.html

461 Interview with Vanjom Macanović, The Autonomous Women's Center, 17 February 2022.

in the legislation (for example, the right to privacy and the protection of personal data).[462] Serbia's accession to the EU presupposes its alignment to the EU's acquis and integration with the single concept of combating high-tech crime. Additional standards for human rights protection were therefore included in the national legislation to align with not only the EU directives but also those of the Council of Europe, as well as accompanying protocols. In May 2022, Serbia was among the first countries to sign the Second Additional Protocol to the Council of Europe Cybercrime Convention on enhanced cooperation and the disclosure of electronic evidence. The ratification of this protocol will require further alignment with various provisions of the regulations. The protocol is significant because it strengthens states' cooperation with the private sector to protect the rights of all internet users and to collect electronic evidence more efficiently, in accordance with technological developments and new forms of cybercrime.

Experience to date has shown that in parallel to accepting international standards, human rights in Serbia can still be limited or derogated by the development and approval of new legislation, as in the case of the attempted legalization of biometric surveillance through the adoption of the new Law on Internal Affairs.[463] One of the main challenges in the human rights sphere is the fact that the Serbian authorities are using European integration as a pretext for frequent amendments to the legal framework; as a result, the generation of new regulations often means a step backwards for the civic rights and liberties that have already been achieved. There are also emerging global challenges, such as the war on terrorism and the ongoing war in Ukraine, which could facilitate the expansion of the power and authority of state security actors in cyberspace at the expense of human rights.

Cybersecurity and the right to privacy

The right to privacy is regulated by the systemic Law on Personal Data Protection from 2018, aligned with the EU's General Data Protection Regulation (GDPR). The adoption of the law was one of the prerequisites in Serbia's negotiations with the EU, under the Chapter 23 Action Plan, which refers to the judiciary and human rights. The first law on the protection of personal data was adopted in 2008 but replaced by an entirely new law in 2018. Although it complies with some EU standards, the new law is no better than the previous one. Cybersecurity and legal experts also flag the short time frame given for harmonization (9 months) of various state authorities and entities with the GDPR, which makes its implementation difficult, thus further jeopardizing adequate personal data protection.[464]

The key independent state authority responsible for the protection of privacy and personal data is the Commissioner for Information of Public Importance and Personal Data Protection. The commissioner is responsible for initiating oversight procedures regarding the work of state institutions and private companies involved with data processing, whether as data handlers or processors. The national authorities are obliged to notify the commissioner if an incident occurs. Following the adoption of the Law on Personal Data Protection, the commissioner is entitled to initiate misdemeanours proceedings against the state authority and other private entities processing personal data, and the Misdemeanour Court is competent to rule on these cases. According to the GDPR (art. 83), the fines for violating the right to privacy in the EU can be up to 20 million euros, or 4 per cent of the company's annual turnover, which has not been the case in Serbia so far. The fines envisaged for the violation of legal provisions are from 5,000 to one million dinars (EUR 43 to EUR 8,523) if the offence is established by the court judgment. Due to

462 Interview with Đorđe Krivokapić, Lidija Komlen Nikolić, Zoran Pašalić, and Marko Milošević from the Data Protection Commissioner's Office.

463 Belgrade Centre for Security Policy (BCSP), *BCSP Communication: The Draft Law on the Interior makes way for police abuse*, 17 September 2021.

464 Interview with Bojan Perkov, 25 January 2022.

the low fines for misdemeanours and the inertia of the judiciary, the sanctions available to independent state authorities are 'a sort of reprimand, not a serious penalty for those who violate human rights and citizens' security'.[465] Nevertheless, experts consider that consistent, that is to say regular, sanctions for the violations of the right to privacy could bring about a change in conduct of both state and non-state actors.[466]

The commissioner issued an opinion of the Law on Information Security during the drafting phase, as well as when amendments were made to the law. The commissioner also issued an opinion on the by-laws pertinent to information security. Given the commissioner's competences, his comments referred to the importance of data protection measures and designation of persons responsible for personal data protection. The Strategy for Personal Data Protection is being developed and, although the commissioner is not a member of the working group, he will issue an opinion on the draft. The current draft strategy and its action plan envisage training for the public administration employees on how to handle personal data; however, the policymakers omitted to include the commissioner, with the training delegated to the Ministry of Justice.[467]

Violation of the right to privacy on the internet

The right to privacy becomes an issue in society when it is violated, for instance when there is a massive 'leakage' of personal data into the public domain. In the past seven years, there have been serious cases involving violations of the right to privacy, the leakage of data from state and private institutions, as well as the misuse of personal data. Within a period of only six years (2014-2020), the SHARE Foundation and the Balkan Investigative Reporting Network documented and classified 668 cases of infringement of digital rights and freedoms in Serbia.[468] According to Zlatko Petrović, assistant secretary in the commissioner's office, 'Serbia is a country with a long history of compromising personal data'.[469] Experts add that the reason for this is a culture with very low levels of security and cyber hygiene among citizens, which is why 'citizens' personal data is available for people to pick and choose'.[470]

Besides citizens' poor knowledge in how to protect their personal data and digital rights, violations of the right to privacy most often occur due to neglect and serious omissions in the work of state authorities and private companies.

The first wave of the COVID-19 pandemic in Serbia in 2020 coincided with the first case of an attack on critical infrastructure, with several incidents occurring in a row, causing massive leakage of data on the health status of patients in Serbia's public and private health systems.

The attack took place on 1 March 2020, when the server of the public utility company Informatika, in Novi Sad, was incapacitated after being hacked by ransomware.[471] It affected about 2,000 computers and compromised the data of Informatika employees, but not that of citizens processed by the company for billing purposes. Furthermore, this attack also affected the work of other local services, as their computers

---

465 Interview with Zoran Pašalić, 28 February 2022.

466 Interview with Vanja Macanović, 17 February 2022.

467 Interview with Zoran Pašalić, 28 February 2022.

468 Perkov, Bojan et al., *Greška 404: Digitalna prava u Srbiji 2014-2019*, SHARE Foundation, 2019.

469 Dragana, Prica, *In a land with a long history of compromising personal data, pandemic is a serious challenge* (*U zemlji sa dugom istorijom kompromitacije podataka o ličnosti, epidemija predstavlja ozbiljan izazov*), 02!, 27 January 2021.

470 Interview with Novak Pešić, 2 March 2022.

471 SHARE Foundation, *How Novi Sad was hijacked and locked down* (*Kako je Novi Sad otet i zaključan*), 11 June 2021.

ceased to function, while the payment of bills became problematic for the citizens of Novi Sad. To unlock the data, the hackers requested a ransom of 50 bitcoins, or around USD 50,000 dollars, based on their value at the time.

Since the city of Novi Sad refused to pay the ransom, external IT companies and experts worked to remove the virus and unlock the data, as well as to restore the system.[472] At the same time, competent state authorities were involved in investigating the facts related to the attack – the High-Tech Crime Department of the Serbian MoI, the Security and Intelligence Agency, and the Special Prosecutor's Office for High-Tech Crime. Following the report of the incident, authorized persons from the commissioner's office conducted an ad hoc inspection of the implementation of the Law on Personal Data Protection at Informatika. As a result, the company immediately embarked on the construction of a new hardware and software infrastructure for the information system. However, experts maintained that there was no information exchange or details on lessons learned among the various stakeholders belonging to the Body for Coordination of Information Security Affairs or the Cybersecurity Network, in order to prevent similar incidents from happening to other ICT system operators and to improve the overall infrastructure.[473]

At the start of the pandemic, the COVID-19 information system[474] was also compromised when usernames and passwords to access the system became available to the public online. The SHARE Foundation reported the incident to the Commissioner for Information of Public Importance and Personal Data Protection, nCERT, and MTTT. The commissioner found that the system had failed to conform to the Law on Personal Data Protection and to provide adequate technical, organizational, and human resources measures to protect personal data.[475] State institutions responsible for managing the system (Public Health Institute), processing (National Health Insurance Fund) and handling data (health centres) denied that patients' data was compromised and misused. Nevertheless, the commissionaire issued a reprimand to state institutions and filed a criminal complaint to High Public Prosecutor's Office in Belgarade against an anonymous employee of the health care centre in Majdanpek for disclosing the medical data of 24 people on social networks.

At the beginning of 2021, the medical records of Medigroup patients were leaked to the media and revealed that many former and incumbent officials, as well as celebrities, were being treated within a private health care system. When the commissioner began an investigation into the implementation of the Law on Personal Data Protection, Medigroup obstructed the process by preventing access to both documentation and their database.[476] Medigroup's management has since pressed charges against two of their former employees, and court proceedings are in progress.[477]

In June 2022, two telecommunication companies, Telekom Srbija and Tesla in Zagreb, responsible for an electronic school diary system were found to have failed to adopt rules and procedures related to data security in accordance with the law.[478] As a result, these two companies have personal data on all students in Serbia, including their health records. Despite a data confidentiality clause in their contracts,

---

472 Ibid.

473 Interview with Novak Pešić, 2 March 2022.

474 The Government's Conclusion on establishing a Consolidated and Centralised Software Solution – the COVID-19 Information System (IS COVID-19): 50/2020-9, 57/2020-17, *https://bit.ly/37ljgnX. The system contains medical records of Serbian citizens and information on their treatment, isolation measures, location data, and data on cured and deceased persons.*

475 *Annual Report of the Commissioner for Information of Public Importance and Personal Data Protection for 2020*, pp. 44-46.

476 Kašanski, Borislav, *Medigroup wants to hide data from commissioner: renowned health system obstructing investigation on data leaking!* (*Medigrupa Bi Da Sakrije Podatke Od Poverenika: Poznati zdravstveni sistem opstruira istragu o curenju podataka!*), Republika, 15 January 2021.

477 Politika, *Leaked data of patients from Joana medigroup* (*Iscurili podaci pacijenata iz Joana medigrupe*), 6 January 2021.

478 State Audit Report, 20 December 2021. *https://novaekonomija.rs/assets/Katarina/esDnevnik.DRI.pdf*

the Ministry of Education, Science and Technological Development has not established mechanism to control whether private companies comply with data confidentiality obligations. Moreover, the Ministry has not adopted rules and procedures related to information security, i.e. security act, in accordance with the Law on Information of Security. To make matters worse, the second company won a public tender for the service based on connections with former trade minister Mladen Šarčević.[479]

Besides the cases highlighted above, it is possible to identify a pattern of confidential personal data being leaked from state authorities to the media in order to discredit and/or intimidate political dissenters, and to try to influence the decisions of independent state authorities. One very well-known case in this context involved the leaking of data from health records belonging to Marija Lukić, a former employee of the Brus municipality, who had been litigating for several years against the former mayor of Brus, Milutin Jelačić Jutka, who is also a prominent member of the Serbian Progressive Party.[480]

In several other cases, the state intelligence service (BIA) was found to be responsible for leaking documents from government electronic records through the pro-government media. In 2022, the High Court in Belgrade fined the newspaper Blic for publishing a photo of Serbian citizen Jovan Vukotić from the MoI's electronic records and labelling him as one of the leaders of the Škaljari criminal clan, and proved that the Security Information Agency (BIA) sent the photo to the newspaper. Recently, the leader of the criminal clan Jovan Vukotić from Montenegro was liquidated, while the Serbian citizen of the same name lived in existential danger for years. In 2020, Pink Television published a photo from the MoI's electronic records of the deputy prosecutor for organized crime, Saša Ivanić, who is conducting procedures against drug trafficker Darko Šarić and his group, and the criminal group led by Veljko Belivuk.[481] In both cases, the defence counsels tried to influence the Organized Crime Prosecutor's Office so that Ivanić and other deputies would be exempt from the Šarić and Belivuk trials. Previously, the Data Protection Commissionaire established that in 2014, a BIA officer took the prosecutor's photo from MoI's electronic records, which is why the commissioner filed a criminal complaint against an unknown perpetrator, but no investigation followed. This news disturbed the public because the liquidation of criminals, politicians, police informants, lawyers and police officers is a reality in Serbia.[482]

In recent years, Serbia has seen an increase in digital surveillance performed by state actors. According to media and investigative reports, state security institutions have procured many digital surveillance tools, including the most intrusive equipment capable of secretly penetrating and controlling users' devices and analysing huge amounts of data in detail. This became evident when the Serbian president told the press that Serbian security institutions were monitoring the movement of Serbian citizens returning from hotspots, such as Italy, at the beginning of the pandemic.[483] After the Pegasus scandal became widely known in July 2021, the Citizen Lab reported that Serbian authorities used various spyware programmes.[484] Furthermore, even state-owned enterprises and government bodies that are not mandated to provide security, such as state-owned electric utility power company (EPS) and the MTTT, have bought digital

---

479 Vasić, Jelena and Milica Vojinović, *Elektronski dnevnici: Tender po merama firme Šarčevićevog saradnika*, KRIK, 20 August 2018.

480 Blic, *Dreadful Pressure on Jutka's Victim: Marija Lukić's health records with all personal data published on the Internet* (*STRAŠAN PRITISAK NA JUTKINU ŽRTVU: Zdravstveni karton Marije Lukić sa svim ličnim podacima objavljen na internetu*), 28 February 2019.

481 N1, *NIN about Saric's trial: prosecutor's photo from MoI records in media* (*NIN o suđenju Šariću: Fotografija tužioca iz evidencije MUP-a u medijima*), 10 June 2020.

482 Video clip about Oliver Ivanović, *https://www.youtube.com/watch?v=s60Uw909CZI*

483 Vuksanovic, Vuk, *Fear drives the state's response to COVID-19 in Southeast Europe not the import of a Chinese model*, LSE Blog, 24 April 2020.

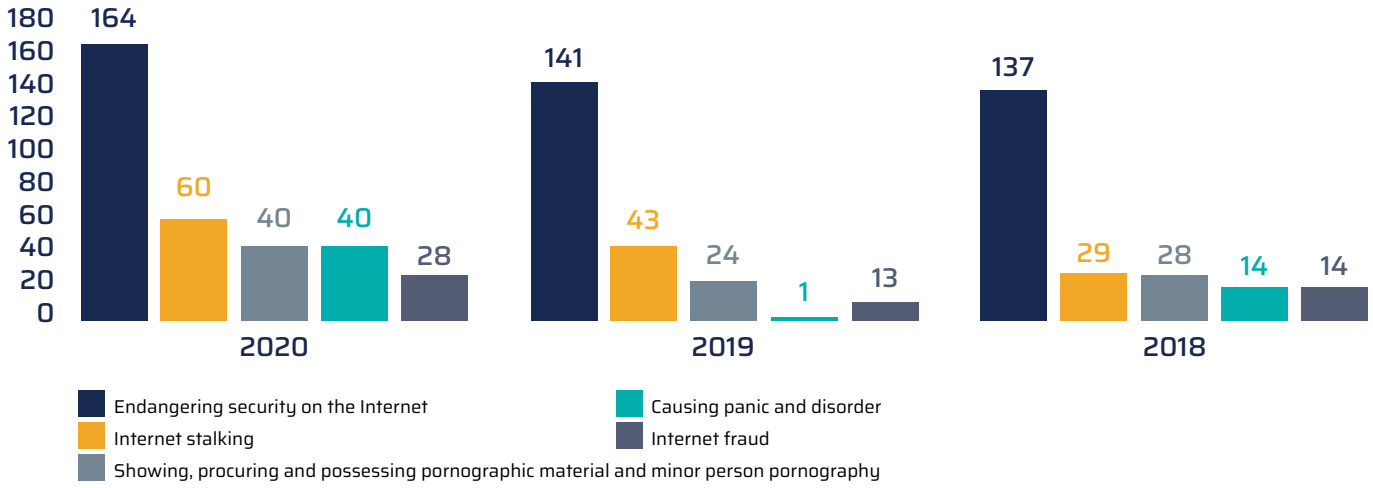
484 Marczak, Bill et al., *Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, The Citizens Lab, 16 December 2021.

surveillance equipment and software.[485] In 2022, the MTTT has so far renewed licences for the following software for market inspection purposes: Maltego, Mozenda and Social Links.[486] The ministry has previously shown interest in purchasing software from the Israeli firm Cognyte. The company reported on Facebook (now Meta) that the targets of the software were mainly journalists, critics, and opponents of the government.[487] The proliferation of digital surveillance in Serbia is very opaque and only individual cases are reported, making it hard to gain a broader picture of the growing digital surveillance system and challenging for citizens to understand the dangers of such infrastructure.

Cybersecurity and freedom of speech and information

In the absence of strong political opposition to the current ruling political elite and the lack of effective parliamentary oversight, civil society and the media are the last barrier against an omnipotent government. Due to their reporting on political corruption, state capture, organized crime, and other issues, journalists, activists, intellectuals, independent media, and civil society representatives are exposed to slander, pressure, arbitrary inspection controls, and other measures aimed at criminalizing them and reducing the space for free expression. Civil society and the independent media have so far managed to resist the regime's attacks, continuing to present critical views that are increasingly making an impact on Serbian and international public opinion.

Chart 1. The five most common types of cybercrime in Serbia



Source: Republic Public Prosecutor's Office

Over the last three years, the crime of 'endangering security on the internet' has increased in the country. According to the SHARE Foundation monitoring report, the most common violations of digital rights and freedoms in Serbia are pressure (due to expression of opinions and activities on the internet), insults

485 Tešić, Aleksa and Jelena Veljković, *Prislušni centri unutar EPS-a: Nabavili opremu kakvu koriste tajne službe*, BIRN.rs, 29 March 2022.

486 Tešić, Aleksa, *Softveri za obradu ličnih podataka, potencijalna pretnja po privatnost građana*, BIRN.rs, 3 June 2022.

487 Dvilyanski, Mike et al., *Threat Report on the Surveillance-for-Hire Industry*, Meta, 2021.

and unfounded accusations, as well as manipulation and propaganda within the digital environment.[488] Citizens and journalists are the most frequently targeted parties, whereas the most common assailants are individuals or unknown persons. Journalists are subjected to abuse almost daily, which increasingly comes from the ruling elite and pro-government media.[489] This is why Serbia was ranked 93rd on the World Press Freedom Index 2021 and is described as 'a country where it is often dangerous to be a journalist and where fake news is becoming more visible and popular'.[490] The number of attacks against journalists and dissenters, and violations of digital rights and freedoms increased between 2014 and 2019, and reached extreme levels during the pandemic.[491] The fact that these attacks have almost become normalized is worrying, and the absence of sanctions for this type of crime only leads to their increase.

There have been numerous cases of online harassment, violence, and smear campaigns against journalists. The largest category of digital rights and freedoms violations is represented by online harassment (threats and calls for violence) aimed at intimidation as a particular form of pressure, to silence journalists and media actors. Almost all high-profile journalists and media actors in Serbia have received online death threats, including the programme director of the Independent Association of Journalists of Vojvodina (NDNV), Dinko Gruhonjić, editor-in-chief of the Autonomija.info portal, Nedim Sejdinović, TV show anchors Zoran Kesić and Ivan Ivanović, deputy editor-in-chief of the weekly magazine Nedeljnik Vreme, Jovana Gligorijević, editor-in-chief of the Beta news agency, Dragan Jovanović, and a journalist from the daily newspaper Danas, Snežana Čongradin, among others. In the words of one journalist, the few independent local media and journalists outside Belgrade are the true heroes and the most vulnerable, as they operate with limited resources and organizational capacity and have an insufficient network among domestic and foreign actors.

Investigative journalists are under constant pressure as authorities seek to discover what they are writing about and who their sources of information are. Because of frequent attacks and surveillance, investigative journalists invest in their personal safety and IT infrastructure by developing security protocols, installing surveillance cameras, employing IT experts, participating in relevant training programmes, and using encrypted communication. According to the former director of the Center for Investigative Journalism in Serbia (CINS), digital security education is ongoing because threats are constantly evolving.[492]

In 2017, in order to address the issue of safety, the government formed a permanent working group focused on journalists' safety, involving the police, the prosecution, and journalists and media associations.[493] Although a large number of attacks on journalists have been reported in the past five years, in many cases 'the authorities were quick to identify those responsible for crimes of violence against journalists, but were much less likely to conduct successful prosecutions'.[494] The conviction of the instigator and two perpetrators of the 2018 arson attack on journalist Milan Jovanović's home was overturned by the appeal court in Belgrade in 2021, requiring a retrial. Since progress in the fight against impunity is slow and limited, journalists feel unprotected and left to fend for themselves. By way of

---

488 SHARE Foundation monitoring lab: *https://monitoring.labs.rs/*

489 See Reporters Without Borders, *Serbia*.

490 Ibid.

491 Perkov, Bojan et al., *Greška 404: Digitalna prava u Srbiji 2014-2019*, SHARE Foundation, 2019.

492 Interview with Branko Čečen, 22 March 2022.

493 Permanent working group for the safety of journalists: *http://www.rjt.gov.rs/sr/bezbednost-novinara*

494 Reporters Without Borders, *Serbia*.

support, the Safe Journalists portal was launched, which aims to provide, in one place, information that is crucial for the work of journalists and editors.[495]

Media portals that defend the public's right to know, including Peščanik and the CINS, as well as NGOs such as the Committee of Human Rights Lawyers (YUCOM) and the Autonomous Women Center, have been the subject of distributed denial-of-service (DDoS) attacks. The DDoS attacks aim to cause websites or pages to crash and to publish inappropriate nationalistic content.[496] In the case of the attack on Peščanik, the Public Prosecutor's Office in Belgrade sent five requests to the MoI to collect information, yet the police did not issue an order to conduct an investigation. In early 2021, another attempt to limit freedom of information on the internet involved copying the identity of local independent portals such as OzonPress.net in 2020 and Južne vesti in early 2021.[497] Based on the lawsuit of the original Južni vesti, the Commercial Court in Belgrade made a decision for the temporary removal of the fake portal that bears the same name and has an almost identical design and logo as Južne vesti. Other well-known cases include the unauthorized access to the Facebook page of the Independent Journalists' Association of Serbia and the accounts of the LGBTIQA+ organization Da se zna on Instagram and Twitter.

Attacks on journalists and the media are fairly well documented and presented in reports by independent state bodies and national and international NGOs. There have also been numerous cases, less in the public eye, in which employees in state and private companies, trade union activists, as well as legal experts in the judiciary have been fired or mobbed at work due to posting on social networks and exposing unlawful or unethical behaviour of members of the ruling coalition.

The government's move to centralize public information about the COVID-19 outbreak in 2020 and the arrest of journalist Ana Lalić for reporting on the poor conditions in the Clinical Center of Vojvodina are the most extreme attempts to stifle freedom of information, especially in the online space. A close associate of the current ruling party, Nebojša Krstić, suggested 'conducting public space pest control' with the immediate barring of social networks such as Twitter, Facebook, and YouTube on the grounds of fighting fake news.[498] This move has not materialized, yet 'censorship through noise' has become widespread as networks of paid commentators and automated accounts multiply pro-government content, spread disinformation to stifle critical voices, and are often used to offend and target political opponents, independent journalists, and anyone who expresses critical opinion. This became most obvious when Twitter cancelled 8,558 false Twitter accounts that served to promote the ruling Serbian Progressive Party and its leader, the Serbian president, Aleksandar Vučić. Furthermore, in 2021, under the pretext of protecting the safety of journalists, the government's amendments to the Code of Civil Procedure (art. 149) sought to reduce the possibility of critical thinking and expression. More specifically, the amendments to the code envisage a new criminal offence: 'The punishment referred to in paragraph 1 shall also be imposed on anyone who without authorization prevents or obstructs the publication of information of public importance through the media, or who significantly endangers the peace of mind of the person who published the information or opinion by gross insult or abuse, insolent or reckless behaviour.'

---

495 Safe Journalist Portal: *https://bezbedninovinari.rs/*

496 SHARE Foundation, *Technical attacks again in the focus of digital rights violations*, 12 April 2018.

497 Canić Milanović, Jelena, *Lažni sajt "Južnih vesti" – još jedan način za obračunavanje sa profesionalnim medijima*, Južne vesti, 19 February 2021.

498 CIVICUS, *Activists, journalists face smear campaign, harassment and censorship during COVID-19*, 7 July 2020.

Cybersecurity and freedom of assembly

In the present-day political context, the right to freedom of assembly is increasingly contested and contentious, and citizens and their associations are deterred from mass protests through intimidation. The introduction of a mass biometric surveillance system in Serbia remains the greatest fear and threat to privacy and data protection,[499] but it also has a deterrent effect on the freedom of assembly, association, and free movement, as well as the freedom of expression.

Fundamental civic rights and freedoms were undermined when the MoI decided to introduce a smart surveillance system and install more than a thousand Huawei cameras with licence plate and face recognition software in Belgrade, but also in other Serbian towns.[500] The installation of cameras coincided with massive protests in Belgrade, denouncing the politically motivated violence against dissenters, under the slogan '1 of the 5 million'. During the 2018-19 anti-government protests, Nebojša Stefanović, then interior minister, presented photos of protesters from surveillance cameras on television, thus revealing their identities. Although the government's primary goal was to persuade the electorate that the protests were not massive, this action also reveals an ulterior motive, which is to intimidate the protesters and deter them from further rallies; people are concerned about going onto the streets now that they know that the cameras are recording them.

Since Serbia does not have a comprehensive organic law on video surveillance and the current legislation makes no provision for its introduction, the MoI decided to legalize biometric surveillance with the development of the Draft Law on Internal Affairs.[501] This draft was developed without a broad public debate or consultations with relevant experts and associations. The general public learned about it just a couple of days before the deadline for public consultations expired, when several civil society organizations raised the alarm. Numerous citizens' associations opposed the introduction of permanent indiscriminate biometric surveillance of citizens, as well as the introduction of 'secret police', referring to a ban on the disclosure of police officers' identities and their recording. In an official letter to the Serbian government, European Digital Rights expressed deep concern over the proposed law and emphasized that its provisions were incompatible with the European Convention on Human Rights, which Serbia ratified in 2004.[502] The draft law was withdrawn as a result, and the Minister of the Interior, Aleksandar Vulin, declared that opponents of the law wanted to see 'blood in the streets of Belgrade' and that 'a few foreign intelligence services, through their web of agents in media outlets, non-governmental organizations, and political parties, had undertaken media preparations for staging violent rallies aimed at Serbia's destabilization'.[503] Two months after the withdrawal of the draft Law, information leaked out that the Serbian and the Russian Ministries of the Interior had created a 'working group for countering coloured revolutions' and that the Serbian police were seeking special training on cybersecurity from the Russian Federation – steps that caused concern among citizens and representatives of civil society.[504] Despite the public's strong reaction, the MoI has not renounced the introduction of biometric surveillance and, in early 2022, it launched a series of consultations with civil society organizations in order to fine-tune the new Law on Internal Affairs. Instead of revising the law, however, civil society organizations

---

499 Bjeloš, Maja. *The Sum of All Fears – Chinese AI Surveillance in Serbia*, in *Western Balkans at the Crossroads*, Prague Security Studies Institute, December 2020.

500 Thousands of Cameras: *https://hiljade.kamera.rs/en/home/*

501 SHARE Foundation, *Total surveillance law proposed in Serbia*, 21 September 2021.

502 EDRi, *Consultation on the proposal for the Zakon o unutrašnjim poslovima*. *https://bit.ly/3ky9fqW*

503 The official statement was published on the MoI website.

504 N1 Beograd, *Serbia and Russia countering "coloured revolutions" together* (*Srbija I Rusija u zajedničkoj borbi protiv „obojenih revolucija*), 3 December 2021.

are demanding that the government declare a moratorium on the use of mass biometric surveillance technologies and systems in Serbia.[505]

Over the last three years, recording and photographing protesters has become an integral part of public gatherings. This is mostly carried out by police officers in uniform, but also by those in civilian clothes, members of the BIA, and unidentified groups of men. Local activists across Serbia claim that the state has stepped up pressure on not only environmental activists and associations (including through intimidation, threats, misdemeanour charges, and summons), but also employees of state-owned companies. For instance, post office workers who were spotted on camera during a protest for drinking water in Zrenjanin in 2018 were later exposed to mobbing at work.[506]

This pressure increased significantly after the first Environmental Uprising was held in Belgrade, in April 2020, and particularly after the radicalization of protests and roadblocks in late 2021. Many citizens who were fined for the crime 'movement and stay in the lane' had not been identified by the traffic police previously, which led to suspicions that the police had used new facial recognition technologies to identify protesters.[507] Following the rallies of 27 November and 4 December 2021, the MoI issued 129 misdemeanour orders in Belgrade and initiated 211 misdemeanour procedures. In other Serbian towns, a total of 1,653 orders were issued and no misdemeanour procedures initiated. A lawyer from the Be One Group association (Grupa Budi jedan) said that people from smaller communities felt bewildered, frightened, and confused, which could impact the number of activists involved in future protests.[508]

On 13 January 2022, the Commissioner for Information of Public Importance and Protection of Personal Data initiated an investigation of the MoI's actions and concluded that the police had not used facial recognition technology during the rallies, but that persons had been identified 'based on the immediate observation of police officers in keeping with the Misdemeanour Law'.[509] Many citizens addressed human rights organizations and attorneys' associations and subsequently pressed charges against the police through the competent courts.[510]

Activists often receive threats through the internet and social media prior to rallies. In early December 2021, an activist from the Fortress Movement, Pokret Tvrđava, received death threats through Twitter, the day before roadblocks occurred in Smederevo. He reported this to the deputy commander of the police station in Smederevo, and then to the high-tech crime inspector. Although he refused to press charges at the time, he emphasized that the Special Prosecutor should prosecute the perpetrator ex officio if they found evidence to support criminal charges.[511] According to the local activist, however, the Special Prosecutor's Office for High-Tech Crime never initiated the procedure.

Police officers often summon citizens to interrogate and apprehend them immediately before rallies to warn them not to attend. According to the N1 Beograd portal, a police patrol in Jagodina came to the office of the Central Media portal on 4 December 2021 and warned the editor, Goran Jevremović, not to participate in the roadblocks; activists and citizens in Niš experienced a similar situation. That same day,

505 SHARE Foundation, *Comments on the Draft Law on Internal Affairs*, 18 September 2021.

506 Interview with Nataša Pušić, 2 February 2022.

507 Vreme, *Štancovanje prijava protiv učesnika protesta: Protivzakonito zastrašivanje*, 21 December 2021.

508 Interview with Nataša Pušić, 2 February 2022.

509 *Commissioner for Public Information of Public Importance and Personal Data Protection, Commissioner conducted surveillance procedure at the MoI, regarding the suspected use of face recognition technology (Poverenik sproveo postupak nadzora u MUP, povodom sumnji na upotrebu tehnologije za prepoznavanje lica), 18* February *2022.*

510 Vreme, *Growing number of complaints about the roadblocks: I'm not paying the fine* (*Sve više prijava zbog blokada: Neću da platim kaznu*), 19 January 2022.

511 Interview with Nikola Krstić, 31 January 2022.

the police warned the president of the environmental association Suvoborska greda, Ljiljana Bralović, not to encourage people to attend the roadblocks.[512]

For members of the LGBTIQA+ community and its supporters, the right to freedom of expression and peaceful assembly is constantly jeopardized due to existing prejudices and discrimination based on sexual orientation or gender identity. Pride parades generally coincide with an increase in human rights violations, along with a sharp rise in off- and online homophobic rhetoric in Serbia.[513] After the September 2020 parade was cancelled because of COVID-19, false rumours circulated claiming that a parade was to be held in Leskovac, southern Serbia, accompanied by calls for violence against the LGBTIQA+ community on social media.[514] As a result, a large group of high school students from Leskovac protested – some violently – against the LGBTIQA+ community.

Cybersecurity and anti-discrimination

The legislative framework for gender equality and anti-discrimination was first developed and approved in 2009, at a time when the area of information security was neither legally nor strategically regulated. The second set of strategic documents and legal regulations, however, took into account the development of modern technologies and their influence on women and girls. Article 38 of the new Gender Equality Law, adopted in 2021,[515] specifies that gender equality in the area of ICT and information society must:

- Promote ICT and the advantages of using modern technologies among women and girls; and
- Ensure a gender balance and equal opportunities for engaging with ICT, as well as mainstream gender in processes related to the financing of these activities.

The law prescribes specific measures for the authorities to take to mitigate the digital gap between women and men, to ensure a balanced representation of women in ICT, and to improve the socio-economic position of women by allowing them to requalify or receive additional training in ICT, as well as by educating girls and young women in science, technology, engineering, and mathematics (STEM).

The legal framework and the newly approved Gender Equality Strategy for the period 2021-2030 recognize the benefits of applying technology for innovation and development purposes. They overlook, however, the violation of digital rights and freedoms of multiple discriminated groups regarding human security and violence against women. The strategic and legislative framework for information security also only identifies children as an important social group, which is perhaps due not only to insufficient knowledge and awareness among lawmakers about the problems faced by multiple marginalized groups in the digital realm, but also to the insufficiently inclusive process of strategy and law development.

For many discriminated groups in Serbia, the challenges posed by online violence and high-tech crime are numerous. The socio-political and economic position of discriminated groups can also affect their level of vulnerability on the internet and the realization of digital rights and freedoms. The political, economic, and social crisis exacerbated by the pandemic has compounded existing inequalities in society and

512 N1 Beograd, *Police warning citizens, activists, even journalists not to go to roadblocks* (*Policija upozorava građane, aktiviste, pa i novinare da ne idu na blokade*), 4 December 2021.

513 Kastelec, Kristina, *Serbia's Violent Homophobic Youngsters Are Victims as Well*, BalkanInsight, 12 March 2020.

514 Perkov, Bojan, Kovačević, Anka, and Bajić, Mila, *Digital Rights Falter Amid Political and Social Unrest Report*, SHARE Foundation, 2021, p. 56.

515 The Official Gazette of the RS, No. 52/2021-7.

deepened the gap between the affluent and the poor; equal access to contemporary technologies in Serbia therefore depends on developing not only the ICT infrastructure but also the economy, as well as ensuring access to the education system. After the Ministry of Education, Science and Technological Development took the decision to switch to online schooling, it became clear that certain social groups, such as the Roma community and children in rural areas, did not have equal access to technology and education. Consequently, a lot of time was spent trying to find ways to allow teachers to connect with

Roma students who lacked the necessary equipment (such as televisions, computers, and laptops), which affected their ability to learn.[516]

During the pandemic, migrants – that is, refugees from the Middle East – were targeted by online hate speech. Social media groups, such as the 'STOP naseljavanju migranata' (STOP migrants settling) with more than 330,000 members, shared manipulative, outdated, or completely false news about migrants to intimidate the public and turn them against migrants. Following the declaration of a state of emergency, migrants were isolated in asylum reception centres and surrounded by the army 'to contain the infection';[517] nevertheless, tabloids and right-wing portals launched a series of anti-immigrant articles and fake news during this period, accusing migrants of 'populating Serbia', spreading coronavirus, and committing crimes, such as rapes, murders, and other offences.[518] Xenophobic and racist content was also produced and shared online by prominent political leaders and parties, including Boško Obradović, leader of the parliamentary party Dveri.[519] The Gender Equality Commissionaire condemned those 'inciting fear and creating a hostile environment towards migrants and people of different colour and ethnic origin', while Serbia's Commissariat for Refugees and Migration called upon the competent authorities to sanction the spread of false news but received no response. Consequently, negative attitudes towards migrants have risen, and they are being subjected to harassment and violence in the physical space more frequently. Right-wing extremist organizations in Serbia, such as the so-called people's patrols, undertook illicit activities to limit the migrants' freedom of movement and to perform para-police duties, such as identity checks in streets across the country. Immediately after the state of emergency in Serbia was lifted, a member of the Levijatan (Leviathan) movement, Filip Radovanović, streamed a video on his Facebook page of himself driving at full speed through barbed wire into the migrants centre in Obrenovac.[520] Moreover, the Centre for Protection of Asylum Seekers and the Trans Balkan Solidarity group recorded an incident in which police used unjustified force against migrants in Krnjača, including beating up a minor and using tear gas in huts lived in by families with children.[521]

Besides migrants, media reports and data from various surveys indicate that girls and women are targeted on the internet much more frequently than boys and men. In 2021, Serbian and regional media reported the existence of several groups on the messaging platform Telegram in which more than 50,000 people – mostly men – from Serbia and other Balkan countries participated and shared not only explicit photos

---

516 Portal Grad Kruševac, *Support to students during online lessons*, 29 October 2021.

517 The Official Gazette of RS, *Decision on the temporary limitation of movement for asylum seekers and Irregular migrants placed in asylum centres and reception centres in the Republic of Serbia*, No. 32, 16 March 2020. https://bit.ly/3pYe1kM

518 Ljubičić, Milica, *"They are attacking and raping"– a new surge of news against migrants* (*"Napadaju i siluju" – novi talas vesti protiv migranata*), Raskrinkavanje, 29 February 2020; Pavkov, Ksenij, *Tabloids accused migrants of murder, police denied, but false news doesn't stop* (*Tabloidi optužili migrante za ubistvo, MUP demantovao, ali lažne vesti ne staju*), N1 Beograd, 13 July 2021.

519 https://www.youtube.com/watch?v=u-LU54cqiEA

520 Rogač, Miljana, *The evolution of Leviathan: from care for dogs to chasing migrants* (*Razvojni put Levijatana: Od brige za pse do potere za migrantima*), Istinomer, 29 May 2020.

521 Milenković, Lazara, *Migrants settling in Serbia and the coronavirus: how the pandemic influences false news and dissemination of anti-migrant views* (*Naseljavanje migranata u Srbiji" i korona virus: Kako epidemija utiče na širenje lažnih vesti i antimigrantskih stavova*), BBC, 7 May 2020.

and recordings, but also the addresses of women from the region.[522] On the basis of a private criminal complaint, the police arrested the administrator of one of the groups from Niš on suspicion of having committed the crime of displaying, obtaining, and possessing pornographic material and exploiting a minor for pornography. However, the case has not yet been heard in court. A law office from Belgrade offered all affected women free legal aid, while 139 organizations from the region signed a declaration to address the institutional silence that actively encourages online sexual harassment.
The most common forms of gender-motivated digital violence were stalking or persecution; harassment; jeopardized safety; eavesdropping; threats; offences; and the publication of undesired photos, videos, or messages with sexual contents[523] These forms of online violence against girls were identified by the Alternative Centre for Girls, thanks to the cooperation of high schools in Kruševac and Rasina district in 2014. The initial findings were confirmed by the June 2020 regional survey of the Alternative Centre for Girls, undertaken in cooperation with SOS centres and safe homes, in which 37.7% of girls who participated in the survey said they had experienced online violence. They most frequently cited having received requests for intimate photos or videos of themselves (14%) or having received undesired and offensive photos or messages with sexual content (13%). About 8% of girls said that someone had shared or posted content relative to them without their consent, such as photos of themselves or their actions, texts, or statements. This violence was perpetrated by men in 69% of cases. The following groups of girls and women were particularly affected: human rights defenders; women involved in politics; journalists; bloggers; women from ethnic minorities; lesbian, bisexual, and transgender women; and women with disabilities.

A member of the Autonomous Women's Center emphasized – based on their long-standing work with women victims of family and partner violence – that men with knowledge of new technologies in the context of partner violence belong to a high-risk group of violence perpetrators.[524]

To strengthen online protection and prevent digital violence, some feminist organizations, such as the Alternative Centre for Girls and the Autonomous Women's Center, are conducting training workshops for young women and men. The Autonomous Women's Center has launched a special website, *Nechupedia – Mogu da neću,* to raise young people's awareness about digital violence in partnerships, among other things. The Alternative Centre for Girls also provides informal psychosocial support to women survivors of digital violence, while the Autonomous Women's Center provides legal counselling, assists in filing criminal lawsuits, and shares information about which state authorities and NGOs can offer assistance. Women's organizations agree that women are often discouraged from reporting online violence and give up the process of collecting evidence and prosecution due to poor treatment by the police and mistrust in the institutions. The activists believe that consultations with attorneys for women victims of this form of violence are necessary, since women experience multiple victimization without adequate support from experts or preparation.

Attacks against female activists and human rights defenders

Due to their social engagement activities in a context that is growingly increasingly authoritarian and patriarchal, the so-called women's organizations are exposed to numerous security challenges, online

522 Stevanović, Nemanja, *Policija Srbije istražuje zloupotrebe fotografija žena na Telegramu*, Radio Slobodna Evropa, 9 March 2021.

523 Interview with representatives of the Alternative Centre for Girls, 8 February 2022.

524 Interview with Vanja Macanović, 17 February 2022.

risks, and threats on social media – an extension of the violence that is already taking place in the physical space. Members of the Alternative Centre for Girls in Kruševac were exposed to hate speech and threats via social media because of their cooperation with women's organizations from Kosovo involved in women's peace activism, and due to the mention of Kosovo (not Metohija) outside the context of the UN Security Council Resolution 1244 in its organizational materials. A member of the Autonomous Women's Center (AWC), Sanja Pavlović, stated that the female activists often receive threats via social media due to their involvement in the area of women's rights, human rights, and transitional justice. Three years ago, she received a threat via social media after standing for Srebrenica with the Women in Black organization; she reported the incident to the High-Tech Crime Department at the MoI, but received no response from the competent authority: 'I never received a reply. It's as if I had sent the email to a void. [I did it] then but never again.'[525]

Female activists are also at risk of being discredited or having disinformation disseminated about their work, often from unknown persons. The same discourse, however, is used by representatives of the legislative and executive branches of power. In late 2021, Vladimir Đukanović – a member of parliament from the Serbian Progressive Party, lawyer, and member of the High Judicial Council – published on Twitter[526] a photo of an activist from the Autonomous Women's Center and wrote that: 'There are no worse thugs than feminists. They torture the society in the worst way imaginable, violating us with nonsense and trying with all their powers to destroy Serbian family. This abominable abuse of domestic violence in order to marginalize man and deprive him of his role in the family and society is horrendous.' Female activists believe that online violence is underestimated and that the failure of competent authorities to respond encourages offenders and leads to the repetition of violence.

To protect themselves from threats and attacks, female activists mainly use protective measures in the physical space, such as surveillance cameras and alarms. In the context of cyber protection, they lack specific technical knowledge, adequate IT support, and the means to protect infrastructure. Few civil society organizations and female activists are able to strengthen their cybersecurity capabilities. The Alternative Centre for Girls serves as a good role model as it has spent several years building its cybersecurity capacities, having designed a special programme on digital security, with the support of the donor community, and conducted a series of training programmes for other associations and individuals. In parallel with training, the Alternative Centre for Girls provides mentoring support to SOS centres and safe homes to develop guidelines for the security and integrity of confidential information and databases on gender-motivated violence. It has also expanded its workshop network in Serbia, working with youth on topics related to digital security.

525 Interview with Sanja Pavlović, 2 March 2022.

526 Twitter post by Vladimir Đukanović: *https://twitter.com/adv_djukanovic/status/1475602106279206913*

CONCLUSION AND RECOMMENDATIONS

Despite a solid legal framework, Serbia's fight against cyber attacks and crime progresses slowly due to the chronic lack of qualified staff

Despite a solid legal framework, Serbia's fight against cyber attacks and crime progresses slowly due to the chronic lack of qualified staff, as well as the politicized priorities of the competent institutions. The criminal justice system is not keeping pace with advances in technology; consequently, new forms of cybercrime, where computers or computer networks are used as a means or method of execution, remain outside the criminal law framework. Insufficient training and/or knowledge about cybersecurity among all actors – primarily judges, lawyers, and police officers – leads to a large number of unprocessed 'high-tech' crimes.

Certain individuals and groups, such as women, LGBTIQA+ people, journalists, and human rights defenders, are particularly vulnerable to threats posed by cybercrime, yet they are not mentioned in strategic documents related to cybersecurity. This is due to the limiting state- or corporate-centric understanding of cybersecurity, as well as the insufficiently inclusive process of developing political documents and legal regulations. As a result, most strategic documents appear to be gender neutral, but the number and type of violations of digital rights and freedom in Serbia is in fact alarming. While state bodies are somewhat effective in protecting critical infrastructure against cyber attacks, the general willingness to tolerate massive violations of citizens' digital rights is worrying.

Recommendations

- The Criminal Code should be amended to clearly define the sharing of intimate images and videos without their consent as a criminal offence. Criminal offences involving the unauthorized collection of personal data, on a large scale, should be prosecuted ex officio.
- There is a need to move from a state- or corporate-centric approach to cybersecurity to one that is more human-centric, given the impact it has on not only individuals but also national security and the corporate economy.
- Organizations representing marginalized groups in Serbia must be involved in the development of new cybersecurity strategies and laws to ensure documents reflect their needs and concerns in cyberspace.
- A new action plan should be developed for the implementation of the Strategy for Combating High-Tech Crime for the period 2022-2023.
- The monitoring of ICT system operators of particular importance should be strengthened by specifying certain criteria (such as the number of users and area); the number of operators should also be reduced.
- The number of trained police officers in four sections of the High-Tech Crime Department should be increased to enable them to fight this type of crime more effectively. Police officers should undergo training outside the Department for the Combating of Cybercrime to familiarize them with procedures related to gathering evidence and reporting crimes.

- The infrastructure capacities, the number of employees, and the technical equipment of the Special Prosecutor's Office for High-Tech Crime should be increased to allow it to perform its tasks effectively.
- Judges and attorneys dealing with high-tech crime cases should receive continuous training to avoid problems in proceedings owing to insufficient knowledge of the subject matter.
- Parliamentary oversight in the cybersecurity area should be strengthened and expert support provided to representatives in the new convocation of the assembly – especially to future members of the Committee for Education, Science, Technological Development and Information Society; the Defence and Internal Affairs Committee; as well as the Security Services Oversight Committee.
- Coordination among government bodies, as well as cooperation between the private and public sectors and civil society, must be strengthened to tackle high-tech crime more effectively. Ongoing cooperation is required, given that technology in this area and related security challenges, risks, and threats are constantly evolving.
- To fight against high-tech crime effectively, the general public should be educated about the various forms cybersecurity crime and how to protect themselves against these criminal offences. In this context, it is important to increase the public's awareness of the national CERT and to promote the RATEL contact number for reporting cyber incidents.
- The government should declare a moratorium on the use of mass biometric surveillance technologies and systems in Serbia.
- The competent ministries, as well as the donor community, should invest funds in programmes of civil society organizations that represent marginalized groups and aim to increase digital literacy and strengthen individual and organizational cybersecurity capacities, especially in the fight against online violence.
- There is a need to strengthen the civil society response and build a wider coalition between women's organizations, the LGBTIQA+ community, Roma associations, and so forth, and for cyber experts to pressure the government to end impunity regarding online violence.

CONCLUSION

Towards Better Inclusion of a Human Rights Perspective in Good Governance of Cybersecurity

By Franziska Klopfer | DCAF

CONCLUSION

TOWARDS BETTER INCLUSION OF A HUMAN RIGHTS PERSPECTIVE IN GOOD GOVERNANCE OF CYBERSECURITY

We cannot take democracy, human rights, or the rule of law for granted: they are goods that need to be protected and nurtured. In the past few decades, as an increasing amount of our lives has moved online, we have learned how democracy, human rights, and the rule of law can prosper with and through technology. Early advocates of the Internet heralded it as an unprecedented opportunity for rights such as free speech, and spoke of a new era for democracy. These assumptions were not altogether wrong, but we have also witnessed how technology and life online come with their very own sets of challenges.

The case studies included in this publication show this very well. The authors have analysed the situation regarding human rights – including rights that are essential for democratic participation such as freedom of expression, freedom of information, and freedom of assembly – and cybersecurity in the six Western Balkan economies. Their analysis has a specific focus on governance structures and aims to show how shortcomings in governance – in law; in its implementation; in the set-up, functioning, and cooperation of institutions; and in their management and oversight – can give rise to challenges for human rights and cybersecurity.

The authors have deliberately taken a human-centric approach to defining cybersecurity. This means a focus not only on securing networks and services but also on how these networks and services can be used safely by all members of society.

The six chapters show clear trends across all of these economies: for instance, important cybersecurity laws and structures have been introduced in the last decade, and much has been invested and achieved in terms of securing networks and services. However, these are still not fully secure and remain vulnerable to attacks and the theft of data. This has had detrimental effects on a number of human rights. Not enough is being done to address the issue of growing insecurity online, especially online violence. There has also been an increase in attempts to use technology to limit people's rights.

Most of the six chapters paint a picture of economies which have made great efforts to develop legal and regulatory frameworks for cybersecurity. Bosnia and Herzegovina, which in 2022 still has no national cybersecurity strategy or state-level cybersecurity law, is an exception to the rule. Other economies are already developing their second or third national cybersecurity strategy and are aligning their national legislation with the latest EU standards, such as the updated Network and Information Systems Security Directive, the so-called NIS2 Directive. EU integration has been an important driver in the region for the development of cybersecurity legislation. Digitalization has been another. Indeed, digitalization in the region is being promoted by the EU: see, for example, the Digital Agenda for the Western Balkans.

A CALL FOR A HUMAN-CENTRIC APPROACH TO CYBERSECURITY

The fact that digitalization and EU integration are the major drivers for policymaking on cybersecurity is not without its problems, as the authors point out. In fact, there seem to be few other framing principles in this arena. None of the six economies has made strong commitments to human rights in its cybersecurity policy; the objective of cybersecurity, rather, is defined as protecting networks and systems. While it can be assumed that this should be done with the aim of protecting national security, the democratic order, and the human rights of all, it is rarely spelled out explicitly. This is problematic, because it means that the limited resources available for cybersecurity are focused on securing technical systems, and national strategies do not aim to analyse or protect the rights of users – the exception being a focus on protecting children, which is a very prominent element of the current national cybersecurity strategy of Albania. Several of the authors point out these gaps and call for a more human-centric (as opposed to state-centric or technology-centric) approach to cybersecurity.

THREATS TO HUMAN RIGHTS REPRESENT A THREAT TO PEOPLE'S SAFETY AND A DEGRADATION OF DEMOCRACY ONLINE

Applying a lens of good governance to cybersecurity helps to show how threats to human rights online can become systemic threats to online democracy. The authors of the six chapters reviewed the protection and promotion of human rights online in the Western Balkan economies. Where they found challenges to human rights, they analysed the underlying governance systems. This provides a very informative picture of why abuses happen, and how and why laws, institutions, or technical systems fail or lag behind.

The six chapters identify a number of challenges to human rights online in the Western Balkan economies. One of the most prevalent is online violence. In fact, online bullying, harassment, stalking, threats, and other attacks on the safety of individuals and groups have become widespread. They are mainly directed against groups which already experience discrimination and violence in the offline world: women, minorities (in particular, the Roma community), migrants, and LGBTIQA+ persons.[527] Online violence features prominently in all six case studies, and it has a detrimental effect on a number of human rights.

Online violence also has detrimental effects on freedom of expression, the right to information, and freedom of assembly when persons are threated online with the aim of silencing them and discouraging them from being present or expressing themselves and being politically, socially, or culturally active, either online or offline. The case studies show clearly that this no longer involves just isolated cases of an individual being insulted or facing aggression. Rather, increasingly we are seeing the emergence of cyber mobs[528] – organized groups that use a variety of techniques to silence in particular journalists, activists and human rights defenders.[529] Many of them can be linked to ideological or political groups. Occasionally, there is speculation that government actors or other national or foreign political powers are behind

527 Chapter 6: Serbia – Drawing the Links to Human Rights and Investing in People', 117; 'Chapter 3: Kosovo – Strengthening New Foundations and Institutions', 65, 71; 'Chapter 5: North Macedonia – Driving Implementation to Strengthen Stakeholder Inclusion', 105; 'Chapter 4: Montenegro – Improving Awareness as a Foundation for Tailoring the Approach', 87.

528 'Chapter 4: Montenegro – Improving Awareness as a Foundation for Tailoring the Approach', 85.

529 'Chapter 6: Serbia – Drawing the Links to Human Rights and Investing in People', 130; 'Chapter 4: Montenegro – Improving Awareness as a Foundation for Tailoring the Approach', 83; 'Chapter 1: Albania – Bridging the Gap Between Cyber Policy Fragmentation and Human Rights', 28.

these organized campaigns.[530] It is clear that the intention behind such attacks is not simply to express disagreement with certain individuals or groups but to intimidate them and to stop them from taking part in social, cultural, and political lives. The authors of the chapter on Bosnia and Herzegovina link organized cyberviolence with the phenomenon of hate speech – speech meant to incite hate and violence. This shows that violence conducted online is linked to what is done offline, in the physical world.

GOVERNANCE CHANGES ARE NECESSARY TO ADDRESS ONLINE VIOLENCE

Unfortunately, the Western Balkans are not the only region where cyber violence has become widespread, organized, and detrimental to the rights and democratic participation of individuals. The case studies show why this is happening in the six economies and what needs to be done to address these issues.

In several economies, the law does not seem to adequately cover cyber violence. As authors point out, all the economies have ratified, or aligned themselves with, relevant international standards such as the Council of Europe's Convention on Cybercrime (the Budapest Convention) or its Convention on preventing and combating violence against women and domestic violence (the Istanbul Convention). However, while laws generally cover discrimination or hate speech, online discrimination and violence are not yet fully covered.[531] Moreover, the six chapters provide many examples of cases where law enforcement and the judiciary have been either unable or unwilling to investigate, prosecute, and adjudicate on cases of online violence. In some cases, there is a clear refusal to see that online violence can have similar effects to physical violence.[532] In others, police, prosecutors, and judges seem to lack the training needed to deal properly with such cases.

CYBERSECURITY, ANTI-HATE SPEECH, ANTI-DISINFORMATION MEASURES LEADING TO SILENCING OF OPPOSITION VOICES

The authors also report on a number of cases where authorities possibly over-reached in applying anti-disinformation and anti-hate speech legislation to silence opposition voices. Social media users were investigated for their online posts. Voices criticising government responses to public emergencies such as an earth quake or the COVID-19 have led to the prosecution of journalists or the shutting down of a website for reasons of 'disinformation' or 'causing panic and disorder'[533]

530 'Chapter 6: Serbia – Drawing the Links to Human Rights and Investing in People', 121, 'Chapter 2: Bosnia and Herzegovina – Navigating the Legal System and Promoting Good Practice', 43.

531 'Chapter 1: Albania – Bridging the Gap Between Cyber Policy Fragmentation and Human Rights', 14; 'Chapter 6: Serbia – Drawing the Links to Human Rights and Investing in People', 111.

532 'Chapter 2: Bosnia and Herzegovina – Navigating the Legal System and Promoting Good Practice', 53; 'Chapter 4: Montenegro – Improving Awareness as a Foundation for Tailoring the Approach', 86-87; 'Chapter 3: Kosovo – Strengthening New Foundations and Institutions', 71.

533 'Chapter 1: Albania – Bridging the Gap Between Cyber Policy Fragmentation and Human Rights', 22; Montenegro – Improving Awareness as a Foundation for Tailoring the Approach' 85; 'Chapter 6: Serbia – Drawing the Links to Human Rights and Investing in People', 124.

DATA PROTECTION AND NETWORK AND SYSTEMS SAFETY

The chapters on Albania and North Macedonia illustrate how large-scale theft of data held by public institutions can violate the right to privacy of citizens and erode their faith in institutions and democratic procedures. Large-scale cyber attacks have become more frequent in Europe, including in the Western Balkans. There is also a real or perceived increase in cases of data misuse, leakage, or theft in the region. As the authors explain, this is also a result of the increasing digitalization of public services,[534] which means that more data on citizens is stored in the networks of public institutions. The chapter on Albania examines several cases involving the theft or leaking of citizens' data and demonstrates that systems do not appear to be built with sufficient security measures. There also appears to be a lack of appropriate technical solutions and procedures to keep data safe from criminals.

A number of high-profile cyber attacks that have targeted public institutions in the Western Balkans region demonstrate how important it is to protect systems and services.[535] If this is not done, economies in the region risk experiencing interruptions to their critical national infrastructure and public services, the loss of data, and also the loss of public trust. Cyber attacks can have detrimental effects on national security and on the rights of all citizens, in particular the right to privacy (in the case of data theft or leakages) and citizens' access to public services. The case studies show that, in almost all economies, there are not enough cybersecurity experts working in the public sector and that cybersecurity infrastructure still needs to be strengthened. For example, personal data have been lost due to technical omissions by public or private actors who are unable to properly protect the systems where data are stored.[536] Human rights can therefore only be protected if these governance challenges are addressed.

GOVERNANCE SHORTCOMINGS ARE JEOPARDIZING DATA PROTECTION AND NETWORK SAFETY

The six case studies examine in detail the lack of expert cybersecurity personnel in the public sector and the reasons for this. The chapter on Albania tells a familiar story: when a major leakage of citizens' data occurred, it proved difficult to determine which institution had been at fault.[537] This points to several potential problems. There seems to be insufficient clarity on roles and responsibilities between different state institutions, and in some cases between state bodies and private actors supplying data protection services. In Albania, and in similar cases in the region, no definitive report was made or conclusions drawn to hold the relevant institutions or individuals to account. This in turn leads to a loss of trust in governments and the online services they provide.[538] In addition to challenges of coordination, the lack of qualified cybersecurity staff to protect data systems adds to the vulnerability of publicly stored data.[539] The economies of the region need to make more investments in educating, training, recruiting, and retaining cybersecurity experts in the public sector.

There also seems to be little parliamentary oversight on cybersecurity. Parliaments rarely oversee governments' cybersecurity activities and may lack the knowledge to do so effectively.[540] As regards

534 'Chapter 1: Albania – Bridging the Gap Between Cyber Policy Fragmentation and Human Rights', 23.
535 Kajosevic, Samir, *Western Balkans Urged to Prepare for Uptick in Cyber-Attacks*, BIRN, 12 September 2022.
536 'Chapter 6: Serbia – Drawing the Links to Human Rights and Investing in People', 119.
537 'Chapter 1: Albania – Bridging the Gap Between Cyber Policy Fragmentation and Human Rights', 16-17.
538 'Chapter 5: North Macedonia – Driving Implementation to Strengthen Stakeholder Inclusion', 97.
539 'Chapter 1: Albania – Bridging the Gap Between Cyber Policy Fragmentation and Human Rights', 10.
540 'Chapter 6: Serbia – Drawing the Links to Human Rights and Investing in People', 113.

independent state bodies that could oversee cybersecurity, in general appropriate institutions have not been set up. On the one hand there are institutions in charge of cybersecurity, and on the other bodies (state or non-state) that deal with human rights protection. When approached by the authors of the different chapters, ministries or state agencies responsible for cybersecurity pointed out that human rights were not part of their mandate. Human rights bodies said that they lacked expertise in cybersecurity, but some did say they believed that this was an area requiring attention.[541]

THERE ARE DANGERS IN TECHNOLOGIES ENCROACHING ON PEOPLE'S RIGHTS AND DEGRADING DEMOCRACY

The greater availability of technologies that can monitor people easily, almost anywhere and anytime, appears to be too much of a temptation for governments, even those which are considered democratic and respectful of human rights.[542] As the case studies show, governments in the Western Balkans have made use of these technologies – and this is no longer occasional use but in some economies has become systematic. The case study on Serbia explains how the government had attempted to grant its law enforcement agencies extended scope for using surveillance devices, but that a draft law was withdrawn after widespread civil society protests. This example shows how important it is to be vigilant when it comes to the use and the regulation of surveillance technologies. The compliance of legislation with international human rights standards is crucial. However, even when surveillance technologies are being used in conformity with national law and international standards, their use can have a chilling effect on human rights. The examples from Serbia and Bosnia and Herzegovina show that people have started to become hesitant about attending public protests because they are afraid of being monitored.[543]

MORE RESEARCH AND AWARENESS-RAISING ARE NEEDED TO BRING ABOUT SUSTAINABLE CHANGE

As this publication has shown, there are very real challenges for human rights in cybersecurity in the Western Balkans region. Researching these challenges allows for a detailed examination of how ICTs can have an effect on the enjoyment of rights and on democratic participation and the democratic order. By applying a lens of good governance and looking at the failures of governance that have given rise to those challenges, we can better understand them and begin searching for solutions. The case studies in this publication demonstrate that much more research and awareness-raising on governance challenges are needed. In particular, further research is needed at the national level on the roles and responsibilities of different actors in addressing human rights and cybersecurity, and on the institutional blockages that exist to addressing these challenges.

Leading on from this analysis of human rights and cybersecurity, the next piece of work planned by the Western Balkans Cybersecurity Research Network will focus specifically on gender and cybersecurity. The present publication has paved the way for this in terms of methodology and in identifying key actors and issues that also apply to gender concerns to a greater or lesser extent. This will mark progress towards a complete set of publications on the most significant issues around good governance in cybersecurity, both regionally and relating specifically to the economies of the Western Balkans.

---

541 'Chapter 1: Albania – Bridging the Gap Between Cyber Policy Fragmentation and Human Rights', 23; 'Chapter 5: North Macedonia – Driving Implementation to Strengthen Stakeholder Inclusion', 113.

542 The Guardian, *The Pegasus project*.

543 'Chapter 6: Serbia – Drawing the Links to Human Rights and Investing in People', 125-126; 'Chapter 2: Bosnia and Herzegovina – Navigating the Legal System and Promoting Good Practice', 51.

ACRONYMS AND ABBREVIATIONS

AAMS	Agency for Audio and Audiovisual Media Services
AEC	Agency for Electronic Communications (North Macedonia)
AJM	Association of Journalists of Macedonia
AKCESK	National Authority for Electronic Certification and Cybersecurity (Albania)
AKEP	Electronic and Postal Communications Authority (Albania)
AKSHI	National Agency for Information Society (Albania)
AMA	Audiovisual Media Authority
AMC	Albanian Media Council
APC	Association for Progressive Communications
APDP	Agency for Personal Data Protection
AWC	Autonomous Women's Centre
BCSP	Belgrade Centre for Security Policy
BHRT	Radio and Television of Bosnia and Herzegovina
BIA	Security Intelligence Agency
BiH	Bosnia and Herzegovina
BIRN BiH	Balkan Investigative Reporting Network in Bosnia and Herzegovina
CBM	Confidence-Building Measure
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CDT	Center for Democratic Transition (Montenegro)
CEDAW	Convention on the Elimination of All Forms of Discrimination Against Women
CEDEM	Center for Democracy and Human Rights (Montenegro)
CERD	Convention on the Elimination of All Form of Racial Discrimination
CERT	Computer Emergency Response Team
CIB	Coordinated Inauthentic Behaviour
CIIP	Critical Information Infrastructure Protection
CINS	Center for Investigative Journalism in Serbia
CIRT	National Computer Incident Response Team
CIRT.ME	Computer Incident Response Team in Montenegro
CoE	Council of Europe
CPD	Commissioner for Protection from Discrimination
CPPD	Commission for Prevention and Protection against Discrimination
CPRC	Criminal Policy Research Centre
CRC	Convention on the Rights of the Child
CRMW	International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families
CRPD	Convention on the Rights of Persons with Disabilities

CSIRT	Computer Security Incident Response Team
CSO	Civil Society Organization
DCAF	Geneva Centre for Security Sector Governance
DDoS	Distributed Denial-of-Service
DPA	Personal Data Protection Agency
EC	European Commission
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EKIP	Agency for Electronic Communications and Postal Services
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUSR	European Union Special Representative
FBiH	Federation of Bosnia and Herzegovina
FOC	Freedom Online Coalition
FOI	Freedom of information
FShF	Albanian Federation of Football
GBV	Gender-Based Violence
GDPR	General Data Protection Regulation
HERA	Health Education and Research Association
HRA	Human Rights Action (Montenegro)
HRD	Human Rights Defender
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats
IANA	Internet Assigned Numbers Authority
ICANN	International Corporation for Assigned Names and Numbers
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICTs	Information and Communication Technologies
IDM	Institute for Democracy and Mediation
IGF	Internet Governance Forum
IDP	Information and Data Protection
ISA	Information Society Agency
ISP	Internet Service Provider
ITU	International Telecommunication Union
JGI	Jones Group International
KJC	Kosovo Judicial Council
KIPRED	Kosovar Institute for Policy and Research
KOS-CERT	National Cyber Security Unit (Kosovo)
LGBTIQA+	Lesbian, Gay, Bisexual, Transgender, Intersex, Queer/Questioning, Asexual + minority gender identities and sexualities not explicitly included in the term LGBTIQA+
MANS	Network for Affirmation of the NGO Sector (Montenegro)
MISA	Ministry of Information Society and Administration
MKSF	Ministry of Kosovo Security Force
MKD-CIRT	National Centre for Computer Incident Response (North Macedonia)
MoD	Ministry of Defence
MoI	Ministry of Interior
MoS	Ministry of Security
MoU	Memorandum of understanding
MTTT	Ministry of Trade, Tourism and Telecommunications
NATO	North Atlantic Treaty Organization
nCERT	National Centre for the Prevention of Security Risks in ICT Systems of the Republic of Serbia

NCSC	National Cyber Security Council
NGO	Non-governmental organization
NIS	Network and Information Systems
NSA	National Security Agency
ODIHR	Office for Democratic Institutions and Human Rights
OIK	Ombudsperson Institution of Kosovo
ORA	Operation-Technical Agency (North Macedonia)
OSCE	Organization for Security and Co-operation in Europe
PDP	Party of Democratic Progress
PII	Personally Identifiable Information
PWDs	Persons with Disabilities
RATEL	Regulatory Agency for Electronic Communication and Postal Services
RS	Republika Srpska
SLAPP	Strategic Lawsuit Against Public Participation
SNSD	Alliance of Independent Social Democrats
SOCTA	Serious and Organized Crime Threat Assessment
SP	Socialist Party
SPAK	Special Prosecution Office Against Corruption and Organized Crime
TLD	Top-Level Domain
UBK	Administration for Security and Counterintelligence
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNSA	University of Sarajevo
UPR	Universal Periodic Review
UTIC	University Tele-Informatics Centre
VPN	Virtual Private Network
WHRDs	Women Human Rights Defenders

ABOUT DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity-building of both state and non-state security sector stakeholders. DCAF's Foundation Council members represent over 50 countries and the Canton of Geneva. Active in over 70 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality. For more information visit www.dcaf.ch and follow us on Twitter @DCAF_Geneva.

ISBN: 978-92-9222-675-6

Cover: shutterstock_450689707.jpg

EDITORS: Franziska Klopfer, Ena Bavcic, and Laylo Merali

ACKNOWLEDGEMENTS: Valentina Pellizzer has generously provided her insight and guidance throughout this year-long collaborative research.

TABLE OF CONTENTS

DCAF Geneva Centre for Security Sector Governance

DCAF-Geneva Centre for Security Sector Governance

Maison de la Paix, Chemin Eugène-Rigot 2E

CH-1202, Geneva, Switzerland

Tel: +41 22 730 94 00

Email: info@dcaf.ch

Website: www.dcaf.ch

Twitter @DCAF_Geneva