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[1] 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[2] with NATO that aims to facilitate the exchange of information and best practices on cyber threats. The Global Cybersecurity Index for 2020[3] 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

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

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

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

part of the Berlin Process,[4] 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.[5]

The Cyber Defence Strategy[6] 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.[7]

The Law on Electronic Communications established the National Centre for Computer Incident Response (MKD-CIRT) as a separate unit of the AEC[8] 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,[9] 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.[10] The Law on Interception of Communications allows for the interception

---

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

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

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

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

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

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

10 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.[11] 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,[12] which increases distrust towards institutions and creates a sense of individual powerlessness.[13]

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.[14]

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.[15] 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.

---

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

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

13 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.

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

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

The MKD-CIRT[16] 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.[17] 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.[18]

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.

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

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

18 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[19] 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.

19 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,[20] 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.[21]

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[22] 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.[23]

---

20 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.

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

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

23 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[24]) – 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.[25]

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.[26] 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.[27] 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

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

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

26 Available at *www.govornaomraza.mk*.

27 Ibid.

media.[28] The agency has also prepared guidelines for monitoring hate speech[29] 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.

---

28 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*

29 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[30] – 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[31], 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.[32] 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,[33] for example, the law states that the

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

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

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

33 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[34] 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

34 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[35] 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

35 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'.[36] Given that Russian hackers are seeking to target Western countries supporting Ukraine in its efforts to resist Moscow's invasion,[37] 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.

36 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.

37 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.