ITS INSTITUTE FOR TECHNOLOGY AND SOCIETY

Research Report

LEGAL LANDSCAPE OF DIGITAL RIGHTS IN KOSOVO

November 2024

Publisher: Institute for Technology and Society (ITS)

Author: Drinas Zeqiraj

Editor: Atdhe Lila and Lirim Bllaca

Financed by: HumanRightivism project, implemented by the Community Development Fund (CDF) and supported by the Embassy of Sweden in Pristina

Prishtina, 2024

Supported by:

ITS INSTITUTE FOR TECHNOLOGY AND SOCIETY

Institute for Technology and Society
Str. Zenel Salihu no. 28 Prishtina
https://institutets.com/

Contents

Acronyms 4
Executive Summary 6
Chapter 1 - Introduction 8
1.1 Methodology and objectives 10
1.2 Framing digital rights in Kosovo 10
Chapter 2 - International Human Rights Framework on Digital Rights 12
2.1 United Nations framework 12
2.2 Regional Human Rights Framework 13
2.3 Protection of human rights in the cyberspace 14
2.4 States' obligations towards human rights 15
2.5 Limitations of human rights 16
Chapter 3 - ICT Infrastructure in Kosovo 17
3.1 Internet disruptions and shutdowns in Kosovo 18
3.2 Internet governance in Kosovo 19
Chapter 4 - Cybersecurity, Cybercrime and Data Protection 22
4.1 Cybersecurity 22
4.3 Cybercrimes legislation 26
4.4 Data protection and the right to privacy 31
Chapter 5 - Freedom of Expression Online and Access to Information 37
5.1 The concept of Media in the context of Digital Rights in Kosovo 37
5.2 Hate speech 40
5.2.1 Legal Framework regarding Hate Speech in Kosovo 42
5.3 Defamation 45
5.4 Disinformation and Misinformation 46
5.5 Online Content Moderation 49
Chapter 6 - Digital Governance in Kosovo 54
Chapter 7 - Artificial Intelligence 58
Chapter 8 - Conclusion 60

Acronyms

AI: Artificial Intelligence

ARKEP: Regulatory Authority of Electronic and Postal Communications

ASK: Kosovo Agency of Statistics

CcTLD: Country Code top-level domain

CEDAW: Convention on the Elimination of All Forms of Discrimination Against Women

CoE: Council of Europe

CRC: Convention on the Rights of the Child

DSA: EU's Digital Services Act

ECtHR: European Court of Human Rights

ECHR: European Convention on Human Rights

EU: European Union

EU AI Act: European Commission Proposal for a Regulatory Framework on Artificial Intelligence

ICANN: Internet Corporation for Assigned Names and Numbers

ICCPR: International Covenant on Civil and Political Rights

ICESCR: International Covenant on Economic, Social, and Cultural Rights

ICT: Information and Communication Technology

IMC: Independent Media Commission

IPA: Information and Privacy Agency

NFRT: National Flash Reaction Team

OSCE: Organization for Security and Co-operation in Europe

PCK: Press Council of Kosovo

SCCs: Standard Contractual Clauses

UDHR: Universal Declaration of Human Rights

UN: United Nations

Executive Summary

This report provides a comprehensive overview of the state of digital rights in Kosovo, examining the current legal and regulatory landscape, the challenges faced in safeguarding these rights, and the initiatives being undertaken to promote a safe and inclusive digital environment. The analysis is guided by both national and international human rights frameworks, focusing on areas such as freedom of expression, privacy, cybersecurity, and access to information.

Kosovo has made significant strides in digital transformation, driven by the e-Government Strategy 2023–2027 and the Digital Agenda of Kosovo 2030, which aim to modernize public administration and enhance service delivery through digital means. Despite these efforts, the report highlights several challenges, including gaps in the legal framework, underutilization of digital infrastructure, and limited public awareness of digital rights. The report also emphasizes the need for robust cybersecurity measures and a comprehensive approach to data protection to build trust in digital services.

The findings of this report underline the importance of updating legal frameworks to align with European standards, enhancing digital literacy among citizens, and fostering collaboration between the government, private sector, and civil society. To ensure the protection and promotion of digital rights in Kosovo, the report provides targeted recommendations for stakeholders, including the development of specific regulations for emerging technologies, improved public awareness campaigns, and stronger enforcement mechanisms.

Key Findings and Recommendations:

Key Findings:

1. Kosovo faces numerous cybersecurity challenges due to gaps in legislation, a lack of public awareness, inadequate infrastructure, and insufficient skilled professionals. These factors leave the country vulnerable to cyberattacks.
2. Institutions such as the Information and Privacy Agency (IPA) are constrained by limited staff and budgets, and on the other hand the Cyber Security Agency is not yet functional, at the same time key legislation needs to be adopted.
3. Despite political independence, Kosovo lacks its own country code top-level domain (ccTLD), limiting its digital autonomy. This reliance on foreign jurisdictions for domain management affects Kosovo's ability to regulate its digital infrastructure, posing legal, privacy, and cybersecurity risks.
4. While Kosovo has adopted comprehensive data protection laws aligned with EU standards, adherence to the law on data personal data protection is inconsistent across public institutions.

5. Despite having progressive digital rights legislation, there is a lack of public awareness regarding data privacy, cybersecurity, and how to protect personal information online. This gap weakens individuals' ability to exercise and defend their digital rights.
6. Defamation is addressed through civil remedies in Kosovo, which aligns with international standards. However, disinformation and misinformation, particularly from external actors, remain prevalent, and existing regulations are insufficient for tackling the scale of the issue in the digital environment.
7. Kosovo lacks a comprehensive legal framework to regulate the moderation and removal of illegal content online. Self-regulation through the Press Council of Kosovo and other voluntary frameworks is insufficient to ensure that harmful content is effectively removed from digital platforms.
8. Platforms like Facebook have restricted content based on Kosovo's requests, but Kosovo lacks the legal mechanisms to compel online platforms to remove harmful or illegal content. This gap presents challenges for content moderation and protection against harmful digital expressions.

Key recommendations from this report include:

1. Expedite the establishment and operationalization of the Cybersecurity Agency and ensure it is adequately funded and staffed. Implement comprehensive reforms to bolster national cybersecurity efforts, including regular public awareness campaigns on data protection and online safety.
2. Amend the Cybersecurity Law to make cybersecurity training mandatory for all public officials, to enhance cybersecurity capacity across all levels of government.
3. Allocation of additional resources to the AIP to improve its capacity in handling data protection issues, ensuring that it can effectively manage its increasing case load
4. Strengthen enforcement mechanisms to ensure that all public institutions, particularly government ministries, adhere to the required data protection and cybersecurity standards.
5. Kosovo should pursue diplomatic and legal avenues to secure its own ccTLD, which would allow it to manage its digital infrastructure independently, enhance cybersecurity, and protect citizens' digital rights.
6. Develop a national strategy to combat misinformation and disinformation by incorporating media literacy programs in schools and public institutions. Engage civil society and media outlets in efforts to improve fact-checking and debunk false narratives.
7. Introduce legal frameworks that explicitly regulate online media, ensuring that digital platforms are subject to similar rules as audiovisual media. This should include mandatory adherence to ethical standards, enforceable by regulatory bodies.
8. Introduce national laws requiring online platforms to adhere to content moderation standards. Adopt principles from the EU's Digital Services Act (DSA) to enhance transparency and accountability in content moderation and online advertising.

Chapter 1 - Introduction

Digital rights are an increasingly crucial aspect of modern human rights discussions and legislative development. This report is designed to enhance ongoing efforts regarding the state of digital rights in Kosovo. It aims to serve as a valuable tool for civil society organizations, government officials, regulatory agencies, and other relevant parties committed to promoting and protecting digital rights within the country. By providing detailed analysis and recommendations, this document supports the development of informed policies and effective advocacy strategies to ensure the safeguarding of digital rights in Kosovo.

In the past, human rights concerns have been designed primarily to enhance and protect the enjoyment and exercise of rights in offline arenas. It is in this light of the development of digital technologies, in particular social media platforms, the proliferation of data-driven technologies deepfakes, bot content creation, and data lakes that put to question these limits and possibilities of rights. As a result, digital rights are now being recognized as an extension of traditional offline human rights.[1] This marks a shift from the conventional approach where individuals asserted their rights in relation to the state through human and civil rights claims. Previously, the state was responsible for respecting, protecting, and fulfilling these rights, including preventing abuses by third parties such as businesses. However, with the emerging of new technologies, the relation of the state and the market to the citizen also needs to be carefully balanced in a way that will protect civic digital rights and freedoms.

In the current era of the Internet, emerging technologies, artificial intelligence tools, decentralized databases, data management technologies, digital platforms have become integral to both personal and professional life in Kosovo. These technological advancements have transformed how people interact, conduct business, and participate in civic life, moving from traditional methods to digital and virtual environments.

Communication, financial transactions, payment systems, data storage, accounting, taxation, political organization, civic activism, legal proceedings, education, science, and business operations increasingly occur online. However, this digital transformation has introduced new challenges related to the protection of fundamental rights and freedoms, as well as the safeguarding of national security in cyberspace.

A pivotal example can be found in recent years when Kosovo experienced the powerful impact of social media as a tool for political communication, [2]democratization and government

[1] *Claudia Padovani, Francesca Musiani, and Elena Pavan, 'Investigating Evolving Discourses on Human Rights in the Digital Age: Emerging Norms and Policy Challenges' (2010) 72(4) International Communication Gazette 1. Available at https://minesparis-psl.hal.science/hal-00839944*

[2] *Arben Fetoshi and Remzie Shahini-Hoxhaj, 'The Impact of the Media in Election Campaign During the COVID-19 Pandemic: The Case of Kosovo' (2023) 16(1) Central European Journal of Communication 59. Available at: https://www.researchgate.net/publication/374843253_The_Impact_of_the_Media_in_Election_Campaign_During_the_COVID-19_Pandemic_The_Case_of_Kosovo*

accountability. Digital platforms in Kosovo have empowered freedom of expression, access to information, the ability to share ideas, protest, and associate online. The digital space has significantly influenced political campaigning, citizen journalism, and civic activism, expanding the opportunities for political engagement and public discourse.

This report presents an overview of the state of digital rights in Kosovo, guided by the Constitution and respective international human rights standards and laws, which set a human rights framework regarding the protection of these rights. The report addresses the challenges related to cybersecurity, freedom of expression online, and surveillance effects on digital rights. Finally, the report recognizes Kosovo's efforts towards advancing and protecting human rights in the digital realm and provides a series of recommendations for additional improvements.

The First Chapter introduces the concept of digital rights, highlighting their growing importance in the age of new technologies such as AI, deepfakes, bot content creation, and data lakes. It emphasizes the increasing need to recognize digital rights as extensions of human rights. The chapter underscores the shift from traditional offline rights to a more balanced approach that includes state and market responsibilities in protecting civic digital rights.

The Second Chapter discusses the international legal frameworks governing digital rights, starting with foundational UN human rights instruments like the Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights ("ICCPR"), and regional frameworks like the European Convention on Human Rights (ECHR). The chapter highlights how these frameworks apply to digital spaces and the state's obligations to protect digital rights.

The third chapter addresses Kosovo's ICT infrastructure, including internet penetration and mobile service availability. It touches on the gaps between mobile and fixed internet access and emphasizes the digital divide, especially for rural areas. The chapter also discusses internet disruptions and shutdowns, their legal framework, and implications for digital rights like freedom of expression and access to information.

The fourth chapter focuses on Kosovo's cybersecurity landscape, its legal frameworks, and challenges such as a lack of resources and public awareness. It discusses the new Cybersecurity Law, its alignment with the Budapest Convention, and the need for cybersecurity awareness and education. The chapter also delves into Kosovo's data protection legislation, the Information and Privacy Agency's role, and the challenges related to personal data protection.

Chapter five explores how media and digital platforms shape digital rights in Kosovo, with a focus on freedom of expression, hate speech, defamation, disinformation, and misinformation. It looks into Kosovo's legal provisions and regulations that protect freedom of expression online, as well as the challenges in moderating online content and ensuring access to accurate information.

In Chapter six, the focus is on how digital governance affects digital rights, particularly in areas like data management, public administration, and e-governance initiatives. It discusses Kosovo's Digital Agenda and the push for modernizing public services through digital platforms, as well as the challenges in implementing effective governance frameworks.

Chapter seven touches on the impact of AI and related technologies on digital rights, including potential risks to privacy, security, and fairness in digital interactions. It also looks at how AI-driven technologies might exacerbate existing gaps in digital governance if not properly regulated.

The concluding chapter provides a summary of findings and reiterates the importance of updating legal frameworks to protect digital rights amidst the rapid technological changes. It calls for better collaboration between the government, civil society, and private sector to strengthen Kosovo's digital infrastructure and governance mechanisms.

1.1 Methodology and objectives

The preparation of this report involved an extensive review of both international and national sources related to digital rights, including legal statutes, policy documents, research findings, and academic insights. This report aims to provide a thorough and balanced analysis of digital rights issues within Kosovo, and is structured to achieve four primary objectives:

- To analyze digital rights in Kosovo through the prism of relevant international human rights laws and national legal standards;
- To evaluate recent trends and developments concerning digital rights in Kosovo;
- To identify the existing gaps and challenges that hinder the protection and promotion of digital rights in Kosovo; and
- To offer targeted recommendations for a range of stakeholders involved in the enhancement of digital rights, including governmental agencies, civil society organizations, and private sector entities within Kosovo.

1.2 Framing digital rights in Kosovo

Digital rights are human rights in the digital realm or cyberspace, or in interaction with technology.[3] Thus, digital rights are not a set of rights in and of themselves, but are related to other human rights, particularly freedom of expression and the right to privacy in online and digital

[3] *UN Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (27 June 2016) UN Doc A/HRC/32/L.20. Accessed at < https://documents.un.org/doc/undoc/ltd/g16/131/89/pdf/g1613189.pdf?*

environments.[4] Therefore, the list of digital rights is not exhaustive, However for the needs of this report the term 'digital rights' pertains to how fundamental human rights — such as freedom of expression, privacy, and access to information — are exercised and protected in the era of the internet, social media, and technology. Saying this, digital rights are not a set of rights in and of themselves, but are related to other human rights, particularly freedom of expression and the right to privacy in online and digital environments. This framing of digital rights is deeply based in international human rights law. Instruments in human rights under the United Nations ("UN") and in the European human rights framework affirm that the very same rights people have offline should be taken online.[5] These rights are enshrined in several foundational international law instruments, including the Universal Declaration of Human Rights ,[6] the International Covenant on Civil and Political Rights ,[7] the European Convention on Human Rights ("ECHR").[8] The Constitution of Kosovo stipulates the direct applicability of these international human rights instruments, which contain specific provisions guaranteeing the rights such as freedom of expression and setting out the criteria and conditions when rights can be restricted.

[4] *Rosamond Hutt, 'What are your digital rights' (World Economic Forum, 13 November 2015) available at https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/.*

[5] *ibid. See also Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies) available at https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2014-6-of-the-committee-of-ministers-to-member-states-on-a-guide-to-human-rights-for-internet-users-adopted-by-the-committee-of-, see also European Declaration on Digital Rights and Principles for the Digital Decade (adopted by The European Parliament, the Council and the Commission)*

[6] *Universal Declaration of Human Rights, UNGA Res A/RES/217A (III) (10 December 1948).*

[7] *International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).*

[8] *Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature 4 November 1950, ETS No 5, 1951 (entered into force 3 September 1953).*

Chapter 2 - International Human Rights Framework on Digital Rights

A human right is a moral claim that an individual can raise in virtue of being a human being with inherent dignity.[9] The interrelations of humans demand mutual respect for the other's human dignity and life.[10] It is human dignity that is therefore at the center of the human rights regime. Human rights are implemented based on principles that they are 'universal, indivisible and interdependent and interrelated.'[11] Universality implies that all humans in the world are entitled to a claim of a dignified existence without any discrimination. Characteristics such as race, sex, or social position are immaterial to their entitlement to human rights. Further, human rights are indivisible in the sense that one right can invoke/imply another right.[12] For example, freedom of association implies freedom of assembly. Additionally, the effective implementation of one right can depend upon implementation of another right. For instance, freedom from arbitrary arrest invokes the right to equal protection of law. It therefore means that every right is dependent on another, and the two complement each other. Therefore, a violation of one right could be a violation of another depending on the first rights. The international human rights system is described as the body of standards enshrined in the agreement and principles expressed by states to safeguard and promote the dignity and rights of all people. It encompasses a broad area of rights that are inalienable to every human being regardless of their nationality, race, religion, gender, or any other condition.

2.1 United Nations framework

The genesis of the UN human rights framework can be traced back to its inception in 1945, emerging in response to the grave atrocities against human dignity witnessed during World War II. In the aftermath of the conflict, states united in their determination to establish a robust moral edifice aimed at safeguarding the inherent dignity of all individuals.[13] This collective resolve materialised in the form of a comprehensive human rights framework, marking the commencement of a global endeavour to enshrine fundamental rights and freedoms. The process of international recognition of human rights began with the adoption of the UN Charter in 1945 where the UN agreed that 'all people matter.'[14] Subsequently, the UN undertook the momentous task of codifying these principles, culminating in the adoption of three pivotal instruments: the UDHR in 1948, followed by the ICCPR and the International Covenant on Economic, Social, and Cultural Rights ("ICESCR") in 1966.

---

[9] *Frans Viljoen, International Human Rights Law in Africa (2nd edn, Oxford 2012; online edn, Oxford Academic, 20 April 2015).*
[10] *ibid 4.*
[11] *Vienna Declaration and Programme of Action, World Conference on Human Rights in Vienna (25 June 1993), para 5. Available at https://www.ohchr.org/en/instruments-mechanisms/instruments/vienna-declaration-and-programme-action.*
[12] *Viljoen (n 9) 327*
[13] *C J Hamelink, 'Human Rights in Cyberspace' in D Haenens (ed) Cyberidentities: Canadian and European Presence in Cyberspace (1999) 31–46.*
[14] *Ibid.*

The three UN instruments, which are referred to as the International Bill of Rights, contain several human rights including the right to life,[15] freedom from torture,[16] right to liberty,[17] right to equality before the law and equal protection of the law without discrimination,[18] right to a fair trial,[19] right to privacy,[20] freedom of expression,[21] freedom of assembly and association,[22] right to political participation,[23] right to work,[24] right to education,[25] right to free and fair elections[26] and right to health.[27]

2.2 Regional Human Rights Framework

At the regional level applicable to Kosovo, European countries, through the Council of Europe, adopted the ECHR in 1950. The ECHR guarantees fundamental civil and political rights, such as the right to life, prohibition of torture, freedom of expression, and the right to a fair trial. The ECHR came into force in 1953 and has been one of the most important frameworks for human rights protection across Europe. While Kosovo is not yet a member of the Council of Europe, its legal and institutional framework is expected to align with the standards set by the ECHR as part of its constitutional obligations. Simultaneously, the European Court of Human Rights ("ECtHR") plays a key role in ensuring the enforcement of human rights across Europe. Though Kosovo is not under the direct jurisdiction of the ECtHR due to its non-membership in the Council of Europe, its rulings and legal interpretations of the ECHR serve as guiding principles for Kosovo's court proceedings.

At the sub-regional level, Kosovo is also influenced by the human rights mechanisms of the Organization for Security and Co-operation in Europe ("OSCE"), which actively promote human rights, rule of law, and good governance in the Western Balkans. These bodies help ensure that Kosovo's legislation complies with international human rights standards.

In terms of specific instruments applicable to vulnerable groups, Kosovo also aligns with international treaties such as the Convention on the Rights of the Child ("CRC") and the Convention on the Elimination of All Forms of Discrimination Against Women ("CEDAW"). Furthermore, Kosovo has made efforts to improve gender equality and children's rights through its national laws and policies, which are heavily influenced by European and international human rights frameworks.

---

[15] *Article 3 of UDHR; Article 6 of ICCPR*
[16] *Article 5 of UDHR; Article 7 of ICCPR*
[17] *Article 9 of UDHR; Article 9 of ICCPR.*
[18] *Article 7 of UDHR; Article 25 of ICCPR.*
[19] *Article 10 of UDHR; Article 14 of ICCPR.*
[20] *Article 12 of UDHR; Article 17 of ICCPR.*
[21] *Article 19 of UDHR; Article 19 of ICCPR.*
[22] *Article 20 of UDHR; Article 21 & 22 of ICCPR.*
[23] *Article 21 of UDHR; Article 25 of ICCPR.*
[24] *Article 23 of UDHR; Article 6 of ICESCR.*
[25] *Article 26 of UDHR; Article 13 of ICESCR.*
[26] *Article 25 of ICCPR.*
[27] *Article 12 of ICESCR.*

In sum, while Kosovo is not yet fully integrated into the European human rights framework, the European Convention on Human Rights and related instruments form the backbone of its legal obligations and reforms.

2.3 Protection of human rights in the cyberspace

According to the principles of human rights solidarity, the relationship between cyber security and human rights can be complex and multifaceted as the internet and other digital technologies have become increasingly crucial for the exercise of many human rights. Recognizing the alarming instances of human rights violations in cyberspace perpetrated by both governments and non-state actors, the UN has acknowledged the significance of safeguarding human rights in the online realm.[28] Upholding human dignity is important both offline and online

Consequently, the UN General Assembly therefore committed to creating an inclusive, people centred information society that aligns with and respects the principles of the UDHR.[29] In 2016, the UN reiterated the principle that 'the same rights that people have offline should also be protected online.'[30] This paradigm of 'human rights in the internet era' is encapsulated by the concept of digital rights, which serve as an extension of traditional human rights tailored to the demands of the digital age.[31] The UN Joint Declaration on Freedom of Expression and the Internet, for example, spotlights the significant role of the internet in empowering billions worldwide by amplifying their voices, facilitating access to information, and enhancing their capacity for reporting. Based on this, promoting and safeguarding freedom of expression and the right of access to information in the digital sphere is important.[32] While the ICCPR does not expressly address the realisation of freedom of expression in a digital space, Article 19 is expansively formulated to ensure the exercise of this fundamental right through any chosen medium. The Human Rights Committee, in its General Comment 34, further elaborated on Article 19, emphasising the indispensable nature of freedom of opinion and expression for promoting transparency and accountability within societies. Additionally, the scope of this right is wide and includes political discourse, canvassing, teaching, discussion of human rights, and journalism through various means including 'electronic and internet-based modes of expression.'[33]

---

[28] *MI Franklin, 'Human Rights Future for the Internet' in Mathias Ketteman (ed) Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations (2019) 7*

[29] *ibid 5.*

[30] *United Nations Human Rights Council, Resolution A/HRC/RES/32/13: Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet (18 July 2016, 32nd Session, Geneva) para 1.*

[31] *Rosamund Hutt 'What are your digital rights' World Economic Forum 13 November 2015, available at: https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/#:~:text=Rosamond%20Hutt&text=Digital%20rights%20are%20basically%20human,Universal%20Declaration%20of%20Human%20Rights.*

[32] *United Nations Human Rights Council, Joint Declaration on Freedom of Expression and Elections in the Digital Age (30 April 2020), available at https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/JointDeclarationDigitalAge_30April2020_EN.pdf.*

[33] *United Nations, 'General Comment 34 CCPR/C/GC/34: General Comment 34 of the International Covenant on Civil and Political Rights on Freedom of Opinion and Expression' (2011) para 12, available at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.*

Another important document is the Budapest Convention on Cybercrime (2001), which was the first international treaty to focus specifically on crimes committed via the internet and other computer networks. It provides a legal framework for combating cybercrime, including attacks against information systems.[34] It also addresses issues such as infringements of copyright, computer-related fraud, child sexual exploitation material, hate crimes, and violations of network security. The convention resulted from recognition by signatories that it was necessary "to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation".[35] It requires parties "to adopt appropriate legislation against cybercrime; ensure adequate procedural tools to effectively investigate and prosecute cybercrime offences; and to provide international co-operation to other parties engaged in such efforts".[36] The Convention also recognizes the need for cooperation between states and private industry in combating cybercrime. It promotes the need for better international police and judicial cooperation in the area of cybercrime, reinforced through the creation of a 24/7 network This required every party to: Designate a point of contact available on a twenty-four hour, seven-days-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.[37]

Although Kosovo is not a member of the Council of Europe and, as such, has neither signed nor ratified the Budapest Convention on Cybercrime, according to a profile prepared by the Cybercrime Programme Office of the Council of Europe 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. 08/L-173 on Cyber Security; Code No. 06/L-074 Criminal Code of the Republic of Kosovo; Law No. 04/L-109 on Electronic Communications; and Law No. 04/L-213 on International Legal Cooperation in Criminal Matters.[38]

2.4 States' obligations towards human rights

Governments are obliged to respect, protect, fulfil, and promote human rights of all equally without distinction. Similarly, they are tasked with honoring human rights by enabling individuals to freely exercise their entitlements without undue interference.[39] For example, the state should refrain from curtailing freedom of expression which includes the right of individuals to freely express their opinions. Any unwarranted encroachments on these rights is regarded as human rights violations. To ensure the protection of human rights, governments are required to adopt measures including legislative frameworks, to prevent violations by both private entities and governmental bodies.

---

[34] *A Minovic, A Abusara, E Begaj, V Erceg, P Tasevski, V Radunović and F Klopfer, Cyber Security in the Western Balkans: Policy Gaps and Cooperation Opportunities (Diplo Foundation 2016).*
[35] *Council of Europe, Convention on Cybercrime (Budapest, 23 November 2001) ETS No 185, art 3.*
[36] *ibid 8.*
[37] *Ibid 20.*
[38] *Council of Europe, Kosovo Cyber Crime Legislation: Domestic Equivalent to the Provisions of the Budapest Convention, available at https://rm.coe.int/octocom-legal-profile-kosovo/16809e5451.*
[39] *Article 2 of ICCPR, member states of the ICCPR undertake to respect and ensure rights in the convention.*

Thus, not only governments but individuals as well have a duty to uphold these rights and refrain from infringing upon the rights of others. Moreover, fulfilling these rights necessitates proactive steps from governments to ensure their citizens can fully enjoy them. This might involve initiatives like constructing schools to facilitate access to education—a fundamental human right. Additionally, governments have a crucial role in promoting awareness and understanding of human rights among the populace. Through the ratification of international human rights instruments, governments commit to upholding and safeguarding the rights of all individuals within their jurisdiction, without distinction of any kind such as race, sex, birth or other status.[40] States should ensure that human rights are upheld on the internet just as they are in the physical world, including respect, fulfilment, protection, and promotion. This necessitates the implementation of legal frameworks and other measures to safeguard internet users from digital rights infringements, including cybercrimes. However, some regulations run the risk of encroaching upon the very rights they aim to safeguard. Therefore, it is crucial for states to find a delicate balance between combating digital offences and guaranteeing the protection and promotion of digital rights.

2.5 Limitations of human rights

Though human rights are legally protected, most rights are not absolute and can be subject to justifiable limitations. A limitation should be lawful; serve a particular objective such as balancing human rights with state security or public order; preserve the rights of another; or any legitimate purpose.[41] To justify the limitation, the impact it has on human rights should be carefully weighed against the legitimate state interest being pursued. The negative impact of the limitation should be outweighed by the importance of the state interest. Additionally, the limitation should be deemed necessary and proportionate in relation to achieving its intended goal. Before analyzing Kosovo's protection of digital rights, it is prudent to provide a national context of the state of internet access.

[40] *Ibid.*
[41] *See for example Carson and others v. the United Kingdom, application no. 42184/05, March 16, 2010, § 61.*

Chapter 3 - ICT Infrastructure in Kosovo

Effective Information and Communication Technology ("ICT") infrastructure comprises multiple essential components, including a significant inventory of computers and mobile phones, robust connectivity infrastructure with global access, and widespread availability of electricity to support a broader population.

The 2023 survey on Information and Communication Technology usage in households, conducted by the Kosovo Agency of Statistics ("ASK"), highlights the nation's impressive internet penetration rate, with 98.6% of households reporting access to the internet.[42] This widespread connectivity underscores Kosovo's continued advancement in digital infrastructure. Age group analysis reveals that internet access is particularly high among younger populations, with 21.5% of users falling in the 16-24 age bracket and 21.4% in the 25-34 age range. In contrast, the older generation, specifically those aged 65 and above, represents the smallest proportion of users, with only 7.9% having internet access. The survey also identifies a relatively balanced gender distribution in internet use, with women slightly outpacing men at 51.7% compared to 48.3%. In terms of devices used to access the internet, mobile phones and smartphones dominate, with 94.8% of individuals utilizing these devices, reflecting the increasing reliance on mobile technology. Other devices, such as laptops (22.1%), desktops (11.9%), and tablets (9.7%), were also used, though to a lesser extent.

Additionally, the Overview of the Electronic Communications Market for Q1 2024 done by Regulatory Authority of Electronical and Postal Communications ("ARKEP") shows that there is a high penetration of mobile services at 104.2% (meaning that, on average, there are more mobile subscriptions than the total population) and mobile internet access at 89% reflecting a significant progress in ensuring that the majority of Kosovars have access to communication tools.[43] This widespread access is fundamental to supporting digital rights, as it enables individuals to participate in the digital economy, access information, and express themselves online. However, despite this progress in mobile services, there are notable challenges when it comes to fixed internet access, which lags with a penetration rate of only 20.7% per capita.[44] This slower growth might raise concerns about digital inclusion, especially for those relying on more stable and high-speed broadband services, often needed for work, education, and other essential services. This discrepancy between mobile and fixed internet access suggests that while basic digital rights are being upheld, there may be inequalities in the quality of access, with rural or lower-income households potentially facing greater barriers to reliable, high-speed internet. On the long term, the recent issuance of a general authorization by ARKEP for Starlink, a global leader in satellite internet services, might address these challenges.[45] Starlink's satellite technology offers the

[42] *Statistical Agency of Kosovo, Rezultatet e Anketës së Përdorimit të Teknologjisë Informative dhe Komunikimit (TIK) në Ekonomitë Familjare 2023 [Results of the Information and Communication Technology (ICT) Usage Survey in Family Economies 2023] (2023) available at https://ask.rks-gov.net/Releases/Details/7600.*

[43] *Regulatory Authority of Electronic and Postal Communications, Publikim Nr.02/2024 [Publication No.02/2024], available at https://www.arkep-rks.org/desk/inc/media/187B29B9-D1A1-4E35-824C-3AF6B2C74306.pdf.*

[44] *ibid*

[45] *Regulatory Authority of Electronic and Postal Communications, 'Notification on General Authorization for Satellite Services by Starlink' (ARKEP, October 2024) available at https://www.arkep-rks.org/NewsDetails/7/1187*

potential to provide high-speed internet access to remote and underserved areas, which have traditionally struggled with reliable connectivity. By introducing satellite internet services in Kosovo, this development could help bridge the gap in fixed internet access, ensuring that more citizens, particularly those in rural and isolated regions, can benefit from stable, high-speed internet. This would contribute to greater digital inclusion and further support digital rights, ensuring equal access to online resources and services across the country.

However, on the other hand, the Q1 overview reported a 9% decline in total sector revenues and a substantial 35.9% decrease in investments in the ICT sector. Thus if investments continue to fall, it may slow down the goal of achieving 50% coverage of population with a 5G connection by 2025, respectively 100% coverage of population with a 5G connection by 2030 as foreseen in the Kosovo Digital Agenda 2030,[46] limiting future improvements to digital accessibility and thus infringing on the digital rights of those currently without reliable quick connection.

The decrease in the average revenue per user for mobile services from €5.10 to €4.78 suggests that mobile services are becoming more affordable, which is positive from a digital rights perspective.[47] More affordable services ensure that a larger proportion of the population can access the internet and mobile communications.

3.1 Internet disruptions and shutdowns in Kosovo

People have the ability to access information and share their viewpoints across various internet forums. However, during periods of heightened political tension, governments may resort to shutting down or interfering with internet access, effectively preventing the public from utilizing these platforms. AccessNow, an international NGO that focuses on digital rights defines an internet shutdown as "an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information."[48] A shutdown can take the form of blocking, when certain websites or apps are inaccessible; or full blackout, when internet-based applications, platforms, and pages are inaccessible.

Under the ICCPR, individuals are entitled to exercise their rights "regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of their choice."[49] This broad definition supports wide freedom of expression and the right to access information among others via the internet. However, disruptions to internet service hinder these rights by obstructing participation in decision-making processes, and restricting the flow of information. Essentially,

[46] *Government of Kosovo, Agjenda Digjitale e Kosovës 2030: Orientimi strategjik për transformimin e Kosovës në një vend të suksesshëm digjital [Digital Agenda of Kosovo 2030: Strategic Orientation for Transforming Kosovo into a Successful Digital Country] (2024), 32 available at https://arkep-rks.org/desk/inc/media/82582FB3-CD31-4D3D-A2AA-F7CC21ACADCA.pdf.*
[47] *Ibid.*
[48] *'Keep It On' (Access Now, n.d.) available at https://www.accessnow.org/campaign/keepiton/.*
[49] *Article 19, para 2 of ICCPR.*

these internet shutdowns infringe upon digital rights, notably the rights to freedom of expression and access to information.

In 2024 alone, worldwide as of the time of writing of this report there have been 35 major internet shutdowns in 16 countries. Numerous countries have enacted legislation that permit authorities to interrupt internet services or assume control over telecom networks, citing national security or public safety justifications. For example, India's "Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules" provides a legal framework for the government to halt internet and telecommunications operations.

In response to such practices, the United Nations took a significant step in 2016 by passing a resolution that decries actions aimed at deliberately blocking or disrupting access to and distribution of information online.[50] This resolution labels such measures as violations of international human rights law.

Having that in mind, it is interesting to note that article 7 paragraph 1 subparagraph 1.9 stipulates that the Ministry responsible for electronic communication sector (i.e. Ministry of Economic Development) "in cases of force majeure, extreme situations, or other extraordinary circumstances, as well as for the purpose of preparing for general mobilization or national defense, or guaranteeing national security and public order, in accordance with the procedures defined by laws and acts of other legal provisions, provides mandatory instructions, duties and obligations for entrepreneurs who provide networks and/or services." While the provision in question is broad in scope and might initially seem to permit the authority to mandate service providers among others to shut down the internet, it is important to consider the constitutional safeguards in place. Article 55 of the Constitution of Kosovo stipulates that any limitation on human rights must be explicitly authorized by law and must adhere to the principles of necessity and proportionality. Therefore, without a specific and clear legislative provision that explicitly authorizes internet shutdowns, such actions would not be legally supported within the existing legal framework of Kosovo, rendering them unlawful. Thus, it is worth noting that there has never been an internet shutdown in Kosovo.

3.2 Internet governance in Kosovo

One critical area where Kosovo's independence remains constrained is in the digital domain. The refusal of the Internet Corporation for Assigned Names and Numbers ("ICANN") to grant Kosovo its own country code top-level domain ("ccTLD") has left the country in a state of digital uncertainty, directly impacting its ability to assert full autonomy in the online sphere.[51] The ccTLD is the portion of a web address that comes after the second "dot" when it is shorthand for a country

[50] *Article 19, Internet Statement [Internet Declaration] (Adopted 15 March 2020) available at https://www.article19.org/data/files/Internet_Statement_Adopted.pd*

[51] *Marc J Randazza, 'Kosovo's Digital Independence: Time for Kosovo's ccTLD' (2016) Wisconsin International Law Journal, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2754182.*

code,[52] as such it is not just a technical asset; it is a symbol of national sovereignty and independence. It gives countries control over their digital presence, allowing them to manage their own domain registries, direct internet traffic locally, and govern legal issues tied to online content.

Thus, despite its political independence from Serbia, Kosovo's official ccTLD remains ".rs" under the Serbian National Internet Domain Registry. This means that, technically, any attempt to claim a Kosovar ccTLD is blocked by international systems that rely on political recognition frameworks. For practical reasons, Kosovo uses generic top-level domains ("gTLDs") like ".com", ".net", and ".org" for government, business, and civil society websites.

In this aspect, accTLD is not just a technical asset; it is a symbol of national sovereignty and independence. It gives countries control over their digital presence, allowing them to manage their own domain registries, direct internet traffic locally, and govern legal issues tied to online content. For this reason, the absence of a ccTLD has quite some economic consequences. Owners of Kosovar websites are forced to compete on the international domain market to secure desirable domain names, often paying inflated prices. As a result, many Kosovar websites resort to convoluted web addresses with hyphens and acronyms, diminishing their legitimacy and branding. Government websites like rks-gov.net and mfa-ks.net are examples of this compromise, undermining the authority of official communication channels. Moreover, the inability to control its own domain registry means that Kosovo cannot generate revenue from domain sales.

On the other hand, Kosovo's lack of a ccTLD also raises complex legal and security concerns. Without its own domain registry, disputes over Kosovar websites using gTLDs like ".com" fall under U.S. jurisdiction.[53] This exposes Kosovo-based businesses and government entities to external legal threats. For example, in 2012, American prosecutors shut down a Canadian betting website with a ".com" domain, highlighting the potential vulnerability of Kosovar websites to foreign legal actions.[54]

Kosovo's lack of digital independence has profound implications for the digital rights of its citizens. The UDHR guarantees the right to freedom of expression and access to information "through any media and regardless of frontiers." Yet, without its own ccTLD, Kosovo's online presence is subject to foreign jurisdictions, which may not always uphold the same standards of free expression or privacy.

Kosovo's use of ".com" or ".net" subjects its internet traffic to U.S. laws, where surveillance practices have been criticized,[55] placing Kosovar citizens at risk of having their data monitored by foreign governments without their consent, thus infringing on their right to privacy. Without control over its own ccTLD, Kosovo cannot effectively regulate or protect its online content from

[52] *Ibid.*
[53] *Ibid.*
[54] *Ibid.*
[55] *American Civil Liberties Union, 'NSA Surveillance' (ACLU) available at https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance.*

censorship or cyberattacks originating in other countries. From a security perspective, this reliance on U.S.-based domains exposes Kosovo's digital ecosystem to surveillance and cybersecurity risks, as data is routed through foreign jurisdictions, leaving Kosovo with little control over who accesses or monitors its internet traffic. This not only compromises the privacy of its citizens but also undermines the sovereignty of Kosovo's digital infrastructure.

The broader implications for digital rights in Kosovo extend beyond privacy. Search engine optimization, a vital tool for visibility in the digital age, is also affected.[56] With no local domain, Kosovar websites struggle to rank higher in Google searches, particularly on local search engines like Google.ks, which does not exist. This lack of visibility hampers local businesses, civil society organizations, and even government outreach efforts, limiting their ability to reach a global audience.

To achieve full digital independence, Kosovo needs its own ccTLD. This would allow it to manage its own internet traffic, protect its digital infrastructure, and ensure that its citizens' digital rights are fully respected. In the absence of this, Kosovo remains a digital vassal, forced to operate under foreign jurisdictions and deprived of a critical component of its sovereignty.

While ICANN's rules are tied to political recognition frameworks, there is a growing case for reform. The digital world moves faster than political bodies like the UN, and the ability of a nation to control its own digital infrastructure should not be beholden to geopolitical disputes. Granting Kosovo a ccTLD would not only affirm its sovereignty in the digital realm but also safeguard the rights of its citizens in an increasingly interconnected world.

[56] *Kosovo 2.0, 'Kosovo's Recognition Missing in Online Domain' (Kosovo 2.0) available at https://kosovotwopointzero.com/en/kosovos-recognition-missing-in-online-domain/.*

Chapter 4 - Cybersecurity, Cybercrime and Data Protection

The section discusses the protection of digital rights in the context of cybersecurity, cybercrime and data protection.

4.1 Cybersecurity

Cybersecurity is 'the practice of protecting computers, electronic systems, networks and data from malicious attacks.'[57] It involves ensuring the confidentiality, integrity, and availability of information within the digital space, as well as protecting the assets of internet users.[58] Confidentiality of information relates to 'preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.'[59]This aspect of cybersecurity is closely tied to the preservation of privacy rights. Integrity ensures that data, whether stored, transmitted, or processed, remains protected from unauthorized changes or destruction, thereby ensuring its authenticity and accuracy. This principle is related to the broader framework of data protection. Lastly, availability emphasizes the timely and reliable access to information, ensuring the right to information and the free flow of data is upheld.

Safeguarding information and computer systems is accomplished through a comprehensive strategy that includes encryption methods, strict user access regulations, regular hardware upkeep, and prompt system updates to address potential security risks.[60] Cyberattacks frequently target weaknesses in digital infrastructures. As a result, cybersecurity acts as a crucial defense mechanism in the online environment, playing a significant role in protecting privacy rights, ensuring access to information, and maintaining the free flow of data.[61]

The unrestricted flow of information in cyberspace is closely tied to the freedom of opinion and expression, as it fosters open interaction.[62] In the digital world, people from various backgrounds come together to discuss political and socioeconomic issues.[63] As such, protecting freedom of expression online is essential because it also supports the rights to assembly, association, and public participation. The UN Special Rapporteur on Freedom of Expression and Opinion has highlighted the internet's vital role as a communication tool that enables the exercise of information rights, as outlined in Article 19 of both the UDHR and the ICCPR.[64] In support of this

---

[57] *Kaspersky, 'What is cyber security?', available at <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.>*
[58] *M D Cavelty and C Kavanagh, 'Cybersecurity and Human Rights' in B Wagner et al (eds) Research Handbook on Human Rights and Digital Technology (2019) 75.*
[59] *ibid.*
[60] *As above, See also International Organisation for Standardisation, ISO/IEC 27032:2012 Guidelines for Cybersecurity (2012).*
[61] *See Article 3 of the UDHR, see Article 36 of the Constitution of Kosovo.*
[62] *See Article 40 of the Constitution of Kosovo*
[63] *Cavelty & Kavanagh (n 58) 86.*
[64] *United Nations, Report A/HRC/17/27: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue (2011) available at* https://www.ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/17/27

view, the UN continues to emphasize the importance of the principle that the rights individuals have offline must also be safeguarded in the digital environment.[65]

In 2023, Kosovo adopted the Law No. 08/L-173 on Cyber Security addressing cybersecurity challenges the country. As it was noted on the Kosovo 2023 Report of the European Commission, the legislation on Cybercrime is generally in line with the EU *acquis*.[66] The Law on Cyber Security mandates the obligation to develop the requisite regulatory frameworks including the establishment of effective regulatory authorities. Through this law the Cyber Security Agency is foreseen to be created as the central authority designed to coordinate cyber agencies across the country. However as of now the Agency for Cyber Security is not operational yet. The Agency will act as the central hub for the rules, management, and regulation of cybersecurity policies, as well as for inter-agency coordination. The Cybersecurity Agency will be established as an executive agency responsible for regulating the duties of two main categories of entities: Operators of Essential Services[67] and Digital Service Providers[68]. Within the category of Operators of Essential Services, both public and private entities that possess critical infrastructure as defined by the Law on Critical Infrastructure are included. While in the category of Digital Service are included all entities that offer digital services.

This new regulation effectively addresses the existing fragmentation in the cybersecurity sector. Thus, the Agency for Cyber Security as a centralized agency will streamline the coordination and management of cybersecurity efforts across various public and private entities.

The Agency's role is envisaged to coordinate and monitor the activities and operations of critical infrastructure and cybersecurity agencies, and at the same time manage and supervise incident response alongside the National CERT (the team for response to computer emergencies at the national level) and sector specific National sectoral CSIRTs (the cyber security or cyber security incident response teams that affect a specific sector at the national level) and will facilitate the exchange of intelligence and information.[69]

---

[65] *United Nations Human Rights Council, Resolution A/HRC/RES/32/13: Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet (2016).*

[66] *European Commission, Report on Kosovo 2023 (Brussels, 2023) 45, available at https://neighbourhood-enlargement.ec.europa.eu/kosovo-report-2023_en.*

[67] *Operators of Essential Services are considered critical infrastructure ownesr or other persons that manage, run or operate, in whole or in part, the day-to-day operations of critical infrastructure (an asset, system or part thereof, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and disruption or destruction of which would have a significant impact on the Republic of Kosovo) See Republic of Kosovo, Law No 06/L-014 on Critical Infrastructure [Ligji Nr. 06/L-014 për Infrastrukturën Kritike] (2013) available at https://gzk.rks-gov.net/ActDetail.aspx?ActID=16313&langid=2.*

[68] *Operators of Digital Service Providers are defined as entities that offer digital services, which include a range of technology-based information and communication services such as online marketplace services, internet search, and cloud-computing services. See Republic of Kosovo, Law No 08/L-173 on Cyber Security (2023) art 3 para 1.13–1.14 available at https://gzk.rks-gov.net/ActDetail.aspx?ActID=70933*

[69] *See Law No. 08/L-173 on Cyber Security.*

Broadly the Agency's role is envisaged to: recognize and identify threats to critical information infrastructure;[70] develop national strategies to respond to cybersecurity attack incidents together with the Ministry of Internal Affairs and the National Cyber Security Council;[71] adopt cyber security monitoring structures; sensitize the public and build capacity on cybersecurity; and establish international cooperations on the matter.

Nevertheless, Kosovo Cyber Security Strategy indicates that the increase in internet users has 'brought with it an increased risk in terms of cyber crimes and attacks',[72] indicating that Kosovo Kosovo is susceptible to cybersecurity attacks due to several key factors.

Firstly, Kosovo faces challenges streaming from inadequate adoption of cybersecurity legislation, leaving gaps in regulatory frameworks necessary for robust protection.[73] Secondly, the general public has a limited understanding of cyber threats and the crucial steps required for protection against such risks.[74] Thirdly, the presence of inadequate infrastructure intensifies vulnerabilities and provides openings for potential cyber-attacks. To continue, Kosovo faces a shortage of skilled cybersecurity professionals equipped to effectively mitigate and respond to cyber-attacks,[75] further compounding its vulnerability in this rapidly evolving digital landscape. Lastly, as noted on the

[70] *See article 8 of the Law No. 08/L-173 on Cyber Security.*
[71] *See article 23 the Law No. 08/L-173 on Cyber Security. The National Cyber Security Council is an independent advisory body that provides strategic guidance on cybersecurity matters to the government and business community, composed by both representatives from government institutions, law implementation institutions, public and private organizations and scientific community. The role of this Council is to coordinate national and international cybersecurity initiatives, and monitor the implementation of the National Cyber Security Strategy.*
[72] *Government of Kosovo, Kosovo National Cyber Security Strategy 2023-2027 (2023) 33, available at: https://mpb.rks-gov.net/Uploads/Documents/Pdf/EN/2692/Strategjia%20p%C3%ABr%20Siguri%20Kibernetike%20-%20ENG..pdf.*
[73] *The sublegal acts needed to enforce the law were supposed to be approved within one year after the entry into force of this Law. The law entered into force on 14 March 2024 and as of now only 4 out of 12 sub-legal acts foreseen by the law were adopted. Out of this sub laws that were not adopted, deal with:*

1. *The description of the security measures for the network and information system, used for the provision of an essential service and the requirements for the preparation of the risk assessment (article 5, paragraph 6 of the Law);*
2. *Procedures and response measures in the case of a cyber incident (article 5, paragraph 8 of the Law);*
3. *The procedure for taking the measures for the purpose of preventing an imminent serious threat or the elimination of any disruption in the event of a cyber incident, that allows Kosovo Cyber Security Agency to temporarily restrict or discontinue the use or access to a network or system (article 11, paragraph 3 of the Law);*
4. *Rules and procedures for the process of certification and preparation of the list of non-reliable information and communication technology equipment and services (Article 16, paragraph 14 of the Law)*
5. *Rules and security measures for children's access to the Internet, which all Internet service providers in the Republic of Kosovo will be obliged to implement (Article 16, paragraph 15 of the Law)*
6. *Rules for the functioning of the National Cyber Security Council (Article 20, paragraph 8 of the Law)*
7. *Rules for the coordination and cooperation of state mechanisms for the prevention of cyber attacks and cyber protection in the Republic of Kosovo (Article 22 of the Law)*
8. *The composition and the mandate of the members of the Complaint Commission responsible for fines that are issued against operators of essential services and providers of digital services that not take the measures in accordance with the Law on Cyber Security*

[74] *Balkan Policy Research Group, Kosovo in the Face of Cybersecurity Threats: Critical Actions to Consolidate Resilience (Balkan Policy Research Group) available at: https://balkansgroup.org/wp-content/uploads/2023/09/Cyber-Security.pdf.*
[75] *Government of Kosovo (n72), 28.*

Kosovo 2023 Report of the European Commission the budgetary resources for cybersecurity remain insufficient.[76]

The Kosovo Cyber Security Strategy has introduced several key improvements aimed at strengthening the country's cyber defenses. Notably, the establishment of the National Flash Reaction Team ("NFRT") is a very positive development. The NFRT will provide technical assistance, continuously monitor systems for potential vulnerabilities and ensure that security patches are applied promptly.[77] Additionally, a cyber range will be created as a platform for testing and implementing new technologies, and simulate real-world cyber threats, to test new cybersecurity tools, strategies, and response mechanisms in a controlled environment.[78] The importance of cybersecurity education is also emphasized, with plans to develop training programs and curricula for schools and universities, including courses on hacking and cybersecurity fundamentals that will also focus on closing the gender gap in the field.[79]

On the other hand, through the new Law on Cyber Security, the Cybersecurity Training Center within the Ministry of Defense was created.[80] This center although not operational yet, it is designed to train and enhance the capabilities of all staff involved in managing and administering information systems. Although the respective sub-law has been adopted, there are noticeable gaps in the regulation of this new institution. Notably, while the training is intended to be accessible to a broad spectrum of public officials, there is no mandatory requirement for undergoing such cybersecurity training.[81] Furthermore, the training appears to be tailored to individuals who already possess a basic understanding of cybersecurity, as all participants are required to have foundational knowledge in this area.[82]

While the training sessions are optional, they are open to a wide range of public administration employees.[83] Yet, article 6 of the Regulation (GRK) – No. 22/2023 on the Duties and Responsibilities of the State Cyber Security Training Center, judges and prosecutors are not granted the right to attend these trainings. This omission is particularly significant since these officials play a crucial role in investigating and prosecuting cybercrime. Notably, this group of employees has been identified in the EU Commission report for Kosovo as having limited access to cybercrime training,[84] underscoring the need for inclusive and comprehensive training provisions that encompass all key public officials involved in cybersecurity and cybercrime enforcement.

---

[76] *European Commission (n66), 96.*
[77] *Government of Kosovo (n72), 23.*
[78] *Ibid 24.*
[79] *Ibid 26.*
[80] *See Article 21 of Law No. 08/L-173 on Cyber Security.*
[81] *See Regulation (GRK) – No. 22/2023 on the Duties and Responsibilities of the State Cyber Security Training Center.*
[82] *See Article 9, paragraph 1 of Regulation (GRK) – No. 22/2023 on the Duties and Responsibilities of the State Cyber Security Training Center.*
[83] *See Article 7 of Regulation (GRK) – No. 22/2023 on the Duties and Responsibilities of the State Cyber Security Training Center.*
[84] *European Commission (n66) 48.*

Another shortcoming of the new cybersecurity law is the absence of responsible disclosure measures.[85] Responsible disclosure, also known as coordinated vulnerability disclosure, is when security flaws are reported privately to the responsible parties before being made public. This gives organizations time to fix the issues, which helps to prevent cyberattacks. Many governments and big companies use this model, often rewarding those who report vulnerabilities with recognition, not just money. Without including responsible disclosure, the law misses an opportunity to boost security by encouraging experts to share their findings safely. The issue of responsible is mention only briefly, in the Kosovo Cyber Security Strategy saying that "one of the mechanisms that should be implemented is the establishment of a reward system for reporting vulnerabilities".[86]Although setting up such a system might have costs, the long-term benefits of preventing cyberattacks and reducing response costs far outweigh the expenses.

4.3 Cybercrimes legislation

Cybercrime refers to the use of computer systems, network devices, or the internet to commit criminal acts, including computer fraud and forgery.[87] In this regard, cybercrime legislation provides a framework for tackling cybercrimes, though defining conduct that should be criminalized and provides the procedure for the investigation and prosecution.[88]

The 2001 Convention on Cybercrime, also known as the Budapest Convention[89], established by the Council of Europe, emphasizes that while addressing cybercrime, countries must ensure a balance between law enforcement efforts and the protection of human rights as outlined in ICCPR. This includes key rights such as freedom of expression, privacy, and access to information. As the first international treaty to tackle crimes committed on the internet,[90] the Budapest Convention aims to create a unified approach to safeguarding society from cybercriminal activities through the implementation of relevant laws and fostering global cooperation.[91] The convention criminalizes offenses like computer-related fraud and forgery, breaches of computer networks, and child exploitation material. Additionally, it outlines procedures for investigating these crimes, such as the search of computer systems, real-time data collection, and lawful interception of communications.

Although Kosovo is not a state party to the Budapest Convention, it has previously made efforts to align its legislation with it by enacting Law No. 03/L-166 on the Prevention and Fight Against Cyber Crime. However, this law was abolished in 2023 and replaced by two new legal frameworks: Law No. 08/L-173 on Cyber Security and Law No. 08/L-187, which amends and supplements the

[85] *Balkans Policy Research Group (n74) 3.*
[86] *Government of Kosovo (n72) 25.*
[87] *Michael Aaron Dennis, 'Cybercrime' (Encyclopedia Britannica, 19 September 2024), available at https://www.britannica.com/topic/cybercrime.*
[88] *Cavelty & Kavanagh (n58) 97.*
[89] *Council of Europe, Convention on Cybercrime (n35)*
[90] *Council of Europe, 'Impact of the European Convention on Human Rights' available at https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime#/.*
[91] *Council of Europe, Convention on Cybercrime (n35), see the Preamble.*

Criminal Procedure Code No. 08/L-032.[92] Notably, Law No. 08/L-173 on Cyber Security does not include specific provisions related to the prosecution or criminalization of cybercrime, unlike the previous legislation which directly addressed cybercrime offenses. However, the sanctioning of cybercrime is now incorporated into the newly adopted Law No. 08/L-188, which amends and supplements the Criminal Code No. 06/L-04 of the Republic of Kosovo ("Criminal Code of Kosovo"), thereby ensuring that cybercrimes are still prosecuted under the updated legal framework.[93]

The Penal Code of Kosovo comprehensively addresses various cybercrimes, and aligns closely with the provisions of the Budapest Convention. Both frameworks criminalize:

1. **Illegal Access and Unauthorized Computer Access (Article 2 of Budapest Convention) (Article 277/D of Criminal Code of Kosovo**): Both the Budapest Convention and Kosovo's Penal Code criminalize unauthorized access to computer systems. However, Kosovo's code also specifies penalties under conditions where the crime is considered more severe, such as unauthorized access to military or other critical systems.
2. **Illegal Interception and Unlawful Interception of Computer Databases (Article 4 of Budapest Convention) (Article 277/E of Criminal Code of Kosovo):** Both frameworks prohibit the unauthorized interception of non-public transmissions of computer data. Kosovo's legislation imposes penalties for offenses involving critical national infrastructures.
3. **Data Interference and Impeding the Operation of Computer Systems (Article 4 of Budapest Convention) (Article 277/F of Criminal Code of Kosovo):** Similar to the Convention, Kosovo's Penal Code penalizes the intentional damaging, deletion, or alteration of computer data. The severity of punishments escalates when offenses impact national security or critical public systems, echoing the Convention's graded approach based on potential impact unauthorized access, illegal interception, data interference, system interference, and the misuse of devices, highlighting a shared commitment to protecting computer systems and data integrity. Notably, Kosovo's code specifies stricter penalties for offenses involving critical national infrastructures.
4. **System Interference (Article 5 of Budapest Convention) (Article 277/F of Criminal Code of Kosovo)** Both legal frameworks treat the hindrance of computer systems as a criminal offense.
5. **Misuse of Devices (Article 2 of Budapest Convention) (Article 6 of Budapest Convention) (Article 277/G of Criminal Code of Kosovo):** The production and distribution of devices intended for committing cybercrimes are criminalized under both the Convention and Kosovo's laws. Kosovo extends this to include the possession of such devices.

[92] *See for a comparative legal analysis between the Budapest Convention and provisions of Law No. 03/L–166 on Prevention and Fight of the Cyber Crime, available at https://rm.coe.int/octocom-legal-profile-kosovo/16809e5451.*
[93] *See Chapter XXIV/A of Law No.08/L-188 on Amending and Supplementing the Criminal Code No.06/L-04 of the Republic of Kosovo.*

6. **Content-related Offenses (Articles 277/A, 277/B, 277/C of Criminal Code of Kosovo):** Kosovo's Penal Code expands the scope of the Budapest Convention by addressing the dissemination of content that promotes genocide, crimes against humanity, racism, and xenophobia through digital platforms.
7. **Computer-related Forgery and Fraud (Article 7 of Budapest Convention) (Articles 277/J, 277/K of Criminal Code of Kosovo):** Both the Convention and Kosovo's legislation address the manipulation of computer data for fraudulent purposes, with Kosovo's law specifying penalties and considering attempts to commit these offenses as crime.
8. **Materials Containing Sexual Exploitation and Abuse of Children (Article 8 of Budapest Convention) (Article 277/I of Criminal Code of Kosovo):** Kosovo's laws align with the Convention's stance against child pornography by imposing severe penalties for the production, distribution, and possession of such materials, demonstrating a robust stance against child exploitation.

Thus, it could be said that the majority of the crimes in cyberspace are adequately covered in the Penal Code of Kosovo, and the same is in good conformity with the Budapest Convention. Further, the legislation in Kosovo provides an extra step further from the Convention in that it makes explicit reference to materials intended to promote genocide, crimes against humanity, racism, and xenophobia disseminated through systems.

Nonetheless, it is important to note the protection that it is offered with phrasing used with regards to unauthorized computer access. Specifically, Article 277/D paragraph 2 and 4, regulates that:

> "2. Whoever, in an unauthorized manner and with the intention to unlawfully gain material benefit, for himself or another person or to cause damage to another person, changes, publishes, deletes, disposes or destroys data or computer programs or in any other way enters to a computer system of another, shall be punished by fine or imprisonment from one (1) to three (3) years.
>
> […]
>
> 4. For the purpose of this Article, Unauthorized Access shall be considered:
>
> 4.1. actions of a person who is not authorized under the law or the contract;
> 4.2. actions of a person that exceeds the limits of authorization;
> 4.3. actions for which there is no permission from the competent and qualified person, according to the law, to use, administer or control the computer system or to conduct scientific research in a computer system.

In the current legal framework, especially concerning whistleblowers and the media, the phrasing of the article offers an additional safeguard against prosecution for what might be interpreted as 'unauthorized access.' This protection arises because, while whistleblowers' actions might be seen

as damaging by publishing someone's data, they can assert that they are legally authorized to disclose this information under Law No. 06/L-085 on Protection of Whistleblowers. Therefore, their actions would not fall under the category of 'unauthorized access,' providing them a defense against potential legal challenges. This nuance in the law ensures that whistleblowers and journalists can operate without fear of prosecution when engaging in acts of public interest disclosure.

Nevertheless, analyzing the changes to the Criminal to the Criminal Procedure Code through Law No. 08/L-187, article 98B, a legal ambiguity is noticed which could be worrisome, which provides that:

> "1. The internet service providers shall, upon the application of the investigative body for the collection of data on the subscriber, be obliged to provide the data on IP address user in accordance with the respective legislation on electronic communications.
>
> 2. The collection of data on the subscriber, including personal data and physical address, shall be allowed only for the purpose of investigation or when it is necessary to determine the whereabouts of the suspect."

This provision raises several significant concerns, particularly regarding privacy and data protection as guaranteed by article 36 of the Kosovo Constitution. First, the requirement for internet service providers to disclose subscriber data, including personal information such as IP addresses, in accordance with the respective legislation on electronic communications. Article 104 of Law No. 04/L-109 on Electronic Communications among others provides that "Pre-trial investigation institutions designated by the Government shall provide their subdivisions and/or other pre-trial investigation institutions with access to such information in accordance with the procedure established by the Government." As such it is seen that Law on Electronic Communications is not carefully regulated and it is legally ambiguous in a way that allows the Government to regulate this issue and not the Assembly through Law, and this could result in unwarranted surveillance or misuse of personal data, undermining individuals right to privacy in the digital space.

Another potential issue with article 98B of the Criminal Procedure Code lies in the broad scope of data collection. The provision permits the collection of personal data and physical addresses when it is deemed necessary for "the purpose of investigation" or when it "necessary" to locate a suspect. However, the terms "the purpose of investigation" and./or "necessary" could be interpreted too loosely, allowing for investigative overreach in cases where the threshold for such collection is unclear or poorly defined. Moreover, the absence of judicial oversight is worrisome. There is no mention of requiring a court order or legal approval before Internet Service Providers can release sensitive subscriber information, which opens the door for potential abuse of power by investigative authorities. Without proper checks and balances, there is a risk that these powers could be misused. Ultimately this could create concern for the right to freedom of expression. If

individuals fear that their online activity could be monitored or tracked, they may be less likely to engage in open discourse, which could infringe upon their freedom of speech and expression. However, these issues seem that will be soon delt with, as in 2024 legislative agenda is foreseen the adoption of the Draft Law on the Protection of Personal Data by Law Enforcement Institutions which will stipulate how law enforcement institutions must handle personal data.[94] Special emphasis should be placed on ensuring that data processing by law enforcement respects the principles of necessity, proportionality, and lawfulness. Through this Law enforcement bodies will need to balance their duty to investigate crimes with their obligation to protect the privacy of individuals, ensuring that personal data is only accessed and processed when absolutely required for public safety and justice.

Lastly, the new Cybersecurity Law establishes a Cyber Incident Registry maintained by Agency for Cybersecurity.[95] This registry is a database for recording cyber incidents with the goal of documenting, analyzing, and resolving such incidents, sending alerts, and conducting surveillance operations. This mechanism mirrors the existing but underutilized online platform provided by KOS-CERT, which allows for the reporting of cyber incidents affecting both private and public entities, as well as citizens.[96] Due to a lack of public awareness, victims often report cybercrimes to the Kosovo Police, which then directs cases to its Investigation Department. [97]

Thus, given the underutilization of the KOS-CERT platform and the establishment of the Cyber Incident Registry, it is crucial to enhance public awareness and understanding of these resources. A robust public awareness campaign is recommended to educate both private and public entities, as well as individual citizens, about the existence and importance of these platforms. This effort should include clear information on how to report incidents, the benefits of timely reporting for security and response, and assurances about the confidentiality and security of the information provided.

Recommendations

- It is recommended that Article 98B of the Criminal Procedure Code be amended to enhance legal clarity and security by eliminating ambiguities. The amendment should clearly define the procedures and requirements for obligating the disclosure of IP address data.
- Additionally, clear criteria for data collection should be established through strict guidelines, outlining the specific conditions under which such data can be collected and include obligations with regards to specify the category of data that is necessary for conducting the investigation.

---

[94] *Government of Kosovo, 'Legislative Agenda for 2024' (Government of Kosovo, 2024), available at https://kryeministri.rks-gov.net/wp-content/uploads/2024/02/Programi-Legjislativ-per-vitin-2024-.pdf.*
[95] *See article 10 of the Law, See also Administrative Instruction (MIA) No. 04/2024 for the Registry of Cyber Incidents.*
[96] *Western Balkans Cybersecurity Research Network, Cybersecurity and Human Rights in the Western Balkans: Mapping Governance and Actors, ch 3, 'Kosovo: Strengthening New Foundations and Institutions' by Lulzim Peci and Valdrin Ukshini (Kosovar Institute for Research and Development (KIPRED)), 59 available at https://www.kipred.org/repository/docs/CybersecurityHumanRightsWesternBalkans_EN_March2023_469629.pdf.*
[97] *Ibid.*

- Specify that such requests require a court order or warrant before Internet Service Providers are allowed to disclose subscriber data.
- Ensure that even in the cases where a court order exists, law enforcement officers are required to obtain an extension of a court order from the appropriate judicial authority before conducting searches and seizures that extend beyond the scope of the original court order.
- Implement a comprehensive public awareness campaign to inform both private and public entities, as well as citizens, about the existence and functions of the Cyber Incident Registry. This campaign should detail the process for reporting cyber incidents, emphasize the benefits of timely reporting, and provide assurances about the confidentiality and security of the information shared.
- Develop educational programs that include workshops, seminars, and online tutorials aimed at educating potential users on the significance of the registry and how it can aid in the swift resolution of cyber incidents.
- Implement a responsible disclosure framework, allowing security vulnerabilities to be reported privately and providing sufficient time for organizations to address the issues before public disclosure. This framework should also include a reward system (monetary or recognition-based) to encourage responsible reporting from security researchers and experts.
- Invest in technology and human resources to enhance the operational capabilities of institutions involved in cyber incident management, ensuring they can handle the complexities and demands of modern cybersecurity challenges.

4.4 Data protection and the right to privacy

The right to privacy is both guaranteed and protected by international human rights laws, as well as by Constitution of Kosovo.[98] Article 36 of the Kosovo Constitution enshrines the right to privacy, emphasizing the "secrecy of correspondence, telephony, and other communications". It stipulates that these rights can only be temporarily restricted by a judicial decision if necessary for the progress of criminal proceedings or national defense, as specified by law. Additionally, the article guarantees the right to data protection, regulating the collection, storage, access, correction, and use of personal data through law.

Although Kosovo has enshrined the protection of personal data within its constitutional framework, the requirement to align its existing data protection legislation with that of the EU has facilitated the adoption of a comprehensive data protection law in line with the General Data Protection Regulation.[99] This alignment was driven by the stipulations of the Stabilization and Association Agreement with the EU, which set the approximation of EU legislation as a precondition for further integration processes.[100]

[98] *See article 36 of Constitution of Kosovo, See Article 12 of UDHR and Article 17 (1) ICCPR, See Article 8 of the ECHR*
[99] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*
[100] *See Article 74 paragraph 1 of the Stabilization and Association Agreement between Kosovo and the European Union.*

According to Law No. 06/L-082 on Protection of Personal Data ("Law on Protection of Personal Data"), the definition of "personal data" under the applicable data protection legislation mirrors the comprehensive scope found in international standards. Specifically, "personal data" is defined as any information that relates to an identified or identifiable natural person.[101] This can be through direct or indirect means, particularly by reference to an identifier such as a name, an identification number, location data, and an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Processing of personal data is defined as any operation or set of operations performed to personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[102] Article 6 of Law on Protection of Personal Data provides circumstances under which personal data processing is considered lawful. These include instances where the data subject provides explicit consent to the processing; if processing is necessary for the performance of a contract to which the data; where processing is necessary for compliance with a legal obligation to which the data controller is subject; if processing is necessary in order to protect the vital interests of the data subject or of another natural person; if processing is intended to protect the legitimate interests of the data subject; or for the proper execution of a public law duty by a public body.

Additionally, the law establishes vital principles for the processing of personal data. These include the principles of lawfulness, fairness, and transparency, ensuring that data is handled in a legal, impartial, and clear manner without compromising the dignity of data subjects.[103] It requires that personal data must be collected for specific, clearly defined, and legitimate purposes and should not be used for any other purposes that are incompatible with the original intent.[104] The law also mandates that personal data may only be processed if it is adequate, relevant, and not excessive in relation to its intended purpose,[105] and that the data should be kept up to date, with inaccuracies promptly corrected.[106] Another important principle is that the data should only be stored insofar as necessary to achieve the purpose for which are further collected or processed.[107] Furthermore, the law places a responsibility on data controllers to ensure the security of personal information, protecting it against unauthorized access, loss, or damage, and preserving its accuracy and integrity throughout its handling.[108]

---

[101] *Article 3, paragraph 1, subparagraph 1.1 of Law No. 06/L-082 on Protection of Personal Data.*
[102] *Article 3, paragraph 1, subparagraph 1.2 of Law No. 06/L-082 on Protection of Personal Data.*
[103] *Principle of lawfulness, justice and transparency Article 4, paragraph 1, subparagraph 1.1 of Law No. 06/L-082 on Protection of Personal Data.*
[104] *Principle of purpose limitation, Article 4, paragraph 1, subparagraph 1.2 of Law No. 06/L-082 on Protection of Personal Data.*
[105] *Principle of data minimization, Article 4, paragraph 1, subparagraph 1.3 of Law No. 06/L-082 on Protection of Personal Data.*
[106] *Principle of accuracy, Article 4, paragraph 1, subparagraph 1.4 of Law No. 06/L-082 on Protection of Personal Data.*
[107] *Principle of storage limitation, Article 4, paragraph 1, subparagraph 1.5 of Law No. 06/L-082 on Protection of Personal Data.*
[108] *Principle of integrity and confidentiality, Article 4, paragraph 1, subparagraph 1.6 of Law No. 06/L-082 on Protection of Personal Data.*

Consent plays a key role in the lawful processing of personal data. The law requires that the data subject's consent be freely given, informed, specific, and unambiguous, and it must be obtained through a clear affirmative action, such as a written or verbal agreement, which can be withdrawn at any time by the data subject.[109] Importantly, when consent is part of a broader written declaration, it must be presented in a clear and distinguishable manner from other matters. This ensures that the individual is fully aware of what they are consenting to.

The law imposes stricter conditions for the processing of personal data relating to children, who are deemed particularly vulnerable. Data processing involving children under the age of 16 requires the explicit consent of a parent or guardian and the data controller must make reasonable efforts to verify that the consent is provided by a person with parental responsibility.[110] The law recognizes that children may not fully understand the implications of their consent, hence the need for additional protection. In cases involving children between 14 and 16 years old, the law requires extra verification measures to ensure that parental consent has been obtained, taking into consideration available technology.

It is very important to note that the law provides robust rights for data subjects, empowering individuals to control how their personal data is processed.[111] Data subjects have the right to access their personal data,[112] request rectification of inaccurate data,[113] or demand the erasure of data that is no longer needed (the right to be forgotten)[114]. They can also restrict[115] or object to the processing of their personal data[116] and request the portability of their data[117]. In cases of automated decision-making, including profiling, individuals have the right not to be subject to decisions made solely based on automated processing that significantly affect them.[118] These rights are fundamental to ensuring transparency and fairness in personal data processing. So far, regarding the right to rectification, there have been no recorded requests for data correction.[119] As for the right to be forgotten, it is often invoked in cases where individuals request the deletion of defamatory news articles by media platforms.[120] While with regards to foreign data controllers outside Kosovo, so far there has not been a complaint with regards to the right to be forgotten or

[109] *Article 6 of Law No. 06/L-082 on Protection of Personal Data.*
[110] *Article 7 of Law No. 06/L-082 on Protection of Personal Data*
[111] *Article 14 of Law No. 06/L-082 on Protection of Personal Data, which outlines the Right of Access by the Data Subject, allowing individuals to control how their personal data is processed.*
[112] *Ibid, where it is explicitly provided the right for individuals to request access to personal data that is being processed.*
[113] *Article 15 of Law No. 06/L-082 on Protection of Personal Data, outlines the Right to Rectification, allowing data subjects to correct inaccurate or incomplete personal data.*
[114] *Article 16 of Law No. 06/L-082 on Protection of Personal Data, defines the Right to Erasure (also known as the right to be forgotten), enabling individuals to request the deletion of personal data when it is no longer necessary or when consent has been withdrawn.*
[115] *Article 17 of Law No. 06/L-082 on Protection of Personal Data*
[116] *Article 20 of Law No. 06/L-082 on Protection of Personal Data*
[117] *Article 19 of Law No. 06/L-082 on Protection of Personal Data, allows individuals to request their personal data in a structured, machine-readable format, and transmit it to another controller.*
[118] *Article 21 of Law No. 06/L-082 on Protection of Personal Data, which addresses Automated Individual Decision-Making, including Profiling, ensuring that individuals are not subject to decisions solely based on automated processing that have significant effects on them.*
[119] *Interview with IPA officials.*
[120] *ibid.*

the right to rectify personal data.[121]Additionally, Article 27 sets out the obligations of data processors when handling personal data on behalf of a controller. It mandates that controllers engage only processors who provide sufficient guarantees for data protection and specifies that a binding contract must govern the relationship. This contract must outline the scope, purpose, and nature of the processing, ensuring the processor acts solely under the controller's instructions. Sub-processors can only be engaged with the controller's prior authorization, and the same data protection obligations must be imposed on them. Processors are required to implement appropriate security measures, assist controllers in fulfilling their legal duties, and allow for audits. If the processor determines the purposes of processing, they are considered liable as a controller.

The law also provides that the Information and Privacy Agency ("IPA") may lay down Standard Contractual Clauses ("SCCs") for the matters referred above.[122] In that aspect, SCCs are pre-approved legal agreements that provide a mechanism for ensuring adequate protection of personal data during its transfer between controllers and processors. These clauses set clear terms and obligations for the parties involved to comply with data protection standards, making it easier to ensure legal conformity without having to negotiate individual contracts. However, a shortcoming arises from the fact that the Agency has not yet published these SCCs. Therefore, this delay poses a significant challenge, as it leaves data controllers and processors without a clear, generally accepted template for legally compliant data transfers and processing. Publishing SCCs would provide legal clarity, reduce the administrative burden for organizations, and ensure a consistent standard of data protection in contracts. It would also enhance international data transfers by providing businesses with an officially recognized and legally sound framework, on which to be assured in cross-border data flows, but without lowering the standards of protection for data privacy.

The Law establishes the IPA, tasked with a broad mandate including promoting education and public awareness of information protection principles, monitoring and enforcing compliance with the law's provisions, and monitoring technological advancements to minimize adverse effects on personal data. If a data subject believes their personal data has been mishandled or unlawfully processed, they can lodge a complaint with the IPA.[123] The IPA is required to investigate the complaint and assess whether there has been a violation of data protection laws.[124] The data subject also has the right to be informed about the outcome of the investigation and any corrective measures taken by the Agency.[125] Additionally, IPA can carry out audits, conduct inspections, and request information from organizations to assess their compliance with data protection regulations.[126] If the IPA finds that an organization has violated the law, it has the authority to impose corrective measures, such as ordering the cessation of unlawful data processing or requiring the implementation of proper security measures.[127] Additionally, the IPA can issue

[121] *ibid.*
[122] *Article 27, paragraph 7 of Law No. 06/L-082 on Protection of Personal Data*
[123] *Article 14, paragraph 1, subparagraph 1.6 and Article 52 of Law No. 06/L-082 on Protection of Personal Data*
[124] *Article 65 of Law No. 06/L-082 on Protection of Personal Data*
[125] *Article 52 of Law No. 06/L-082 on Protection of Personal Data*
[126] *Article 68 of Law No. 06/L-082 on Protection of Personal Data*
[127] *Article 71 of Law No. 06/L-082 on Protection of Personal Data*

administrative fines for breaches of data protection obligations.[128] These fines can vary in severity depending on the nature and seriousness of the violation however the fines generally vary from twenty thousand to forty thousand euro. Despite this broad mandate, IPA faces certain constraints, particularly concerning its limited staffing, and budget, which is especially critical regarding cybersecurity matters. Despite issuing around 200 decisions annually, the agency's workload is substantial considering its small team. This limitation in resources hinders the IPA's ability to fully execute its broad mandate, particularly in addressing the increasing cybersecurity challenges with respect to personal data protection matters.

This is especially important, since generally an issue across public institutions in Kosovo is the lack of awareness regarding the importance of technical and organizational security measures. While many institutions may have policies in place, adherence to these policies is often lacking. One notable exception is the State Agency of Information, which has specific measures and adheres to them rigorously. In contrast, other government institutions, such as ministries, do not consistently follow these measures. To add to that, a recent project initiated by the API aims to create Technical and Security Organizational Measures for municipalities, meaning municipalities will soon have standardized security protocols in place.[129] Despite that, an important aspect to highlight is that the E-Kosova platform has ISO 27001 certification and is fully compliant with its requirements. As an overall overview the banking sector in Kosovo is considered the most advanced in terms of data privacy.

In terms of enforcement, fines are typically issued only in cases where harm to the public is significant and where the consequences have already occurred, such as the publication of personal data.[130] On average, 2-3 fines are issued per year with regards to breach of personal data protection legislation.[131] For example, the Ministry of Education was fined after personal data of applicants for book subsidies were published, with educational directories sharing the information with teachers and students through platforms like Viber. Municipality of Gjakova was fined because it published lists with the data of sensitive personal data of subjects, which contained data such as: first name, last name, year of birth, personal number, disease diagnosis, bank account number, the phone number of natural persons who have benefited from health subsidies for the year 2024, as well as the benefited amount. Additionally, with regards to private institutions, for example in 2022 an insurance company was fined for violations related to personal data security. This penalty was split into two parts: a 30,000-euro fine for specific security violations and a 20,000-euro fine for general breaches of the Law on Personal Data Protection. The insurance company was found to have entrusted personal data processing to a third party without a written contract. Additionally, the company was ordered to temporarily halt the online sale of products until necessary measures to protect personal data were implemented. The violation was identified after a customer's personal data appeared on search engines following an online purchase. Despite initial removal efforts, the

[128] *Article 91 of Law No. 06/L-082 on Protection of Personal Data*
[129] *Interview with IPA officials.*
[130] *Ibid.*
[131] *Ibid.*

data was still accessible, prompting an inspection by IPA. The company admitted to the data breach and cooperated with authorities to resolve the issue.

Overall, IPA in light of the recent adoption of Kosovo's data protection law and the general lack of public awareness, has been proactive in increasing public education on data protection rights. A quick glance at their website reveals a variety of published resources aimed at informing and guiding the public. These include the Guide on Personal Data Protection, Advices on Personal Data Protection), Status of Personal Data Protection Decisions on Personal Data Protection Complaints. Yet it would be advisable to provide an extensive range of resources, including detailed guides on data protection compliance for businesses, organizations, and individuals. Additionally, the IPA should provide downloadable templates for businesses and organizations in Kosovo, such as data protection impact assessments, data breach notification forms, and privacy notice templates.

Moreover, to ensure that legal requirements are more easily understood, to ensure that legal requirements are more easily understood, IPA should develop an interactive checklist that details each step of data protection compliance. This tool would provide data controllers and processors in Kosovo with a clear, actionable guide to help them navigate the complexities of the law. Such interactive checklists and guides would streamline compliance efforts, making it easier for businesses to meet their legal obligations while reducing the risk of errors and enhancing overall data protection practices. An interesting example of such an interactive checklist could be found at https://gdpr.eu/checklist/.

Recommendations

The following recommendations are proposed to enhance privacy protection and align regulatory frameworks with international standards:

- The IPA should prioritize the development and publication of SCCs to provide organizations with a clear, standardized framework for legally compliant data transfers.
- Provide downloadable templates for key data protection tasks, such as Data Protection Impact Assessments, data breach notification forms, and privacy notice templates, to assist organizations in adhering to the law.
- Develop an interactive checklist to guide data controllers and processors through each step of compliance, ensuring that legal requirements are easily understood and followed.

Chapter 5 - Freedom of Expression Online and Access to Information

Digital rights are expressed through a wide range of media platforms, such as television, radio, print, and digital outlets such as websites, mobile applications, and social media networks. This section examines the impact of these media channels on the realization of digital rights, including the challenges and limitations that can impede their full expression and protection.

5.1 The concept of Media in the context of Digital Rights in Kosovo

The media holds a crucial responsibility to both inform and educate the public. Its role goes beyond simply sharing information; it also involves oversight, particularly of those in positions of power within the government, public institutions, or the private sector. By closely monitoring and reporting on their actions, the media acts as an essential watchdog, uncovering issues that have both direct and indirect effects on the public. In promoting accountability, fairness, and transparency, the media supports good governance and democracy, helping to create a more informed and engaged society.

Article 42 of the Constitution of Kosovo provides that the freedom and pluralism of media is guaranteed. Media, in today's context, encompasses a wide array of communication platforms and tools that facilitate the dissemination of information to the public. Traditionally, media referred to channels like print (newspapers and magazines), radio, and television. However, with the advancement of technology, the definition of media has evolved to include digital platforms such as websites, social media, mobile applications, and other forms of digital communication. However, the legislation of Kosovo does not define what media is. However, this could be understood from the context of ICCPR, particularly Article 19, that the phrase "through all kinds of media" has a broad and dynamic interpretation. As such courts at national, regional, and international levels have increasingly acknowledged the broadening of media to include not only traditional forms, such as print and broadcast, but also modern digital platforms like the Internet, mobile applications, and other communication technologies.[132]

For example, in the case *Times Newspaper Ltd v. the United Kingdom*, the ECtHR dealt with the role of online media in disseminating information. The case involved two news articles published in both print and digital formats concerning a Russian mafia boss allegedly involved in money laundering. The ECtHR recognized the potential of online news archives to enhance public access to information and contribute to the dissemination of news. The Court highlighted the importance of Internet archives, considering them a valuable source for education and historical research, readily accessible and often free of charge. It accorded the same level of protection to online press

[132] *Lee Ahreum, International Human Rights Law in Digital Space: An Examination of the Need for New Legal Measures for the Protection of Rights Online (PhD thesis, Graduate Institute of International and Development Studies 2020), 174, available at: https://repository.graduateinstitute.ch/record/298081?ln=en&v=pdf.*

publications as it does to traditional print media, thereby expanding the scope of media protection in the digital era.

Similarly, in *Magyar Kétfarkú Kutya Párt v. Hungary*, the ECtHR further broadened the concept of media by including mobile phone applications. This case involved an app developed for voters to comment on and share anonymous photos of invalid ballots during a referendum on EU migrant relocation plans. The Court found that the app had communicative value, as it was specifically designed to enable voters to share their opinions using digital tools. By acknowledging this, the Court extended the definition of media to mobile applications, affirming that digital tools, like apps, fall within the scope of protected media.

The dynamic interpretation of media builds on these cases, recognizing that media should not be limited to traditional outlets like newspapers and television. The phrase "through all kinds of media," as used in Article 19 of the ICCPR, is understood in light of present-day technological realities, incorporating broadcasting programs, cable retransmission, the Internet, mobile apps, and even social media platforms. Under this evolving understanding, any new communication process is automatically protected under the freedom to receive and share information, reinforcing the principles of freedom of expression. Therefore, the term "media" must be interpreted broadly to encompass innovative technological developments, ensuring that rights related to the freedom of expression adapt to the modern digital landscape.

In advancing media freedom, Kosovo has adopted legislation and other regulatory instruments that guarantee fundamental rights that correspond to the use of media. Firstly, article 40 of the Constitution provides that every person is entitled to freedom of expression, to disseminate and receive, information, opinion and other messages without impediment. Article 38 enshrines the freedom of conscience, including the right to express personal beliefs. This provision empowers journalists to fearlessly engage with critical public issues, fortified by the assurance of protection from undue interference. Thirdly, Article 36 paragraph 2 as a derivative of the right to privacy and Article 46 paragraph 3 of the Constitution as a derivative of the right to property, guarantee freedom from arbitrary search and entry, shielding journalists' materials such as notebooks and digital storage devices from unwarranted intrusion. This safeguard extends to safeguarding the confidentiality of journalists' sources and informants, ensuring the integrity of investigative journalism through Article 42 of the Constitution. The Constitution also provides for the right to life, the right to personal freedom, freedom of movement, and freedom from inhuman treatment. 4 Collectively, these legal safeguards serve as pillars underpinning the vitality of Kosovo 's media landscape, both in traditional and digital spheres, creating an environment conducive to robust journalism and public discourse.

Key legislation, such as the Law No. 04/L-137 on the Protection of Journalism Sources, Law No. 02/L-65 Civil Law against Defamation and Insult, Law No. 06/L085 on Protection of Whistleblowers, Law No. 06L-081 on Access to Public Documents, provide essential protections for journalists and media entities. These laws ensure the protection of journalistic sources, offer

recourse for defamation and insult, and grant access to public documents, all while maintaining a balance with the right to freedom of expression. However, significant gaps remain, particularly concerning the regulation of online media.[133]

As a general legal overview of media regulation in Kosovo: media are divided into two main groups: audiovisual media (television and radio) and written media (print and online media). Two main institutions contribute to media regulation: the Independent Media Commission ("IMC") and the Press Council of Kosovo ("PCK"), as a self-regulation body. The IMC is the institution responsible for audiovisual media regulation, starting with their licensing and ensuring that the content they broadcast complies with the law. On the other hand, the press and online media are self-regulated through the PCK a body created by the media industry itself. While audio-visual broadcasters are required to obtain licenses from the IMC, online media entities are not subjected to the same licensing requirements, creating an uneven regulatory landscape.[134]

PCK operates based on a code of ethics that is developed and approved by the editors and editors-in-chief of its member media outlets.[135] This code serves as a guideline for journalists to uphold ethical standards in their work. The PCK addresses complaints related to ethical breaches by the media, including issues such as inaccurate reporting, invasion of privacy, or unauthorized use of content. While the PCK does not have the power to impose sanctions, it issues decisions and requests that its members publish these rulings. Currently, the PCK consists of over 50 members, primarily online media outlets (news portals) since print media is no longer operational in Kosovo.[136] Individuals who believe that an online media outlet has violated the code of ethics can file a complaint with the PCK, which then determines if a violation has occurred and publishes the decision on its website. To date, the PCK has addressed approximately 1,600 complaints.[137]

Finally, while the public now has diverse forms of engagement in the online civic space, this shift has contributed to the decline of traditional media. As readers increasingly turn to the internet for news consumption, newspapers and magazines are fading, and online reporters, particularly bloggers, are gaining influence.[138] This widespread digital engagement has replaced traditional media, as print outlets are no longer operational in Kosovo. Unlike professional journalists, many bloggers lack formal training in journalistic standards, which can lead to the spread of misinformation. They often bypass essential practices like fact-checking or verifying sources, and

---

[133] *NDI, Information Integrity in Kosovo: Assessment of the Political Economy of Disinformation (July 2022), 16 available at: https://www.ndi.org/sites/default/files/Information%20Integrity%20in%20Kosovo%20-%20Assessment%20of%20the%20Political%20Economy%20of%20Disinformation.pdf*

[134] *Ibid.*

[135] *Press Council of Kosovo, Code of Written Media of Kosovo (2013), available at https://agk-ks.org/site/assets/files/2614/press-code-for-kosovo_alb_1.pdf.*

[136] *See Press Council of Kosovo, 'Anëtarët' available at https://presscouncil-ks.org/?page_id=13 .*

[137] *Ibid.*

[138] *See NDI (n133) 8. This phenomenon is also supported Facebook is the most popular platform, with 910,000 users, followed by Instagram at 750,000, while Twitter remains less common with 63,200 users. Especially among youth, 87 percent of are on Facebook and 77 percent on Instagram.*

they don't adhere to the same ethical obligations as traditional media.[139] This trend challenges the stability of conventional media structures and poses a risk to the accuracy and reliability of news, though the regulation of misinformation is addressed in section 5.6 of the report.

5.2 Hate speech

Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech recognizes the powerful role of the internet in enabling the dissemination of hate speech.[140] Internationally, there are many human rights documents that prohibit discrimination, including hate speech as a form of discrimination. In Article 22 of the Constitution of the Republic of Kosovo is contained the obligation for the direct implementation of some international human rights instruments, therefore below are explained the main obligations within those international human rights instruments which apply directly in the Republic of Kosovo.

International Covenant on Civil and Political Rights:

- Article 19 protects freedom of expression but allows limitations to respect others' rights, protect national security, public order, health, or morals.
- Article 20 mandates prohibiting national, racial, or religious hatred that incites discrimination, hostility, or violence.

European Convention on Human Rights:

- Article 10 guarantees freedom of expression but allows restrictions to protect national security, public safety, health, morals, and others' rights.

International Convention on the Elimination of All Forms of Racial Discrimination:

- Article 4 requires states to condemn propaganda and organizations that promote racial superiority or hatred.

Convention on the Elimination of All Forms of Discrimination Against Women:

[139] *Abit Hoxha, Resilience: For Media Free of Hate and Disinformation (SEENPM, Tirana, Peace Institute, Ljubljana and Kosovo 2.0, September 2020) 12, available at: https://seenpm.org/wp-content/uploads/2020/10/Resilience-research-publication-1-KOS-ENG.pdf.*

[140] *Council of Europe, Recommendation CM/Rec(2022)16 of the Committee of Ministers to Member States on Combating Hate Speech (20 May 2022) available at https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680a67955%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}*

- Article 5 mandates the elimination of stereotypes, prejudices, and practices that marginalize or discriminate against women.

The notion of hate speech is not defined in any of the human rights instruments as a legal term.[141] Broadly, The Committee of Ministers of the Council of Europe, in Recommendation R (97) 20, defines hate speech as encompassing "all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, antisemitism, or 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."[142] Given the variety of content and likely effects falling within this definition, the notion of hate speech contains an inextricable link between the right to freedom of expression, the right to equality before the law and the right to non-discrimination. However, determining that line of when freedom of expression crosses over into hate speech is a legal challenge in itself. This is particularly an important issue in the online world, where the speed and scale at which content spreads make it easier to express opinions and views freely, however, the internet can also amplify the harmful effects of hate speech, leading to greater hostility, division, and violence in society.[143]

In this particular context, Recommendation CM/Rec (2022)16 outlines that hate speech encompasses a spectrum of harmful expressions, which vary in severity, the damage they inflict, and their impact on targeted groups in different settings.[144] Thus, hate speech can be categorized as follows:

i. hate speech that is prohibited under criminal law; and
ii. hate speech that is subject to civil or administrative law, which refers to expressions, though not severe enough for criminal liability, still promote discrimination or intolerance and are dealt with under civil or administrative law.
iii. offensive or harmful types of expression, which although not serious enough to be legally restricted, these types of speech call for non-legal responses, such as counter-speech, intercultural dialogue, and educational or awareness-raising initiatives, including through media and social media platforms.

---

[141] *Talita Dias, Tackling Online Hate Speech through Content Moderation: The Legal Framework under the International Covenant on Civil and Political Rights (BSG Working Paper Series, Forthcoming in Bahador, Hammer and Livingston (eds), Countering Online Hate and its Offline Consequences in Conflict-Fragile Settings, 2022) 6, available at https://www.elac.ox.ac.uk/wp-content/uploads/2022/07/Dias-Tackling-Online-Hate-Speech-through-Content-Moderation-Working-paper-1.pdf.*

[142] *Council of Europe, Recommendation No. R (97) 20 of the Committee of Ministers to Member States on Hate Speech (30 October 1997), available at: https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680505d5b%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}*

[143] *Dias (n141).*

[144] *Council of Europe, Recommendation CM/Rec(2022)16 of the Committee of Ministers to Member States on Combating Hate Speech (20 May 2022) available at: https://www.coe.int/fr/web/cyberviolence/-/council-of-europe-recommendation-cm-rec-2022-16-1-of-the-committee-of-ministers-to-member-states-on-combating-hate-speech.*

In that regard, in assessing the severity of hate speech and determining which type of category of hate speech and which type of liability, if any, should be attributed to any specific expression, the authorities should, take into account the following factors and the interplay between them: the content of the expression; the political and social context at the time of the expression; the intent of the speaker; the speaker's role and status in society; how the expression is disseminated or amplified; the capacity of the expression to lead to harmful consequences, including the imminence of such consequences; the nature and size of the audience, and the characteristics of the targeted group.[145]

5.2.1 Legal Framework regarding Hate Speech in Kosovo

5.2.1.1 Constitution of Kosovo

Article 40, paragraph 1 of the Constitution states: "Freedom of expression is guaranteed. Freedom of expression includes the right to express, to disseminate, and to receive information, opinions, and other messages without being hindered by anyone." Meanwhile, paragraph 2 of this article emphasizes: "Freedom of expression may be restricted by law in cases when such action is necessary to prevent incitement and provocation of violence and hostility based on racial, national, ethnic, or religious hatred."

At first glance, it may seem that freedom of expression, according to our Constitution, can only be limited when it is necessary to prevent the incitement and provocation of violence and hostility on the grounds of racial, national, ethnic, or religious hatred. However, the restriction of freedom of expression must be read in conjunction with Article 55 of the Constitution, which stipulates that

---

[145] *To gain a better understanding of legislative models, judicial practices, and policies related to the legal concept of hate speech, and to guarantee full respect for freedom of expression, experts from the United Nations have created the Rabat Plan of Action—a concrete guide to distinguish hate speech from low-value expressions and from expressions that are likely to have a higher social impact. See United Nations Human Rights, Office of the High Commisioner, 'Freedom of expression vs incitement to hatred: OHCHR and the Rabat Plan of Action' (2013) available at: https://www.ohchr.org/en/issues/freedomopinion/articles19-20/pages/index.aspx#:~:text=The%20Rabat%20Plan%20of%20Action%20on%20the%20prohibition%20of%20advocacy,Bangkok%20and%20Santiago%20de%20Chile). The Rabat Plan of Action outlines a six-part threshold test to help determine the boundary between objectionable and offensive expression, which is not punishable, and hate speech that is prohibited by law. The six factors are: context, speaker, intent, content and form, extent or magnitude of the speech, and the likelihood that the speech will cause serious social consequences. These factors suggest that the context of the case plays a very significant role in identifying hate speech, which is considered to exist when:*

A. ***Speaker's Conduct****: The speaker addresses an audience, and the expression contains:*
- *Incitement, advocacy, or provocation;*
- *Hatred targeting a protected group based on protected personal characteristics;*
- *Constitutes incitement to discrimination, hostility, or violence.*

B. ***Speaker's Intent****: The speaker must:*
- *Specifically aim to engage in advocating discriminatory hatred;*
- *Intend or be aware of the likelihood that the audience may be incited to discrimination, hostility, or violence;*
- *There must be a real and imminent risk that the audience will be incited to commit an act of discrimination, hostility, or violence as a result of the advocacy of hatred.*

fundamental rights and freedoms may only be limited by law and only to the extent necessary, in an open and democratic society, to fulfill the purpose for which the limitation is permitted.

Consequently, when freedom of expression may infringe upon other rights, the limits of restriction can extend beyond what is provided in Article 40, paragraph 2. For example, Article 24, paragraph 1 of the Constitution states: “No one shall be discriminated against on the basis of race, color, gender, language, religion, political or other opinion, national or social origin, association with any community, property, economic condition, social status, sexual orientation, birth, disability, or any other personal status.” Therefore, protection against discrimination—which includes more protected personal characteristics than paragraph 2 of Article 40—is a legitimate aim on the basis of which freedom of expression can be restricted.

5.2.1.2 The Criminal Code of the Republic of Kosovo

In Chapter XVII, which pertains to Criminal Offenses against Human Rights and Freedoms, the Criminal Code of Kosovo sets forth penalties for violations of guaranteed human rights, including various forms of hate speech.

In this context, Article 141 states:

> "Whoever incites or publicly spreads hatred, discord, and intolerance between national, racial, religious, ethnic groups, or others, or based on sexual orientation, gender identity, and other personal characteristics, in a manner that can disturb public order, shall be punished by a fine or imprisonment of up to five (5) years."[146]

Furthermore, Article 70 specifies that if a criminal offense is an act of hatred, it is considered a special aggravating circumstance for sentencing:

> "If the criminal offense is an act of hatred, which means any criminal offense committed against a person, group of persons, or property, motivated on the basis of race, color, gender, gender identity, language, religion, national or social origin, association with any community, property, economic condition, sexual orientation, birth, disability, or any other personal status, or because of proximity to persons with the aforementioned characteristics, unless any of these characteristics constitute an element of the criminal offense."[147]

From the analysis of these two provisions, it could be deducted that prohibition of hate speech extends to the online environment as well. However, an important distinction should be mentioned, in order to be considered hate speech under criminal law, the Criminal Code stipulates that the incitement or spreading of hatred must be disseminated “publicly” and in a “manner that can

[146] *Article 141, paragraph 1 of Code No. 06/L-07 Criminal Code of the Republic of Kosovo.*
[147] *Ibid, Article 70, paragraph 2, subparagraph 2.12.*

disturb public order", whereas as we will see below, the Law No. 05/L-021 on the Protection Against Discrimination does not make this specification. The latter defines "intent" as an element of the offense, while the Criminal Code does not.

5.2.1.3 Law on Protection Against Discrimination

Law No. 05/L-021 on Protection Against Discrimination is the most significant legislative act concerning hate speech in the Republic of Kosovo. The law establishes a general framework for preventing and combating discrimination and precisely defines the list of protected personal characteristics in article 1. The personal characteristics protected by the law include nationality or association with any community, social or national origin, race, ethnicity, color, birth, origin, sex, gender, gender identity, sexual orientation, language, citizenship, religious belief and conviction, political affiliation, political or other opinions, social or personal status, age, family or marital status, pregnancy, maternity, property status, health condition, disability, genetic heritage, or any other basis, with the aim of implementing the principle of equal treatment.

Article 3 defines the concept of discrimination as any distinction, exclusion, limitation, or preference based on the personal characteristics protected by the law, which have the purpose or effect of nullifying or impairing the recognition, enjoyment, or exercise, on an equal basis with others, of fundamental rights and freedoms recognized by the Constitution and other applicable laws in the Republic of Kosovo.

Article 4, paragraph 1, subparagraph 1.4 directly refers to hate speech:

> "Incitement to discriminate is considered discrimination on the grounds specified in Article 1 of this Law [protected personal characteristics] and includes any promotion of hatred when it is done intentionally."

From this, it can be understood that hate speech is considered a basic and very serious form of discrimination. According to this provision, for an expression to be deemed hate speech, it must be done intentionally, expressed in a context that can incite discrimination, and result in the promotion of hatred. Without fulfilling these prerequisites, a particular expression cannot be considered hate speech.

5.2.1.4 Hate Speech and Media Legislation

Completing the framework of legislation on restricting hate speech particular in the online environment is the regulation provided by the media legislation and self-regulatory bodies. The Law on the Independent Media Commission includes specific clauses that prohibit the dissemination of hate speech through audio-visual media channels, explicitly addressing content

that incites discrimination, hostility, or violence.[148] However as discussed earlier, this law applies only to audio-visual broadcasters and not to online portals, which are self-regulated through the Code of Ethics enforced by the PCK. This code obligates media outlets and journalists, including those operating exclusively on digital platforms, to refrain from inciting criminal acts, violence, hatred, or inequality. It mandates responsible reporting without biased treatment or derogatory expressions based on personal characteristics like ethnicity, religion, gender, or disability. Since online media constitute the major portion of the PCK's membership, the code's provisions are directly applicable to the digital sphere. However, a significant shortcoming—further explored in the subchapter on content moderation—is that the decisions of the PCK regarding media portals on digital platforms are not legally binding. This means that media portals have only an ethical obligation to follow the PCK's decisions and are not legally required to remove content from their publications.

5.3 Defamation

According to Law No. 02/L-65 Civil Law against Defamation and Insult, defamation is defined as "the publication of an untrue fact or statement and the publisher knows or should know that the fact or the statement is untrue, the meaning of which injures the reputation of another person".[149]

According to paragraph 47 of the 2011 CCPR General Comment No. 34 to ICCPR, "States parties should consider the decriminalization of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty."[150]In that aspect Kosovo legislation is more advanced than the legislation of European Union Member States, as only 5 members have decriminalized legislation.[151] The legal framework regulated through Law No. 02/L-65 Civil Law against Defamation and Insult, emphasizes civil remedies over criminal sanctions, aligning with international human rights

---

[148] *Law No. 04/L-044 on the Independent Media Commission includes several legal provisions that indirectly prohibit hate speech. Article 27, paragraph 4 of this law states:*

> *"Commercial audiovisual communications shall not prejudice:*
> *4.1. respect for human dignity;*
> *4.2. discrimination on the basis of gender, race, ethnic origin, nationality, religion or faith, disability, age, and sexual orientation."*

On the other hand, the Regulation on Commercial Audiovisual Communications, as a sub-legal act of this law, in Article 6, subparagraph 1.4.2, states:

"Commercial communications shall not: Degrade or intimidate or incite violence or discrimination against a person or group on the basis of gender, race, ethnic origin, nationality, religion or belief, disability, special needs, age, sexual orientation, social background, or any other circumstance that aims to nullify or impair the recognition, enjoyment, or exercise, on an equal footing, of the rights and freedoms of any person in all areas of public life."
Based on Article 30 of the Law No. 04/L-044 on the Independent Media Commission, penalties for hate speech may include fines, suspension of the program, modification of license conditions, or revocation of the license.

[149] *Article 3, point a) of Law No. 02/L-65 Civil Law against Defamation and Insult*

[150] *United Nations Human Rights Committee, General Comment No. 34: Article 19: Freedoms of Opinion and Expression (102nd session, Geneva, 11-29 July 2011) available at: https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf*

[151] *Center for Media Pluralism and Media Freedom, 'Decriminalisation of Defamation' (Infographic, 2019) available at: https://cmpf.eui.eu/wp-content/uploads/2019/01/decriminalisation-of-defamation_Infographic.pdf.*

standards. In this aspect, it also must be noted that Article 16 of this law provides courts with the authority to issue injunctions against individuals who have committed defamation, compelling them to remove the defamatory content. In the context of the digital environment, this means that if defamatory content is published on a website, social media platform, or any online medium, the affected person can seek a court order compelling the removal of that content.

5.4 Disinformation and Misinformation

Misinformation and disinformation can quickly reach large audiences through the fast-paced nature of social media and other digital platforms, frequently resulting in human rights violations.[152] This issue is further exacerbated by the financial incentives provided to users by social media platforms, encouraging them to post more content and attract a greater number of followers.[153] In Kosovo, the prevalence of misinformation and disinformation is exacerbated by political tensions and external influences, as seen in the significant role that Russian and Chinese state media play in spreading malign narratives. These external actors, particularly Russian media, amplify interethnic discord by drawing false parallels between Kosovo and Crimea, undermining Kosovo's independence and sovereignty.[154]

While there is no legal definition of these concepts, "disinformation" is usually defined as false, inaccurate, or misleading information deliberately created, presented and disseminated, whereas "misinformation" can be defined as false or inaccurate information that is shared unknowingly and is not disseminated with the intention of deceiving the public.[155]

Misinformation and disinformation infringe upon multiple human rights. One key impact is that the flood of false information distorts people's perceptions, preventing them from forming opinions based on facts and undermining their ability to develop independent beliefs.[156] This compromises their freedom of expression, a right protected under Article 40 of the ICCPR. Additionally, false information can endanger the right to health, as outlined in Article 12 of the ICESCR. For instance, conspiracy theories about health policies or vaccines may lead individuals to reject treatments that protect their own health and the health of others, ultimately undermining public health efforts.

---

[152] *Global Partners Digital, 'Digital Disinformation and Human Rights Explained' (01 June 2023) available at: https://www.gp-digital.org/a-human-rights-based-approach-to-disinformation/.*

[153] *Amnesty International, 'A Human Rights Approach to Tackle Disinformation: Submission to the Office of the High Commissioner for Human Rights' (2022) available at https://www.amnesty.org/en/wp-content/uploads/2022/04/IOR4054862022ENGLISH.pdf.*

[154] *National Democratic Institute, 'Information Disorders in Kosovo' (2023) available at https://www.ndi.org/sites/default/files/INFORMATION%20DISORDERS%20IN%20KOSOVO%20-%202023-compressed_0.pdf.*

[155] *Claire Wardle and Hossein Derakshan, Information Disorder: Towards an Interdisciplinary Framework for Research and Policy Making (2017) available at http://tverezo.info/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-desinformation-A4-BAT.pdf. See also M Lesher, H Pawelec and A Desai, 'Disentangling Untruths Online: Creators, Spreaders and How to Stop Them' (2022) Going Digital Toolkit, OECD, Paris available at: https://goingdigital.oecd.org/data/notes/No23_ToolkitNote_UntruthsOnline.pdf.*

[156] *Amnesty International (n153)*

Misinformation and disinformation also undermine the right to free and fair elections as outlined in Article 25 of the ICCPR. Misleading or false information about political parties, candidates, and their campaigns can distort public perceptions and manipulate voters, leading them to make decisions based on inaccuracies. This interference compromises the integrity of elections by undermining voters' ability to make informed choices, violating their right to vote freely and fairly. Additionally, smear campaigns targeting minority groups, such as ethnic communities, violate the right to non-discrimination under the ICCPR.[157] These campaigns can incite hostility, violence, and even attacks against these groups, infringing on their right to life, freedom, and security.[158] For example, throughout 2023, Kosovo experienced significant political and security tensions that were exploited by various actors to spread disinformation, particularly targeting interethnic relations between Kosovo Albanians and Serbs. This not only heightened tensions but also threatened social cohesion in an already fragile political environment.

Despite the challenges, state responses to online misinformation and disinformation have, in some cases, created challenges for digital rights.[159] Governments often introduce policies and regulations aimed at curbing the spread of false information by criminalizing certain acts or restricting specific publications.[160] However, these measures frequently have the unintended consequence of disproportionately silencing critical voices, limiting freedom of opinion, and restricting access to and dissemination of information, particularly for the media and human rights activists. In Kosovo, this challenge is evident with the growing presence of manipulated content and deepfakes, which are used to create false narratives, incite fear, and discredit political figures. The rise of AI-generated content has introduced new obstacles for fact-checkers and public discourse, undermining the integrity of information available online.[161]

Thus, legislation that regulates broad restrictions on freedom of expression that impose blanket bans on sharing information, particularly when based on vague or ambiguous terms like "false news" or "spreading misinformation," conflicts with international human rights law.[162] In this aspect, while Kosovo's legal framework for tackling disinformation and misinformation is in line with human rights standards, there is a severe lack of enforcement which does little to protect society from disinformation.[163]

---

[157] *Article 6 (1) and 26 ICCPR.*
[158] *Articles 6 and 9 ICCPR.*
[159] *Amnesty International (n153).*
[160] *Ibid, 5.*
[161] *National Democratic Institute, 'Information Disorders in Kosovo' (2023) available at https://www.ndi.org/sites/default/files/INFORMATION%20DISORDERS%20IN%20KOSOVO%20-%202023-compressed_0.pdf.*
[162] *7 Joint Declaration on freedom of expression and "fake news", disinformation and propaganda. UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, Special Rapporteur on Freedom of Expression of the InterAmerican Commission on Human Rights, and the Special Rapporteur on Freedom of Expression and Access to Information of the African Commission on Human and Peoples' Rights (2017), para. 2.a; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 23 April 2020, UN Doc. A/HRC/44/49, para. 49*
[163] *Kreshnik Gashi, Visar Prebreza, Dren Gërguri, and Albulena Sadiku, The Story of Our Lies (BIRN Kosovo, 2023) 83, available at: https://kallxo.com/wp-content/uploads/2023/11/THE-STORY-OF-OUR-LIES-FINALE.pdf..*

The legal framework regulating the protection against disinformation in audiovisual media is governed by the Law on the Independent Media Commission. This law requires audiovisual media to verify the accuracy of their information and prohibits the dissemination of false information. Failure to comply with these obligations may result in fines or even the revocation of broadcasting licenses. In contrast, online media outlets are expected to adhere to the Code of Ethics for Written Media, although this is a voluntary framework and lacks the binding legal force necessary to ensure compliance.

Nevertheless, social media platforms and websites that specialize in disseminating fictitious news remain key sources of disinformation.[164] This makes Kosovo a fertile ground for disinformation, especially in the absence of effective mechanisms to combat it. Currently, there are inadequate structures in place to address the growing threat of disinformation in the country.

It must be noted that the new draft Law on the Independent Media Commission, foresees the development of a by-law on 'prohibition of disinformation, specifically under Article 41, paragraph 5 specifies that: "IMC drafts regulations for the prohibition of disinformation. The regulation includes European Union standards and international norms against disinformation".

However, as noted by an independent legal review commissioned by the Council of Europe, this type of regulation raises significant concerns.[165] While aligning with EU standards and international norms is a positive aspect, the broad and vague concept of "prohibition of disinformation" lacks clarity and poses a potential threat to freedom of expression. Without a precise definition of disinformation, such regulation could lead to unintended consequences, including the risk of censorship or limiting legitimate public discourse.

Therefore, instead of regulating restriction to information, to effectively combating disinformation and misinformation requires a multi-stakeholder approach, where individuals, companies, and governments work together to identify and remove false content from the internet. All parties must take responsibility, exercising caution and critical thinking before sharing information online, to ensure the spread of accurate and reliable content.

To this end, to fight disinformation and misinformation it is recommended that:

- Awareness campaigns should be regularly performed about false information online by promoting digital media literacy within the education system. Given that Kosovo's students scored poorly on the Programme for International Student Assessment test, indicating a lack of critical thinking skills, it is essential that the government drafts a comprehensive strategy to integrate media education in schools.

[164] *Ibid*

[165] *Deirdre Kevin, Review of the Draft Law for the Independent Media Commission of Kosovo (Council of Europe, LEX/FoE (2024)11, 21 June 2024) 17, available at: https://rm.coe.int/review-of-the-draft-law-for-the-independent-media-commission-of-kosovo/1680b13315.*

- Provide specialized media literacy programs for public officials to identify and address disinformation: Many public officials lack the skills to detect and combat disinformation. By providing targeted training on media literacy, public officials can better understand how to recognize false information and how to counter it effectively in their communication.
- Kosovo should prioritize the adoption of a comprehensive media literacy strategy, outlining a clear and actionable framework for its implementation. This strategy should incorporate media literacy programs across all educational levels, including primary schools, high schools, and universities. Additionally, the strategy should promote partnerships with civil society organizations and media professionals to provide workshops and training for educators, ensuring they are well-prepared to teach media literacy in the evolving digital landscape.
- Media outlets should enhance their editorial policies and establish more rigorous editing processes to ensure that the content they publish does not contribute to the spread of disinformation. This involves implementing stricter fact-checking protocols at every stage of content production, from the initial gathering of information to the final review before publication. Editorial teams should be trained to identify potential sources of misinformation and be equipped with tools and methodologies to verify the authenticity and accuracy of their sources.
- Additionally, media organizations should establish clear guidelines for addressing and retracting inaccurate reports or disinformation that may have been unintentionally published.
- Kosovo's media organizations should enhance their internal fact-checking capabilities and improve their ability to investigate and identify sources of disinformation.

5.5 Online Content Moderation

Online Content Moderation refers to the process of reviewing and moderating content that users post online to ensure it adheres to established policies and guidelines.[166] This process may include the removal of content deemed offensive or illegal, or reducing the visibility of certain content in online spaces.[167]

In Kosovo there is no specific law that explicitly regulates the blocking and/or filtering of illegal Internet content. However, the provisions of several general laws have the effect of regulating illegal Internet content. The regulations at the level of secondary laws specifically contain provisions for blocking and/or filtering of illegal Internet content, in particular for the protection of children and young people. Self-regulation, as explained in the previous chapters also plays an important role in this field.

[166] *Besedo, 'What is content moderation?' (Blog, 2023) available at https://besedo.com/knowledge-hub/blog/what-is-content-moderation/.*
[167] *ibid.*

Law No. 04/L-109 on Electronic Communications does not apply to the content of services provided through electronic communications networks but it recognizes the right of ARKEP as the regulatory body to supervise the regulatory framework defined by this law in the field of electronic communications. Thus, when an entrepreneur wants to offer network and electronic communication services in Kosovo, in accordance with the requirements of this law, it is obliged to fulfill the general terms and conditions for engaging in electronic communications activities.[168] ARKEP has the mandate to adopt provisions of sub-legal acts which among others regulate "restrictions in content transmission, in case it violates the legal framework", however to this date ARKEP has not enacted such sub law. Nevertheless, according to ARKEP officials this provision does not provide the means to oblige online platforms to remove content, rather it provides an obligation towards network and electronic communication service providers to comply with the regulatory requirements when transmitting or restricting certain content, ensuring that they do not facilitate the distribution of illegal content.[169] This means that while ARKEP can regulate the activities of local service providers in terms of compliance with the legal framework, it lacks the authority to directly enforce content removal or restrictions on international online platforms, such as social media networks or global websites, which are not registered or operating under Kosovo's jurisdiction. Therefore, the existing legislative framework does not provide sufficient mechanisms to compel these platforms to take down illegal or harmful content, leaving a significant gap in effective content moderation and enforcement.

Similarly, the Criminal Code contains a number of provisions that penalize criminal offences performed through the Internet; however it does not provide legal regulations to the blocking or filtering of illegal Internet content.

The Administrative Instruction (QRK) No. 04/2022 on Measures for the Protection of Children Against Websites with Pornographic Content and Those that Harm the Health and Life of the Child is the only legal provision in Kosovo legislation that directly addresses content moderation. This act establishes guidelines for content moderation specifically aimed at protecting children online. It sets measures to block and restrict access to inappropriate or harmful content such as pornography, violence, and exploitation. The instruction involves the use of filters, parental control programs, and other preventive actions to safeguard children from exposure to harmful material.

Nevertheless, the measures that are foreseen to be applied through this administrative instruction are not implemented. As an example, article 10 paragraph 2 foresees that the Ministry of Industry, Entrepreneurship and Trade is obliged to draft and continuously update a list of games that pose a high risk to the health and life of the child, which should be accessible on the official portal of the Republic of Kosovo. Additionally, Article 11 paragraph 3 foresees the obligation for the Ministry of Internal Affairs and ARKEP to develop and issue a special manual through which the forms and actions to be taken by each institution are described in detail, especially the providers of internet services and video games. Yet, despite these obligations none of these actions has been undertaken.

[168] *Article 17 of Law No. 04/L-109 on Electronic Communications.*
[169] *Interview with ARKEP officials.*

In general, the legal framework lacks relevant procedural mechanisms on how to take measures for the take down of the illegal Internet content. From the analyses of the legislation aside from court orders mandating the removal of content distributed by individuals or companies registered in Kosovo that violate criminal code provisions, there are only a few other applicable mechanisms for content moderation. These include the Regulation on Audiovisual Commercial Communications[170], which prohibits audiovisual media from disseminating harmful content, and the voluntary Code of Written Media,[171] which encourages online portals to remove and refrain from publishing illegal content. While these entities are technically required to moderate comments and ensure that illegal content is not present on their platforms, it appears that they lack the capacity to effectively fulfill this obligation.

Nevertheless, content moderation and removal policies are complex and widely debated in global policy discussions.[172] Online platforms such as Facebook, Twitter, Tik Tok and Instagram often have terms of service that are difficult to understand, leading to confusion about what content should or shouldn't be removed. This results in inconsistent enforcement, with some important content, such as educational or historically significant material, being wrongly removed.[173] Governments and platforms have tried various solutions, such as stricter moderation rules in places like Germany[174], or using AI for content moderation, as seen with platforms like Facebook.[175] However, these methods have had mixed results. Harmful content, like extremist material, child pornography, and suicide-related content, needs to be addressed carefully without leading to over-censorship or undermining press freedom. A balanced approach is necessary, including clearer regulations, better oversight of platforms, improved digital literacy, fact-checking, and collaborative efforts between governments, platforms, and civil society. Various global organizations continue to explore ways to harmonize regulation with free expression and fundamental rights, offering valuable guidance for countries like Kosovo in shaping their own policies.

To this end, for the removal of illegal content from online environment, Kosovo depends on the content moderation policies of online platforms, as there is no national law requiring these platforms to comply with requests from Kosovo's institutions. However, online platforms do offer the possibility of responding to such requests. For example, Facebook's report on content restrictions based on local law reveals that in 2023, 37 pages and groups were restricted at the

---

[170] *Regulation on Audiovisual Commercial Communications, article 6 subparagraph 1.4.2 available at< https://www.kpm-ks.org/assets/cms/uploads/files/1353598810.1419.pdf>*

[171] *Code of Written Media, Part III available at http://www.presscouncil-ks.org/wp-content/uploads/2015/04/Press-Code-for-Kosovo_alb.pdf*

[172] *Dias (n135)*

[173] *Brennan Center for Justice, 'Facebook's Content Moderation Rules Are a Mess' (2021) available at https://www.brennancenter.org/our-work/analysis-opinion/facebooks-content-moderation-rules-are-mess.*

[174] *Germany, Network Enforcement Act (Netzwerkdurchsetzungsgesetz - NetzDG) (2021) available at https://bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_NetzDG.pdf. Analysis is available at: Farhad Manjoo, 'Facebook's Deletion Center in Germany' (The New York Times, 19 May 2018) https://nytimes.com/2018/05/19/technology/facebook-deletion-centergermany.html.*

[175] *See Meta Platforms, 'AI Use Policy' (2023) available at: https://transparency.meta.com/features/explaining-ranking/. , See also: Article 19, 'Regulating Social Media Content: Why AI Alone Cannot Solve the Problem' (2018) available at: https://article19.org/resources/ regulating-social-media-content-why-ai-alone-cannot-solve-the-problem/*

request of Kosovo's institutions.[176] Notably, no restrictions were imposed on individual comments, posts, events, or photo albums during this time.

An interesting development in this field is the EU's Digital Services Act ("DSA"), which could serve as a model for Kosovo to strengthen its regulatory framework for online content.[177] The DSA establishes clear obligations for platforms to moderate content and cooperate with national authorities, potentially providing Kosovo with a pathway to demand compliance from online platforms regarding illegal content, transparency of advertising and disinformation online. Although Kosovo is not an EU member, the EU Report on Kosovo 2023 notes that Kosovo should align its legal framework and policies with the principles of the DSA.

To this end, Kosovo could consider adopting a "trusted flaggers" system to prioritize the swift removal of illegal content, such as hate speech and disinformation, and ensuring online platforms comply with these measures. Providers of online platforms have to give priority to notices submitted by trusted flaggers and ensure that these are processed and decided upon without undue delay. Article 19 (1) of the DSA states that: Online platforms shall take the necessary technical and organizational measures to ensure that notices submitted by trusted flaggers through the mechanisms referred to in Article 14, are processed and decided upon with priority and without delay. Article 22 details the concept of a "trusted flagger" whereby: the status of 'trusted flagger' under this Regulation shall be awarded, upon application by any entity, by the Digital Services Coordinator of the Member State in which the applicant is established, to an applicant that has demonstrated that it meets all of the following conditions: (a) it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content; (b) it is independent from any provider of online platforms; (c) it carries out its activities for the purposes of submitting notices diligently, accurately and objectively. Additionally, for improving the regulatory landscape of transparency in online advertising, Kosovo could implement rules similar to those in the DSA, ensuring that users are informed when they are being targeted with advertisements, and have access to clear information regarding the identity of the advertiser and any targeting parameters used. This would help combat disinformation campaigns and politically motivated advertising that may manipulate public opinion.

Recommendations:

- Introduce specific national legal rules that explicitly regulate the blocking and filtering of illegal internet content. These laws should detail the procedures, responsibilities, and penalties associated with non-compliance.

---

[176] *Meta Platforms, 'Content Restrictions in Kosovo' (2023)* https://transparency.meta.com/reports/content-restrictions/country/XK/.

[177] *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1, available at* https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

- The Ministry of Industry, Entrepreneurship and Trade should prioritize drafting and continuously updating a list of video games that pose high risks to the health and life of children. This list must be publicly accessible on the official portal of the Republic of Kosovo.
- The Ministry of Internal Affairs and ARKEP must develop and issue detailed manuals outlining the procedures and actions required for content moderation, particularly for internet service providers and video game providers. These manuals should provide clear guidelines on identifying and handling illegal content.
- Although Kosovo is not an EU member, adopting principles from the EU's DSA can provide a robust framework for regulating online content. This includes:
    - Establishing a system of trusted flaggers to prioritize the removal of illegal content. Trusted flaggers should be entities with proven expertise and independence in detecting and reporting harmful content.
    - Mandating online platforms to adhere to strict content moderation standards, ensuring transparency in their operations and accountability in handling user reports.
- Implement regulations that require online platforms to disclose when users are being targeted with advertisements, including information about the advertisers and the targeting criteria used.
- Encourage audiovisual media and online portals to adopt and rigorously implement the Regulation on Audiovisual Commercial Communications and the Code of Written Media. Provide training and resources to help these entities effectively moderate content.
- Invest in the development of infrastructure and training programs that enable media organizations and online platforms to handle content moderation more efficiently and effectively.
- Implement digital literacy programs to educate citizens about their digital rights, safe online practices, and the importance of reporting harmful content.

Chapter 6 - Digital Governance in Kosovo

Digital governance aims to develop and implement strategies that utilize technology to strengthen the connection between governments, citizens, and businesses. In Kosovo, as explained earlier where internet penetration and online engagement are remarkably high, the digital sphere presents significant opportunities for advancing fundamental rights, such as the right to information, freedom of expression, assembly, and participation in political decision-making processes.

The transformative potential of digital tools in promoting human rights was particularly evident during the COVID-19 pandemic. The E-Kosova platform launched in February 2021, played a pivotal role in facilitating the registration of citizens for COVID-19 vaccinations, ensuring that the right to health was accessible to all, even under challenging circumstances. Moreover, digital platforms enabled continuity in education, thereby upholding the right to education during school closures.

Currently, E-Kosova offers over 155 electronic services, catering to a wide range of needs. With more than 155 electronic services available[178] and over 948,000 registered users[179], the platform reaches a substantial amount of the population of Kosovo. Yet this number of services offered in E- Kosova constitutes a relatively small fraction of all public services.[180]The E-Kosova platform is a centralized digital hub designed to provide citizens with easy access to various government services online. It streamlines interactions between the government and the public, making essential services more accessible and efficient.

Citizens can use the platform for various purposes, such as:

- Social Benefits: Applying for social assistance programs, including child allowances and pensions.
- Health Services: Scheduling appointments, accessing medical records, and registering for COVID-19 vaccinations.
- Education: Applying for scholarships, accessing school transcripts, and other educational resources.
- Civil Registration: Requesting personal documents like birth, marriage, and death certificates.

[178] *Office of the Prime Minister of Kosovo, 'The e-Komuna Platform is Launched: It Facilitates Citizens' Access to Municipal Services' (2023) available at: https://kryeministri.rks-gov.net/en/blog/the-e-komuna-platform-is-launched-it-facilitates-citizens-access-to-municipal-services/.*
[179] *Government of Kosovo, 'eKosova' available at: https://ekosova.rks-gov.net/.*
[180] *OECD, Western Balkans Competitiveness Outlook 2024: Kosovo (OECD Publishing, Paris, 2024), 145 available at: https://doi.org/10.1787/ff74ae0e-en.*

- Business Services: Registering a business, obtaining permits, and accessing various business-related services.

- Public Utilities: Managing utility bills and services, including water and electricity payments.

- Transport Services: Applying for vehicle registration, renewing driver's licenses, and other transport-related services.

Overall, guided by the e-Government Strategy 2023–2027[181] and the Digital Agenda of Kosovo 2030[182], the government aims to modernize public administration, improve service delivery, and create a digitally inclusive society. These strategic initiatives are aligned with European standards and emphasize the development of digital skills, cybersecurity, and innovation within the public sector.

The e-Government Strategy 2023–2027, adopted in October 2023, serves as the foundation for Kosovo's digital transformation. This strategy outlines a cohesive approach to enhancing e-Government coordination, cybersecurity, and digital skills development. It promotes a 'whole-of-government' enterprise architecture, user-centric digital services, and the enhancement of competencies across the public sector. The ultimate vision is for Kosovo to become a digitally advanced country with an efficient public administration and a robust digital economy by 2030.

The Digital Agenda of Kosovo 2030, approved in June 2023, sets a comprehensive framework for the country's digital transformation, focusing on modernizing public services. The government's goal is to provide all essential public services online through the E-Kosova platform by 2030. To support this, the Government has developed an interoperability platform that enables secure data exchange between key institutions such as the Kosovo Business Registration Agency, Civil Registration Agency, Tax Administration of Kosovo, Customs, and the Kosovo Cadastral Agency. However, as highlighted in the OECD Western Balkans Competitiveness Outlook report 2024, this platform is currently underutilized.[183] Legal and administrative inefficiencies, along with poor data quality in digital public registers, mean that only about 10% of public services are available online.[184] Therefore to enhance the digital governance, it is essential to update the legal framework on open data. The government should adopt new legislation aligned with the Open Data Directive and the EU Data Governance Act to expand the obligations of public institutions in making public sector data accessible for reuse. This legislation should cover aspects such as licensing, data formats, and metadata content, and should identify high-value datasets like geospatial and

[181] *Government of Kosovo, e-Government Strategy Kosovo 2023-2027 (2023) available at https://mpb.rks-gov.net/Uploads/Documents/Pdf/EN/2700/e-Government%20Strategy%20Kosovo%202023-2027.pdf.*
[182] *Government of Kosovo, Digital Agenda (2023) available at https://arkep-rks.org/desk/inc/media/82582FB3-CD31-4D3D-A2AA-F7CC21ACADCA.pdf.*
[183] *OECD, Tax Administration 2022: Comparative Information on OECD and Other Advanced and Emerging Economies (2022) available at https://www.oecd-ilibrary.org/docserver/de4be518-en.pdf?expires=1727040150&id=id&accname=guest&checksum=68D2376FF5D9EDD485B156585840CC17.*
[184] *Ibid.*

statistical data. Additionally, there should be a focus on building the capacity of public officials to manage and distribute data effectively, standardize data processes, and foster partnerships with the private sector and civil society for developing data-driven digital services.

Notable developments in Kosovo's digital governance include the implementation of an electronic system by the Kosovo Agency for Prevention of Corruption, which allows public access to property declarations of public officials.[185] This initiative enhances transparency and accountability. Additionally, the E-Consultations platform has been launched to increase citizen engagement.[186] This platform enables citizens to provide feedback on governmental policies and legislation before they are voted on in parliament, ensuring greater public participation in the decision-making process.

Nevertheless, to have successful digital governance initiatives, a robust digital infrastructure is crucial. The government has set ambitious goals to improve connectivity across the country. By 2025, Kosovo aims to have a fully digitized atlas of fixed broadband infrastructure, and by 2026, all public institutions are expected to have gigabit connections.[187] The government also plans to achieve comprehensive 5G network coverage by 2030, ensuring that all citizens have access to high-speed internet.[188]

Despite these goals, significant challenges persist, particularly in upgrading existing networks to support a future gigabit society. Although 5G licenses were granted to two telecom operators, IPKO and Telecom Kosovo, in the 800 MHz and 3.5 GHz frequency bands in early 2023, regulations that would simplify 5G network installations, such as a permit-exempt deployment regime, are still pending.[189] Furthermore, there are no established specifications for the physical and technical characteristics of small-area wireless access points (small antennas) that align with the relevant European Commission regulation.[190] In addition, Kosovo lacks a cybersecurity certification framework for ICT products, services, and processes, consistent with the EU Cybersecurity Certification Framework.[191] Although commercial 5G licenses have been issued, Kosovo has yet to implement specific cybersecurity measures for 5G networks, leaving a gap in the comprehensive protection of this critical infrastructure.[192]

To fully realize the benefits of digital governance, Kosovo is committed to building digital skills among its citizens. The government aims to have 5% of the population become active IT specialists, while equipping the remaining 95% with basic digital skills.[193] However, both the private and public sectors currently face a significant shortage of qualified ICT professionals, who

[185] *See at https://deklarimi-apk.net/*
[186] *See at https://konsultimet.rks-gov.net/*
[187] *Government of Kosovo (n183)*
[188] *Ibid.*
[189] *OECD (n184)*
[190] *ibid*
[191] *ibid*
[192] *ibid*
[193] *ibid.*

represented just 0.5% of the total workforce in 2023.[194] This gap highlights the urgent need for comprehensive educational reforms and the introduction of non-formal education options for training ICT experts and specialists

Recommendations:

- Speed up broadband improvements with a focus on optical fiber to ensure high-speed internet nationwide.
- Simplify regulations for 5G deployment and establish clear standards for small wireless access points.
- Develop and implement a national cybersecurity certification framework for ICT products, services, and processes, consistent with the EU Cybersecurity Certification Framework, to protect the integrity of digital infrastructure.
- Update the legal framework on open data by adopting legislation aligned with the Open Data Directive and the EU Data Governance Act. This legislation should regulate licenses, dataset formats, and metadata content, while identifying high-value datasets (e.g., geospatial, statistical data)
- Train public officials in data management and encourage partnerships with private companies to develop innovative digital services.
- Address the mismatch between educational offerings and labor market needs.

[194] *Government of Kosovo (n182) 12.*

Chapter 7 - Artificial Intelligence

Artificial Intelligence ("AI") has the potential to significantly transform various sectors in Kosovo, such as education, healthcare, and finance, by offering innovative solutions and improving efficiency. For instance, AI can provide personalized learning experiences, enhance medical diagnoses, and streamline financial transactions. However, these advancements also bring considerable challenges, particularly in relation to privacy, freedom of expression, and other digital rights. Ensuring the ethical and responsible use of AI requires a robust regulatory framework that addresses these issues.

Currently, Kosovo does not have a dedicated policy or regulatory framework for the development and utilization of emerging digital technologies, such as AI. While the Digital Agenda Strategy 2030 envisions the creation of an AI strategy and the integration of emerging technologies into tertiary education curricula, these goals need to be translated into actionable, budgeted initiatives with well-defined roles, monitoring, and accountability processes.[195]

The absence of a legal framework leaves a gap in the protection of human rights when AI is deployed, particularly in public service areas where the consequences of automated decision-making can be profound. The automatic processing of data about a person's health, employment, welfare, or credit can lead to discriminatory or unfair outcomes, especially for vulnerable groups. Therefore, it is critical to ensure that AI systems are designed and implemented with full consideration of human rights, data protection, and ethical standards.

In addition, Kosovo should draw lessons from the European Union's approach to AI regulation, including the European Commission Proposal for a Regulatory Framework on Artificial Intelligence" (the 'EU AI Act'),[196] which adopts a risk-based approach to regulating AI systems. This involves applying different levels of regulatory scrutiny based on the potential impact of AI on individuals and society. The development of a similar framework in Kosovo would help mitigate the risks associated with AI, such as discrimination and privacy violations, while supporting innovation.

Moreover, the integration of AI into public administration should be approached with caution. AI systems used in the public sector must be transparent, accountable, and subject to rigorous human oversight to prevent misuse and ensure compliance with democratic principles and human rights. It is also essential to build public trust in AI by involving civil society and affected communities in the development and implementation of AI policies and systems.

---

[195] *OECD (184) 148.*

[196] *European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final, 21 April 2021, available at https://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.*

Given these challenges, Kosovo should prioritize the development of an enabling environment for the responsible use of AI and other emerging technologies. This includes not only regulatory measures but also the promotion of digital literacy and capacity building among public officials and citizens to foster a deeper understanding of AI's implications and potential benefits.

It appears that, through the legislative agenda, the Draft Law on the Protection of Individuals Regarding the Automatic Processing of Personal Data is expected to be adopted by the government by the end of 2024.[197] Given its title, the law could potentially regulate the use of AI, particularly in how AI systems handle the automatic processing of personal data.

However, it is important to note that the draft law has not yet been made available on the public consultations platform, leaving some uncertainty regarding the specific provisions it will include. Without the opportunity for public and expert review, it remains to be seen how comprehensively the law will address the challenges posed by AI technologies, particularly in relation to safeguarding digital rights and ensuring ethical AI use.

Recommendations:

- Formulate a national AI strategy that outlines clear guidelines for the development, deployment, and governance of AI technologies. This strategy should include specific budgeted initiatives, well-defined roles, and accountability mechanisms to support the responsible use of AI in both public and private sectors.
- Develop a legal framework aligned with the EU's AI Act and international best practices. This framework should adopt a risk-based approach, where regulation is proportional to the impact of AI systems on people's lives. It should cover areas such as data protection, transparency, accountability, and ethical considerations.
- Set up a multidisciplinary AI Ethics Committee to oversee the implementation of AI technologies, especially in high-risk sectors like public administration, healthcare, and finance. This committee should include experts from various fields, including human rights, technology, law, and civil society.
- Implement educational programs and public awareness campaigns to enhance understanding of AI technologies and their implications among citizens, public officials, and businesses. This will help build a more informed society that can engage with AI responsibly.
- Encourage collaboration between the government, private sector, and academia to promote innovation in AI while ensuring that the development and deployment of AI technologies are guided by ethical principles and human rights considerations.

[197] *Government of Kosovo, Legislative Program for 2024 (2024) available at https://kryeministri.rks-gov.net/wp-content/uploads/2024/02/Programi-Legjislativ-per-vitin-2024-.pdf.*

Chapter 8 - Conclusion

In conclusion, Kosovo's digital landscape is at a crucial crossroads. The country has made important strides in adopting digital governance frameworks and aligning its policies with European Union standards, but significant challenges remain. The protection of digital rights, including data privacy, freedom of expression, and cybersecurity, is paramount as Kosovo continues its journey toward a fully digital society.

Kosovo's journey toward a digitally inclusive society is marked by both progress and significant challenges. The country's commitment to digital governance is evident in its strategic initiatives, such as the e-Government Strategy 2023–2027 and the Digital Agenda of Kosovo 2030, which aim to bring all essential public services online by 2030. However, to fully realize this vision, it is crucial to address the existing gaps in legal frameworks, improve digital literacy, and ensure robust cybersecurity measures.

The digital transformation of Kosovo is not just about technological advancement but also about upholding human rights in the digital sphere. The protection of privacy, freedom of expression, and access to information must be at the forefront of these efforts. It is essential for the government to establish clear and effective regulations that support innovation while safeguarding digital rights and at the same time the government must allocate adequate resources to institutions responsible for upholding digital rights and ensure that they have the capacity to respond to emerging threats, such as cybersecurity attacks and the rise of disinformation.

By implementing the recommendations outlined in this reports such as enhancing the cybersecurity framework and promoting digital literacy—Kosovo can build a resilient digital environment that benefits all citizens. A collaborative approach involving government agencies, civil society, and the private sector will be key to overcoming the challenges and ensuring that digital transformation contributes positively to the socio-economic development of the country. Kosovo’s digital transformation will only succeed if it ensures that all citizens, regardless of socio-economic background, have access to technology and are protected by robust legal frameworks that safeguard their rights in the digital realm. By prioritizing digital rights, cybersecurity, and public awareness, Kosovo can build a digital society that not only fosters innovation and economic growth but also protects the fundamental freedoms and rights of its citizens.

ITS INSTITUTE FOR TECHNOLOGY AND SOCIETY