

# Balancing Cybersecurity, Artificial Intelligence and Human Rights:

## OPPORTUNITIES AND CHALLENGES IN KOSOVO

IMANE BELLADEM



THIS ILLUSTRATION  
IS GENERATED BY AI



# **Balancing Cybersecurity, Artificial Intelligence and Human Rights:**

**OPPORTUNITIES  
AND CHALLENGES IN  
KOSOVO**

**Title:**

**Balancing Cybersecurity,  
Artificial Intelligence and Human**

**Rights:**

Opportunities and Challenges in  
Kosovo

**Author:**

Imane Bellaadem

**Cover:**

Illustration is generated by AI and  
edited by Tedel.

**Published by:**

Kosovo Foundation for Open  
Society

Prishtina,

May 2023

This publication has been  
produced as part of the Kosovo  
Research and Analysis Fellowship  
(KRAF), an initiative of the Kosovo  
Foundation for Open Society  
(KFOS).

---

## Balancing Cybersecurity, Artificial Intelligence and Human Rights: Opportunities and Challenges in Kosovo



1

— p.09

Introduction

2

— p.15

Cybersecurity,  
AI and human rights

3

— p.25

Kosovo: policy and  
practices overview

4

— p.34

Conclusions

5

— p.36

Recommendations

6

— p.37

Bibliography

BALANCING CYBERSECURITY, ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS:



# 1 Introduction

Cybersecurity, artificial intelligence, machine learning, social media, Internet are only some of the digital technologies available nowadays. With the huge expansion of the Internet, altogether with the development and increasing accessibility of digital gadgets, these technologies inevitably became an essential part of our lives. As these technologies were growing and developing new features, experts and governments commenced to increase their applicability in various layers of critical infrastructures. So nowadays one can find entirely digitalised public administrations where all services can be provided online, physical archives being replaced by digital databases, schools integrating digital tools for learning and so on. Access of individuals to the Internet and the majority of mainstream applications have accelerated the influence of digital technologies on their lives. All spectrums of one's life are covered by some sort of mobile applications, or a service provided online. Some of the most famous

applications include speech recognition, virtual assistance in customer service and recommendation engines.<sup>1</sup> As these technologies assist the users and ensure an increased access to some services and products, privacy concerns have been raised.

Reliability of critical infrastructures<sup>2</sup> on these technologies is a top priority for many governments and other key international stakeholders. The governments are investing capacities in order to mitigate the risks this reliability poses for the state viability. The relevance of strengthening states' cybersecurity remains clear and is undisputable, however, including a human-centric approach whilst regulating these domains must not be neglected. Human rights and good governance are two intertwined and interdependent areas. When taking into account the degree that Internet and digital technologies are incorporated in an average user's life, it becomes clear that cybersecurity serves

---

<sup>1</sup> IBM Cloud, <https://www.ibm.com/topics/artificial-intelligence>, accessed 27st February 2023

<sup>2</sup> EU defines critical infrastructures as 'an asset or system which is essential for the maintenance of vital societal functions'

as a pre-requisite for guaranteeing and exercising human rights. This claim is supported by inclusion of digital rights as a 4<sup>th</sup> generation of human rights in academic theory<sup>3</sup> and by the fact that many international instruments have extended their applicability to online spaces. All protected human rights can be exercised in both online and physical spaces. Existing regulations are rather focused on protecting human rights in physical space, therefore, it is necessary to extend this protection to cyberspaces, as well.

In this paper, we will look closer into how cybersecurity and artificial intelligence (AI) intersect with freedom of expression and privacy in general. Furthermore, we will examine the current cybersecurity and AI landscape in Kosovo and map challenges and obstacles, as well as good practices that are adopted in Kosovo. The paper will examine the extent to which a human-rights based, or human-centric approach is implemented when regulating cybersecurity in Kosovo.

The methodology mostly relies on desk research and interviews. Desk research reviews both primary (ranging from international legislation and standards; national framework including legislation in procedures, policies, strategies) and secondary sources (academic articles, books, reports of both governmental and non-governmental bodies; media articles). During the desk research period, specific dimensions were identified as relevant to discuss with interviewees.

Moreover, desk research indicated which groups of stakeholders are relevant for the research. Seven semi-structured individual interviews were conducted in total, with representatives of civil society and international experts. One of the shortcomings of the research is that no state institutions was interviewed, due to their limited responsiveness.

The study is divided into three main chapters. The first chapter provides definitions of key terms, cybersecurity and AI, and provides a brief overview of international legislation. The second chapter discusses the intersection of cybersecurity and AI with human rights, and the relevance of adopting a human rights-based approach. The following chapter Kosovo's cybersecurity legislation and practices. The study ends with a set of recommendations directed to different stakeholders.

## 1.1. Cybersecurity definitions

This subchapter will look into the definition of cybersecurity as there is not an adopted unilateral approach to what cybersecurity involves. In order to fully understand the scope of cybersecurity, we must firstly understand what are the critical elements of cybersecurity.

Digital Guardian defines cybersecurity as “the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack,

---

3 Risse, M. The Fourth Generation of Human Rights: Epistemic Rights in Digital Lifeworlds, Carr Center for Human Rights Policy, Harvard Kennedy School, Harvard University, 2021

damage, or unauthorised access”.<sup>4</sup> There is no unilateral definition of cybersecurity and European Union Agency for Network and Information Security (ENISA) has noted that there is no need for providing a conventional definition, as this is an evolving term and it is practically impossible to include all components of cybersecurity in one definition. However, in the attempt to standardise the scope of cybersecurity, ENISA agrees it should refer to “security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that cyberspace.” Freedom Online Coalition (FOC),<sup>5</sup> partnership of 36 governments worldwide, defines cybersecurity as “the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline.”<sup>6</sup>

As discussed, these definitions follow the three-key-components structure: *what*, *how* and *against what*. *How* refers to activities, tools, guidelines, policies, education; *what* focuses on networks, systems, programs,

assets; *against what* emphasises attack, damage, incidents. Yet, they scarcely or entirely omit to incorporate the human aspect of cyber security in the definitions. Lack of inclusion of human aspect in the definitions affect the ability to approach and regulate the cyber domain holistically and to assess risks posed to systems and users in cyber domain.<sup>7</sup>

## 1.2. Artificial Intelligence definition

Following the previous subchapter, we are proceeding with providing the definition of AI. Taking into account that AI is a central concept in this study, it is highly important to understand what is AI and what elements of AI are particularly relevant for this study.

AI is a term that is interconnected with algorithmic decision-making and can rarely be analysed solely. Both act as umbrella terms, and no uniform decision can be found.<sup>8</sup> Colloquially, these terms are used interchangeably, however, it is important to note some essential differences.

“Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image

4 Digital Guardian, What is Cyber Security? Definition, Best Practices & Examples, 2022, <https://www.digitalguardian.com/blog/what-cyber-security>, accessed 05th March 2023

5 Freedom Online Coalition website, 2022, <https://freedomonlinecoalition.com/members/>, accessed 01st March 2023

6 Association for progressive communication, Why cybersecurity is a human rights issue, and it is time to start treating it like one, 2022, <https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one>, accessed 01st February 2023

7 Cains, M. et al, Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation, Risk Analysis: an official publication of the Society for Risk analysis, 2021, Author: Cains, Mariana G : Search (wiley.com), accessed 15th February 2023

8 Zuiderveen Borgesius, F. Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, Directorate General of Democracy, 2018. <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decisionmaking/1680925d73>, accessed 05th March 2023

analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications).”<sup>9</sup>

John McCarthy defined AI as “the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence.”<sup>10</sup> International organisations such as Organisation for Security and Co-operation in Europe (OSCE) and Council of Europe have also provided definitions on AI. The Council of Europe glossary defines AI as “a set of sciences, theories and techniques whose purpose is to reproduce, by a machine, the cognitive abilities of a human being to be able to entrust a machine with complex tasks previously delegated to a human”. On the other hand, OSCE refers to AI as “based on algorithms, which are sets of human-designed instructions with encoded procedures for transforming input data into a desired output, based on specific calculations.”

Furthermore, in order to fully understand the scope of algorithms, we must perceive them as an integral part of AI and algorithmic decision-making. Algorithms have the role of recognising patterns to carry out certain tasks independent of human intervention, thus facilitating automated decision-making.<sup>11</sup> Defining AI has the same problematics as

cybersecurity, as both of the terms are constantly advancing and there is a need to re-evaluate their definitions and expand them with new components.

### 1.3. International legislation efforts

Cybersecurity and AI are fairly new topics that are raised in international law community. Therefore, effort to regulate are scarce and incomplete as it was very complex to predict and assess the future of these technologies. However, there is a consensus that the existing international law applies to cyberspaces as well. Human Rights Council Resolution from 2012 emphasises that international human rights law and international humanitarian law have equal effect both online and offline. It also stresses the need for cybersecurity measures to safeguard both technological advancements and the enjoyment of human rights.<sup>12</sup> Efforts to regulate the cyberspace are seriously complicated due to its transnational character. States should be cooperative and have similar stances to have an efficient regulation. Nevertheless, there is a general agreement that states should refrain from wrongful acts in cyberspace and that states have jurisdiction over information and communications technology.<sup>13</sup>

Intensifying efforts to enact regulations have resulted in establishment of the UN Group of Governmental Experts (UN GGE).

---

9 This initial definition of AI HLEG was subject to further discussion in the groups. See AI HLEG (2019)

10 McCarthy, J. What Is Artificial Intelligence?, Stanford University, 2007

11 Kostić, B. & Sinders, C. Responsible AI, Council of Europe, 2022

12 Pavlova, P. ‘Human-rights based approach to cybersecurity: Addressing the security risks of targeted groups’, Peace Human Rights Governance, 4(3), 391-418, 2020, [PHRG-2020-3-04.pdf \(padovauniversitypress.it\)](#), accessed 20th April 2023

13 Geneva Internet Platform DigWatch, UN OEWG, [UN OEWG in 2023 - DW Observatory \(dig.watch\)](#), accessed 29st March 2023

They were operational between 2004 and were discussing how to maintain security and peace in cyberspace. Amid the UN GGE ceasing their work, the UN has formed UN Open-Ended Working Groups (OEWG) since 2020. The focus is to establish programmes that are not limited to mandates, unlike GGE, in the field of cybersecurity.<sup>14</sup> A resolution on the program of action on cybersecurity was adopted in November 2022, assuring that this programme of action becomes a permanent mechanism after OEWG 2021-2025 ends.<sup>15</sup>

The Council of Europe had introduced one of the first conventions on cybersecurity. The Budapest Convention, also known as Cybercrime Convention, has set the standards for criminalisation of cybercrime. It has foreseen increased cooperation among states to prosecute cybercrime and exchange e-evidence.<sup>16</sup> EU has made steps into further regulating cybersecurity and AI. The EU has proposed the AI Act in 2021.<sup>17</sup> This is the first piece of regulation and has adopted a risk-based approach whilst drafting it. This will lead to having transparent obligations of AI deployers and enhance safety and human rights in EU.<sup>18</sup> The introduction of the EU Cybersecurity Act entails the establishment of a certification framework for ICT products, processes and services throughout the EU, which is a step forward to standardisation in cybersecurity.<sup>19</sup>

A better understanding of the expansion of AI and the relevance of cybersecurity has served as a motivation to commence the regulation. While the abovementioned regulations serve as a great starting point, it is still necessary to define international standards of cybersecurity protection which would serve as a baseline for further regulations. Furthermore, it is necessary to enhance international cooperation among states to address cybersecurity threats effectively but also to develop a platform for information sharing and collaboration in research. It would be beneficial to develop standardised ethical guidelines for AI as a common ground to ensure that AI is developed ethically and will not harm individuals or society. Lastly, it can be concluded that we will see more declarations and regulations tackling these matters, in addition to the existing ones due to its advancement and global character.

14 UN Office for Disarmament Affairs, Group of Governmental Experts, [Group of Governmental Experts – UNODA](#), accessed 27st February 2023


15 Geneva Internet Platform DigWatch, UN OEWG, [UN OEWG in 2023 - DW Observatory \(dig.watch\)](#), accessed 29st March 2023

16 Convention on Cybercrime: Special edition dedicated to the drafters of the Convention (1997-2001), Council of Europe, 2022, [1680a6992e \(coe.int\)](#)

17 European Parliament, Artificial Intelligence, 2023, [Artificial intelligence \(europa.eu\)](#)

18 EU Regulatory framework proposal on artificial intelligence, [Regulatory framework proposal on artificial intelligence | Shaping Europe's digital future \(europa.eu\)](#)

19 European Commission, The EU Cybersecurity Act, [The EU Cybersecurity Act | Shaping Europe's digital future \(europa.eu\)](#)



Evolving of AI can bring a wide array of social and economic benefits. Areas that can benefit from the use of AI are of high-impact sectors, and include climate change, environment and health, finance, mobility, home affairs and agriculture. However, the same specifications that unlock the possibilities of socio-economic development represent risks for negative effects for individuals and society.



# Cybersecurity, AI and human rights

Cybersecurity, AI, algorithmic decision-making and machine learning are only some of the digital technologies that are evolving rapidly. The evolution of these technologies is followed by their increased use in public and private sector, but also by individuals in their private life. However, it remains unclear what are the long-term effects of AI on individuals and on the society, whereas cybersecurity is taking a protective role towards critical infrastructure, data and other assets.

Evolving of AI can bring a wide array of social and economic benefits. Areas that can benefit from the use of AI are of high-impact sectors, and include climate change, environment and health, finance, mobility, home affairs and agriculture. However, the same specifications that unlock the possibilities of socio-economic development represent risks for negative effects for individuals and society.<sup>20</sup> Some of the raised concerns are international security,

social and political stability, disruption of the labour markets, economic and social inequality, etc.<sup>21</sup>

All major international organisations identified AI as a critical enabler relevant for increasing and maintaining democratic governance and fundamental rights. It is agreed that AI may facilitate participatory democracy, accountability and transparency. AI-based technologies can foster media pluralism and provide enabling environment for civil society. On the other side, use of these technologies can influence citizens' behaviour and attitudes, which can be manipulated for certain political purposes, such as influencing electoral processes, manipulating public opinion, spread misinformation and propaganda and so on.

The following subchapters look into the interconnections between freedom of expression and media freedoms and right to privacy with cybersecurity and

---

<sup>20</sup> 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 Union legislative acts COM (2021)206, 2020, 2  
<sup>21</sup> Parliamentary Assembly of Council of Europe, Need for democratic governance, Resolution 2341, 2020, 1

AI. It provides definitions to key digital technologies and explains how they effect freedom of expression, media freedoms and right to privacy. The definitions are complemented with illustrative examples for a better understanding.

## 2.1. Freedom of expression and media freedoms

Freedom of expression and media freedoms are considered one of the main pillars of a functioning democracy. Free, uncensored access to information, engaging freely in public debates are crucial for combating disinformation, misinformation, advancement of media literacy and for the right to be informed on topics of public interest. Theoretically, the emergence of social media platforms has played an important role in increasing access of information to the general public. In practice, many challenges and obstacles have found a way of hindering these processes.

Freedom of expression can be affected by multiple factors in the online sphere. Social media platforms, private companies as well as governments can influence availability, accessibility and placement of certain information online.<sup>22</sup> Social media platforms build their power on their omnipresence in the public discourse and their ability to shape opinion power. Opinion power can be defined as the ability of the media to influence processes of individual and

public opinion formation.<sup>23</sup> Concentration of opinion power in social media platforms represent the biggest slippery slope for any functioning democracy. As they can easily be instrumentalised as political tools to shape public discourse into a certain way, it is necessary to disperse the concentration of opinion power and ensure that social media platforms remain a platform where all voices can be heard.<sup>24</sup> The political power and the extremely lucrative possibilities are the leading factors in this interplay.<sup>25</sup> Moreover, content moderation and content curation are AI's most powerful tools that can effect freedom of expression and media freedoms. Discussions about these two terms are found in what follows.

**Content moderation** entails that every content to be published goes through a three-step moderation.<sup>26</sup> First, platforms' Terms of Services require that every content is assessed by automatic filters, to examine whether the content meets defined minimum standards to be published. The second step is placing the specific content within the platform using AI and algorithms. By placing content, we refer to ranking, optimising and recommending the content based on certain criteria. This step is crucial to the visibility of the content, as the automated processes "decide" to whom and to what extent will a certain content be exposed to, e.g. if your content is placed on second page of Google's search, this will affect the information you want to pass on, as only 6%

---

22 Bromell, D. *Regulating free speech in a digital age: hate, harm and the limits of censorship*, Springer, 2022

23 Neuberger, C. "Meinungsmacht im Internet aus Kommunikationswissenschaftlicher Perspektive." *UFITA* 82 (1): 53-68, 2018

24 Helberger, N. *The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power*, *Digital Journalism*, 8:6, 842-854

25 Kostić, B. *AI traps and media diversity: mind the loopholes*, Media Diversity Institute, 2021. <https://www.media-diversity.org/artificial-intelligence-traps-and-media-diversity-mind-the-loopholes/>, accessed 01st February 2023

26 Bukovska, B. *Spotlight on Artificial Intelligence and Freedom of Expression*, OSCE, 2020, 3



of website clicks come from the second page of Google search.<sup>27</sup> The last step concerns the content when it is already published. They consist mainly of the reporting mechanism of each platform. These mechanisms enable users to report, flag or block content, which results in a combined AI and human's assessment of the dispute. The content can be removed, the users can be sanctioned or blocked.<sup>28</sup>

Namely, the last two steps are the most important for freedom of expression and media freedoms, as they decide whether a content will be published, to whom will it be shown and whether it will be removed and censored. This is particularly important in politically sensitive times, such as a preelection campaigns, or campaigns about legislation. Through work with media outlets, a civil society representative highlights that there is a pattern of removing satiric content from social media as they were flagged as problematic.<sup>29</sup> This shows the lack of understanding of political, socio-economical, and linguistic contexts of these technologies, but has the power to restrict the voice of media and assess what is to be removed.<sup>30</sup> Another vivid example is that in May 2018, Facebook suspended Bosnian journalist Dragan Bursać's profile for a period of 24 hours because he posted an image of a detention camp for Bosniaks in Serbia during the war in Bosnia and Herzegovina. As per the reports of the local media, Facebook considered that Bursać's

post violated the "community standards",<sup>31</sup> as the picture contained explicit content. Specifically, Bursać is considered an independent journalist from Bosnia and Herzegovina, opposing governments attempt to glorify and deny war crimes in BiH. So, suspending his Facebook profile can be used as an argument to discredit his work by politicians or other parties whose work Bursać is critical of. This also sparked a discussion of why is it inappropriate to post about detention camps in Serbia and by whom is that assessed as inappropriate if the claims are truthful. Due to the limited transparency of the automated systems utilised, this remains a question for further research. On the other hand, automated systems fail to remove harmful content, despite being updated regularly, and are not always able to distinguish harmful and hateful content.<sup>32</sup> It was discovered that nearly 50% of the reported content originating from the Western Balkans that was reported is still available online.<sup>33</sup>

Content moderation is closely connected to content curation and they complement each other in a way that moderation counters harmful content, whereas curation focuses on placement of the content. Accordingly, **content curation** mainly refers to the recommendation system deployed by each platform. Algorithms seek to optimise what end- users see on their profiles by identifying and assessing patterns in digital behaviour, thus resulting

27 Forbes, The Value Of Search Results Rankings, 2017, [The Value Of Search Results Rankings \(forbes.com\)](https://www.forbes.com/sites/forbes/2017/03/27/the-value-of-search-results-rankings/)

28 Kostić B, Sindere C, Responsible Artificial Intelligence, Council of Europe, 2022, 15

29 Interview with Ena Bavčić, 01st March 2023

30 Ibid.

31 Jeremić et al, Facebook, Twitter Struggling in Fight against Balkan Content Violations, BIRN, 2021, [Facebook, Twitter Struggling in Fight against Balkan Content Violations | Balkan Insight](https://www.birn.net/news/2021/03/23/facebook-twitter-struggling-in-fight-against-balkan-content-violations/), accessed 15th March 2023

32 Bukovska, B. Spotlight on Artificial Intelligence and Freedom of Expression, OSCE, 2020, 56

33 Jeremić et al, Facebook, Twitter Struggling in Fight against Balkan Content Violations, BIRN, 2021, [Facebook, Twitter Struggling in Fight against Balkan Content Violations | Balkan Insight](https://www.birn.net/news/2021/03/23/facebook-twitter-struggling-in-fight-against-balkan-content-violations/), accessed 15th March 2023

in a personalised feed. In an attempt to maximise profit, platforms seek to attract users to spend more time on social media by personalising their feed, based on what their interactions, locations, searching history etc.<sup>34</sup> This is also known as internet filter-bubble phenomenon.<sup>35</sup> This is the main reason why nobody sees the same main feed on a social media platform. Creating an echo chamber in the online spaces by not having a fluctuation of different sources of information and by filtering and blocking content is a fertile soil for sharing misinformation and disinformation,<sup>36</sup> and overreliance of media outlets on social media platforms is a contributing factor to this phenomenon.

While content curation does not prevent an individual to express themselves freely, it can hinder their right to seek, receive and impart information and ideas through any media and regardless of frontiers.<sup>37</sup> It serves to only reinforce the user's confirmation bias and to limit exposure to opposed views. For example, in April 2020, Twitter deleted more than 20,000 fake accounts linked to Saudi, Serbian and Egyptian governments and were assessed as "targeted attempt to undermine the public conversation". A total of 8,558 accounts were associated with Aleksandar Vučić's Serbian Progressive party (SNS), with over 43 million tweets posted promoting

favourable news on Vučić's administration and attacking opposition political leaders.<sup>38</sup> This took place only two months prior to Serbian parliamentary elections,<sup>39</sup> with the aim to shape the opinion of SNS's electorate. One study tested confirmation bias as a misinformation tool regarding climate change. It showed that the confirmation bias achieved when receiving information consistent with pre-existing views is particularly strong among climate change deniers. This position only reinforced their pre-existing views and heightened polarisation on climate change.<sup>40</sup>

Whilst analysing cybersecurity and its effect on freedom of expression and media, we must highlight cyberattacks targeting media outlets and journalists, where cyberattacks are used as an intimidation tool to influence how their target is working or not working.<sup>41</sup> The consequence of a cyberattack is wider than a mere attack on a system or a network, but usually has a political connotation as well. The main goal is "to change their behaviour by making threats to deny, degrade, or disrupt networks or affect the availability or integrity of the data stored on them."<sup>42</sup> This aggravates their freedom to work without fear of persecution, retaliation, and digital assassination. The psychological effect of cyberattacks is not to be neglected. Risk perception among targeted groups

34 Pirkova, E. et al, Spotlight on Artificial Intelligence and Freedom of Expression-A Policy Manual, OSCE, 202, 66

35 Kostić B, Sindere C, Responsible Artificial Intelligence, Council of Europe, 2022, 16

36 Leslie D et al. Artificial intelligence, human rights, democracy, and the rule of law: a primer. The Council of Europe, 2021

37 Universal Declaration of Human Rights, 1948

38 The Guardian, Twitter deletes 20,000 fake accounts linked to Saudi, Serbian and Egyptian governments, 2020, [Twitter deletes 20,000 fake accounts linked to Saudi, Serbian and Egyptian governments | Twitter | The Guardian](#)

39 BBC, Izbori u Srbiji 2020: Šta sve mogu naprednjaci sa dvotrećinskom većinom u skupštini, 2020, [Izbori u Srbiji 2020: Šta sve mogu naprednjaci sa dvotrećinskom većinom u skupštini - BBC News na srpskom](#), accessed 20th March 2023

40 Zhou, Y, & Shen, L. Confirmation Bias and the Persistence of Misinformation on Climate Change. Communication Research, 49(4), 500–523, 2022 <https://doi.org/10.1177/00936502211028049>, accessed 07th April 2023

41 Burton, J. Cyber-Attacks and Freedom of Expression: Coercion, Intimidation and Virtual Occupation, Baltic Journal of European Studies, Tallinn University of Technology Vol. 9, No. 3 (28), 117-132

42 Burton, J. Cyber-Attacks and Freedom of Expression: Coercion, Intimidation and Virtual Occupation, Baltic Journal of European Studies, Tallinn University of Technology Vol. 9, No. 3 (28), 117-132

or individuals differ, however, it can be expected that a change in behaviour will be detected. Having in mind that cyberattacks usually extend to members of journalists' families, they might be more reluctant to cover a topic if they anticipate a cyberattack as a reaction. This means that a cyberattack does not necessarily need to occur, but it is enough that the target is aware of that possibility to achieve the desired result.<sup>43</sup> If this environment is nurtured over a longer period of time, media profession becomes associated with a wide range of negative sides, which can lead to a decrease in interest in journalism as a career.

In conclusion, one of the main consequences that cyberattacks and lack of efficient cybersecurity measures can have is related to self-censorship among media professionals. This can severely aggravate media pluralism and media diversity. Whereas AI has a higher impact on the right to be informed without interference, AI can also be identified as a contributing factor to a hostile environment towards freedom of expression and media freedoms.

## 2.2. Right to privacy

Right to privacy refers to protection of personal data and respect for the confidentiality of one's correspondence and communications.<sup>44</sup> It also encompasses right to be free from surveillance and

interception of our communications, unauthorised data processing, pornographic content, and others.<sup>45</sup> The three key parties in ensuring this right are citizens, governments, and business actors. Data security concerns have emerged by increasing the accessibility of Internet and by understanding the value of data to states and private companies. Companies' revenues and states' exercise of control over citizens are based on data.<sup>46</sup>

Implications that cybersecurity, AI and other similar digital technologies have on freedom of expression are intertwined with the right to privacy and other fundamental human rights. As explained, cyberattacks can be perceived twofold: as an attack on states' critical infrastructure and as an attack on an individual. While a cyberattack on critical infrastructure denies access to services, enables the governments in some efforts, they are also prone to lead to massive leaks of personal data, to track and to surveil target groups or individuals.<sup>47</sup> Some governments use cybersecurity to establish a higher degree of control over the internet and to further restrict rights.<sup>48</sup> The ability of public and private actors to have access to one's digital history, personal information, location, movements raises many privacy concerns. Facial recognition technologies, surveillance in various public and private spheres, coupled with the possibility of tracking and storing this

43 Ibid.

44 Privacy and data protection, Council of Europe, [Council of Europe Data Protection website - Data Protection \(coe.int\)](https://www.coe.int/en/web/privacy), accessed 10st March 2023

45 Leslie D et al. Artificial intelligence, human rights, democracy, and the rule of law: a primer. The Council of Europe, 2021

46 Introduction to digital rights, Share Foundation, 2021

47 Freedom on the Net 2022, Countering an Authoritarian Overhaul of the Internet, Freedom House 2023

48 Human Rights Watch, It's Time to Treat Cybersecurity as a Human Rights Issue : Cyber Heavyweights US and Russia Were Silent on Rights, 2020, <https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue>, accessed 05th March 2023

data concerns personal data protection. This can particularly be concerning in countries with restrictive tendencies, where governments could easily interfere with the one's autonomy and safety.<sup>49</sup> One of few examples of targeting an organisation due to its human rights work occurred in 2018, when Amnesty International reported that their staff member and a Saudi human rights activist were targeted by NSO-powered Campaign.<sup>50</sup> This spyware would allow full access to target's device, including gathering data and tracking the target,<sup>51</sup> which could endanger their lives and work.

In addition to cyberattacks, there are other AI-powered digital technologies that can interfere with right to privacy. In the following part of this subchapter, we will provide definitions and illustrative examples to some of those technologies, namely: surveillance (mass, private and private-state) and facial recognition technologies.

Privacy International explains that “**mass surveillance** involves the acquisition, processing, generation, analysis, use, retention or storage of information about large numbers of people, without any

regard to whether they are suspected of wrongdoing.”<sup>52</sup> Mass surveillance is based on the hypothesis that all gathered data could be useful to combat a hypothetical threat.<sup>53</sup> Systemic monitoring of people's lives provides unlimited data to the governments and private companies, which can further be used for various purposes.<sup>54</sup> OSCE has reported that this technology has been used to hinder work and investigations of journalists, human rights defenders attending protests have been identified, tracking and locating activists with dissenting views and whistle-blowers.<sup>55</sup> Russia and China are well-known for developing the finest surveillance technologies, however, surveillance is widely used in the entire world. The way it is used varies and defines the purposes of surveillance. Citizens Lab reported that only by assuming that one might be a subject to mass surveillance would lead to self-censorship.<sup>56</sup> Self-censorship can be analogically interpreted as refraining from any activity that would be otherwise pursued. For example, Russia is deploying mass surveillance technologies to track opposition protesters to their homes and to arrest them.<sup>57</sup> Furthermore, the US

---

49 Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Surveillance and human rights, A/HRC/41/35, 2019, 7

50 NSO-powered Campaign is a sophisticated commercial exploitation and spyware platform sold by an Israel surveillance vendor

51 Amnesty International, Amnesty International among targets of NSO powered campaign, 2018, <https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/>, accessed 07th April 2023

52 Mass surveillance, Privacy International, <https://privacyinternational.org/learn/mass-surveillance>, accessed 20st March 2023

53 Ibid.

54 Sekalala, S. et al, Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis, Health and Human Rights Journal, Volume 22/2, December 2020, 7 - 20, <https://www.hhrjournal.org/2020/12/analyzing-the-human-rights-impact-of-increased-digital-public-health-surveillance-during-the-covid-19-crisis/>, accessed 01st March 2023.

55 Pirkova, E. et al, Spotlight on Artificial Intelligence and Freedom of Expression-A Policy Manual, OSCE, 2021, 64

56 Knockel, J. et al, We Chat, They Watch How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus, CitizensLab, 2020, <https://citizenlab.ca/2020/05/we-chat-they-watch/>, accessed 18th February 2023

57 The Washington Post, Russia's surveillance state still doesn't match China. But Putin is racing to catch up, 2021, [Russia is growing its surveillance state but not everyone is monitored equally - The Washington Post](https://www.washingtonpost.com/technology/2021/04/01/russia-is-growing-its-surveillance-state-but-not-everyone-is-monitored-equally-the-washington-post/), accessed 01st April 2023

has used surveillance methods to track demonstrators of Black Lives Matter movement.<sup>58</sup> The motivation behind this surveillance is to restrict activities of the target groups and not to facilitate identification of criminal offenders, as it is usually stated.

**Facial recognition technologies** are the key factor that enable mass surveillance to be more alarming. Facial recognition is a tool relying on machine-learning to obtain identity matches through still images and videos displaying people's faces.<sup>59</sup> Another concern is that facial recognition could exacerbate discrimination and enable profiling, as facial recognition seeks to profile individuals based on different characteristics such as ethnicity, gender, race, nationality and other.<sup>60</sup> This could potentially lead to discrimination and to unlawful detention, restricted right to movement, right to personal integrity.<sup>61</sup> Having in mind that AI is not a neutral agent and is not free from bias but it is a tool that is data trained, it could easily be misused for identifying certain target groups based on certain characteristics.<sup>62</sup> Facial recognition

technologies do have high accuracy, however, this is not equally applicable to all demographics.<sup>63</sup> It is more likely that the default patterns will be associated with the common understandings of the majority,<sup>64</sup> and more false positives occur among people of colour, women, children and elderly.<sup>65</sup> African Americans are more likely to be misidentified in the US, whereas AI developed in Asia will more likely accurately identify Asian people than white people.<sup>66</sup> In 2018, South Wales Polices released data that about 92% of facial matches conducted as the 2017 Champions League Final were false positives, corresponding to a figure of 2,297 out of 2,470,<sup>67</sup> which supports the claim that facial recognition technologies cannot always be used for identification of criminal offenders as it often fails to do so. Lastly, Chinese law enforcement has deployed facial recognition with the aim to support "facial recognition to identify Uyghur/non-Uyghur attributes."<sup>68</sup> Therefore, it is important to carefully design facial recognition technologies, taking into account all the benefits and disadvantages it might bring.

58 ICNL, *Protesting in an Age of Government Surveillance*, 2023, [Protesting in an Age of Government Surveillance - ICNL](#), accessed 25th March 2023

59 Human Rights Watch, *Rules for a New Surveillance Reality*, 2019, <https://www.hrw.org/news/2019/11/18/rules-new-surveillance-reality>, accessed 15th March 2023

60 Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Surveillance and human rights*, A/HRC/41/35, 2019, 7

61 Human Rights Watch, *Rules for a New Surveillance Reality*, 2019, <https://www.hrw.org/news/2019/11/18/rules-new-surveillance-reality>, accessed 15th March 2023

62 Zuiderveen Borgesius, F. *Discrimination, artificial intelligence, and algorithmic decision-making*. Council of Europe, Directorate General of Democracy, 2018. <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decisionmaking/1680925d73>, accessed 05th March 2023

63 Najibi, A, *Racial Discrimination in Face Recognition Technology*, Harvard University, 2020, [Racial Discrimination in Face Recognition Technology - Science in the News \(harvard.edu\)](#), 07th April 2023

64 Human Rights Watch, *Rules for a New Surveillance Reality*, 2019, <https://www.hrw.org/news/2019/11/18/rules-new-surveillance-reality>, accessed 15th March 2023

65 Forbes, *Facial Recognition Violates Human Rights, Court Rules*, 2020, [Facial Recognition Violates Human Rights, Court Rules \(forbes.com\)](#), accessed 01st April 2023

66 The Atlantic, *Facial-Recognition Software Might Have a Racial Bias Problem*, 2016, [Facial-Recognition Software Might Have a Racial Bias Problem - The Atlantic](#), accessed 01st April 2023

67 Engadget, *Police face recognition misidentified 2,300 as potential criminals*, 2018, [Police face recognition misidentified 2,300 as potential criminals | Engadget](#), accessed 01st April 2023

68 The New York Times, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, 2019, [One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority - The New York Times \(nytimes.com\)](#), accessed 01st April 2023

Moreover, we can increasingly find private surveillance and private-state partnerships. Private sector acts as a seller, service-provider to many governments, due to their incentives, expertise and resources.<sup>69</sup> Providing governments data subtracted from users' devices and networks has also been a subject of discussion among human rights experts. Law enforcement agencies have increasingly been requesting data from social media platforms. Transparency reports of Apple have reported that in the period from July 2021 to December 2021, they provided data in 85% of requested cases.<sup>70</sup>

Privacy concerns are raised in many other areas, such as recruitment processes, healthcare, customer service, translation tools, home gadgets, toys and similar. This crosscutting digital realm is underregulated and interests of many stakeholders are influencing policy-makers. Lastly, collecting personal data, processing and repurposing of that data must be done in coherence to relevant legislation and upholding fundamental democratic values where every limitation of human rights must be necessary and proportionate to the aim.

### **2.3. Human rights-based approach to cybersecurity and AI**

UN defines the human rights-based approach (HRBA) as a conceptual

framework that is normatively based on international human rights standards and operationally directed to promoting and protecting human rights.<sup>71</sup> It seeks to analyse how are human rights discussed within the framework of cybersecurity and how to shift the focus from national security to human security. The Association for Progressive Communications defines a human rights-based approach to cybersecurity as *“putting people at the centre and ensuring that there is trust and security in networks and devices that reinforce, rather than threaten, human security. Such an approach is systematic, meaning that it addresses the technological, social and legal aspects together, and does not differentiate between national security interests and the security of the global internet.”*<sup>72</sup>

National security is placed at the centre of cybersecurity narrative.<sup>73</sup> Security can be approached in a positive and in a negative way. The negative sense of security concerns the absence of threats to fundamental human rights, while the positive sense refers to the measures and approaches that protect and enable individuals to freely and securely exercise their rights. Unfortunately, the positive aspect of security appears to receive little recognition in present-day discussions on cybersecurity. Governments have traditionally viewed security from a negative viewpoint, and as such, cybersecurity is

---

69 Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Surveillance and human rights, A/HRC/41/35, 2019

70 Apple Inc. Account Requests, <https://www.apple.com/legal/privacy/account.html>, accessed 01st March 2023

71 UN Development Sustainable Group, UNSDG | Human Rights-Based Approach, 25th March 2023

72 Association for Progressive Communications, 2020, [APC policy explainer: A human rights-based approach to cybersecurity](#) | Association for Progressive Communications, accessed 01st February 2023

73 Liaropoulos, A. A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia, *Journal of Information Warfare*, 14, 4, 2015 (PDF) [A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia](#), *Journal of Information Warfare*, 14, 4 (2015). (researchgate.net), accessed 20th March 2023

predominantly associated with preventing harm.<sup>74</sup> The prevailing understanding of what constitutes cybersecurity is focused on the state interests, territory, and infrastructure, rather than the individual.<sup>75</sup> This point of view is coming from pragmatic reasons, as security of these components are a prerequisite to enjoy human rights,<sup>76</sup> and from the fact that states provide its citizens with security.<sup>77</sup> The human element is considered as a part of the threat spectrum rather than a subject of security. This, in addition to the negative conception of security, have led to policies tailored to protect critical infrastructures and not to facilitate the ability of people to gain access to tools and resources of cyberspace.<sup>78</sup> From the perspective of cybersecurity, security does not merely refer to keeping people safe online, it shall have a facilitating role in empowering people to enjoy their rights, as long as they respect other people's human rights.<sup>79</sup>

Furthermore, human rights-based approach entails a detailed assessment of the introduced cybersecurity measures and their impact on both protection of cyberspace and on human rights. In this sense, every restriction should be proportionate, necessary and with a legitimate aim.<sup>80</sup> A cyber practice that

protects people from certain harm but at the same time violates their human rights beyond the level of proportionate and necessary, without a legitimate aim, cannot be assessed as a reasonable measure. This rule is applicable to restrictions in both online and offline space.

Cyberspace is a transnational domain attempting to balance the involvement of international, private stakeholders and states on one side, and various layers of interest on the other side. This domain is different from any other, hence it is a challenging task to safeguard human rights within this cyber realm.<sup>81</sup> Adopting a human rights-based approach increases the understanding of how human rights and security intersect and how their positions are intertwined. By understanding the position that humans have in the cyber realm and the reliance on cybersecurity, it is possible to identify practices and policies that are equally beneficial to both sides. Additionally, the definition of critical infrastructure must be interpreted in a manner that centers citizens, as well. Lastly, the necessity and scope of limiting human rights to mitigate security risks must be guided by principles that prioritise national security as a mean to provide a secure environment for citizens.

---

74 Ibid.

75 Pavlova, P. 'Human-rights based approach to cybersecurity: Addressing the security risks of targeted groups', *Peace Human Rights Governance*, 4(3), 391-418, 2020, [PHRG-2020-3-04.pdf \(padovauniversitypress.it\)](#), accessed 20th March 2023

76 Ibid.


77 Liaropoulos, A. A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia, *Journal of Information Warfare*, 14, 4, 2015 (PDF) [A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia, Journal of Information Warfare, 14, 4 \(2015\). \(researchgate.net\)](#), accessed 20th March 2023

78 Kovacs, A, Hawtin, D. (2013) 'Cyber Security, Cyber Surveillance and Online Human Rights', *Global Partners Digital, Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf (gp-digital.org)*, accessed 05th March 2023

79 Ibid.

80 Ibid.

81 Liaropoulos, A. A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia, *Journal of Information Warfare*, 14, 4, 2015 (PDF) [A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia, Journal of Information Warfare, 14, 4 \(2015\). \(researchgate.net\)](#), accessed 20th March 2023



Kosovo has made significant strides in developing its economy and infrastructure. However, the country still faces many challenges, including a lack of access to technology and limited resources to invest in cybersecurity and AI.





# Kosovo: policy and practices overview

Western Balkans region has made significant progress towards improving cybersecurity in the past years. Most countries in the region have established strategies and institutions to combat cyber threats, and important legislative measures have been initiated to regulate and protect cybersecurity. However, there is still room for improvement in terms of strengthening national and regional cybersecurity capacities, promoting cross-border cooperation and information sharing, and raising awareness among citizens and businesses.<sup>82</sup> As the digital transformation accelerates, cybersecurity is becoming increasingly essential for the stability, prosperity, and security of the Western Balkans region. Since declaring independence from Serbia in 2008, Kosovo has made significant strides in developing its economy and infrastructure. However, the country still faces many challenges, including a lack of access to

technology and limited resources to invest in cybersecurity and AI. Efforts to develop and regulate these areas have been tied to cooperation with the West, based on the best models and practices in EU and NATO. Furthermore, it is important to note that Kosovo's biggest challenges remain linked to its contested statehood. In post-war Kosovo there was a strong presence of international actors, for instance, the United Nations Interim Administration Mission in Kosovo (UNMIK) mission oversaw leading the country through developing institutions, economy, facilitating peace and security.<sup>83</sup> Since its independence, a discussion about the right to self-determination was sparked. This debate stems from the fact that Serbia consider Kosovo as an integral part of Serbian territory, and therefore, dispute its status as an independent country. Kosovo has gained support from major international and European countries, however, to this date 5 EU Member States did not recognise

---

82 Share Foundation, Regulatory Framework in the Field of Digital Rights Comparative Analysis: Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, Serbia, 2021, [Digital-rights-legal-analysis\\_EN-1.pdf](#) (sharefoundation.info), accessed 25th March 2023

83 United Nations Mission in Kosovo, [Mandate | UNMIK \(unmissions.org\)](#), accessed 07th April 2023

Kosovo's independence.<sup>84</sup> Furthermore, Kosovo is not a UN Member State as Russia<sup>85</sup> and China<sup>86</sup> are not willing to recognise Kosovo, due to their close ties with Serbia. Hence, Kosovo's status within international organisations such as NATO, EU and Council of Europe is disputed, as there is no uniform agreement on Kosovo's statehood.

Like many countries in the world and Western Balkan region, Kosovo is no exception when it comes to cyberattacks. Despite having taken critical steps,<sup>87</sup> Kosovo has been subjected to many cyberattacks since 2018. The most recent cyberattack was in September 2022 targeting Kosovo Telecom.<sup>88</sup> Additionally, Economic Bank, Kosovo's Independent Media Commission, HIB Petrol, Ministry of Economy, Kosovo Central Election Commission are only some of victims of cyberattacks in Kosovo. Targets of the attacks have been versatile and some of them had consequences for general public,<sup>89</sup> whereas some of the highlighted the vulnerability of the system.

Kosovo's international relations in cybersecurity are mainly based on agreements on bilateral cooperation. So far, bilateral agreements that include cyber

aspects are scarce and limited to police cooperation. Kosovo has signed agreements with Albania, Bulgaria, Italy, Montenegro, Switzerland, and Turkey. Cooperation with Albania is advanced by signing an ICT Cooperation Agreement and a Memorandum of Understanding on cooperation between the two national CERTs.<sup>90</sup>

Having in mind the widespread use of Internet, social media platforms, and the enhanced efforts of digitalisation, the risk of cyberattacks and of other forms of human rights violations are in rise. DataRe portal report that Kosovo has Internet penetration of 96.6% and 1.6 million Internet users in January 2023. 56.1% of the total population were active social media users whilst 58.1% of Kosovo's total internet user base used at least one social media platform. Kepios noted an increase of 0.2% of Internet users between 2022 and 2023.<sup>91</sup>

The next two sections will analyse the existing legislation and its implementation in Kosovo. A special attention will be paid to the newly adopted legislation which represent the umbrella piece of legislation. This will be followed by an analysis of existing practices and how legislation translates to implementation in Kosovo.

---

84 Al Jazeera, Which countries recognise Kosovo's statehood?, 2023, [Which countries recognise Kosovo's statehood? | Infographic News | Al Jazeera](#), accessed 07th April 2023

85 Written Statement of the Russian Federation to International Court of Justice, 2009, [15628.pdf \(icj-cij.org\)](#), accessed 07th April 2023

86 Written Statement of the People's Republic of China to the International Court of Justice on the Issue of Kosovo, 2009, [15611.pdf \(icj-cij.org\)](#), accessed 07th April 2023

87 Kosovo Has Undertaken Critical Steps in Cybersecurity, Says New Cybersecurity Capacity Maturity Model Assessment, The World Bank, 2020, [Kosovo Has Undertaken Critical Steps in Cybersecurity. Says New Cybersecurity Capacity Maturity Model Assessment \(worldbank.org\)](#), accessed 20th March 2023

88 BIRN, Kosovo to Establish Agency for Cyber Security Amid Recent Attacks, 2022, [Kosovo to Establish Agency for Cyber Security Amid Recent Attacks | Balkan Insight](#), accessed 15th March 2023

89 Cyberattack on Bank Ekonomik in Kosovo, Cybersecurity Ecosystem Report, Western Balkans: Emerging Cyber threats, PwC, 2022, 30, [PwC-Cybersecurity-Ecosystem-Report-WB.pdf \(isac-fund.org\)](#), accessed 20th March 2023

90 Cybersecurity Ecosystem Report, Western Balkans: Emerging Cyber threats, PwC, 2022, 30, [PwC-Cybersecurity-Ecosystem-Report-WB.pdf \(isac-fund.org\)](#), accessed 20th March 2023

91 DataRe portal, Digital 2023: Kosovo, 2023, [Digital 2023: Kosovo – DataReportal – Global Digital Insights](#), accessed 20th March 2023

### 3.1. Legislation

Kosovo has proceeded to adopt several laws central to setting ground for efficiently regulating cybersecurity. In 2022, Kosovo lawmakers have intensified their efforts to bridge the gap that has been present in the cyber legislative framework. A package consisting of a law, national strategy, and action plan are announced to be adopted. Several new institutions and units are foreseen to be established in the field of cybersecurity in Kosovo. The focus of this subchapter is on the Law on Cybersecurity and National Cybersecurity Strategy as they are the newest legislation put in place.

National Cybersecurity Strategy is envisaged to set the strategic objective within the time frame 2023-2027. A provision dedicated to balancing security and human rights is in place, primarily privacy, free access to information and other fundamental rights. It acknowledges that increased cybersecurity can be beneficial for exercising human rights in cyberspace. However, this has not been set as a specific objective of the Strategy. Strategy and the Action Plan are only available in draft versions and are to be adopted in 2023.<sup>92</sup>

The Law on Cybersecurity was adopted in early 2023 after being on hold for several years. National Cybersecurity Agency and a National Cyber Security Council will be established as the main institutions implementing and monitoring cybersecurity in Kosovo. This Agency is

established within the Ministry of Internal Affairs of Kosovo, whereas the Council will be an independent advisory body to the Government, other public and private stakeholders. As the Law was recently adopted, it remains to be seen how that will improve the cyber landscape in Kosovo. The State Cyber Security Training Centre within the Ministry of Defence will organise specialised trainings and certification programs for personnel engaged in the field of cyber security. A civil society representative clarifies of Kosovo opted for adopting one of the existing models, as this is a successful practice in many European countries.<sup>93</sup>

Cybersecurity experts deem that this law was necessary, but its effectiveness depends on how certain provisions will be interpreted. Another concern about its applicability is lack of capacities, which also extends to laws that were adopted before this one. It was noted by a cybersecurity expert that this Law predicts a realistic plan and will enhance the coordination and harmonization, however, the capacities are limited.<sup>94</sup> The Law strengthened the obligation of operators of essential services to report a cyber incident to the National Cybersecurity Agency. It lays out the requirements for the cyber incident to be qualified as having a “significant impact of the system or the continuity of the service”. It also sets the timeframe and the prescribed penalties if not adhered to. Moreover, it obliges the institution to inform the persons affected by the cyber incident, and if the persons

<sup>92</sup> Kosovo Draft Cybersecurity Strategy 2023-2027, Draft version v\_0.1 2022-12-30, 2022, [Anglisht-DRAFT-Strategjia-per-siguri-kibernetike\\_V2.0\\_06032023.DOCX \(live.com\)](#)

<sup>93</sup> Interview with Leonora Hasani, 16th March 2023

<sup>94</sup> Interview with Arianit Dobroshiti, 15th March 2023

are available, the institution shall notify the public.<sup>95</sup>

The main question is how the critical infrastructure will be defined within the scope of cybersecurity. As the Law on Critical Infrastructure has defined critical infrastructure in a wide manner and includes national monuments as one of its segments; the main criticism to Cybersecurity Law, by security expert and a representative of think tank, is that it did not provide a prioritisation of layers of critical infrastructure.<sup>96</sup>

The Law on the Protection of Personal Data is compliant with EU Commission's Directive 95/46/EC on the General Data Protection Regulation. It defines legal protection, institutional responsibilities for monitoring the legality of data processing and access to public documents, and sanctions related to the protection of personal data and privacy of individuals.<sup>97</sup> Prior to this, Kosovo had adopted other laws that are relevant to cybersecurity, however, limited progress has been made.<sup>98</sup> Key legislative acts include: Law on Prevention and Fight Against Cybercrime, Law on Information Society Services, Law on Electronic Communication, Law on Interception of Electronic Communications, Law on Critical Infrastructure.<sup>99</sup>

This subchapter provided a preliminary analysis of the new Law on Cybersecurity

and the National Strategy on Cybersecurity. The majority of conclusions were made based on conducted interviews with representatives of civil society and cybersecurity experts. As it is still early to anticipate the exact results this legislation will yield, we can conclude that Kosovo government had made a very important step forwards towards better cybersecurity protection.

## 3.2. Current challenges

This section focuses on the main issues flagged by cybersecurity and AI experts in Kosovo. It highlights practices aggravating right to privacy and freedom of expression, but also challenges that Kosovo is facing due to its partly recognition. The findings mainly rely on interviews conducted with various stakeholders as primary sources.

### 3.2.1. Cybersecurity challenges

The contested statehood reflects on Kosovo's position in cyberspace, consequently, Kosovo is not recognised in cyberspace and does not have its own domains. Currently, the most frequently used domain are .ks and .rks, but Internet traffic is usually conducted through servers in Albania and Serbia.<sup>100</sup> General public does not know through which server are

---

95 Law on Cybersecurity, 2023

96 Interview with Mentor Vrajolli, 16th March 2023

97 Cybersecurity and Human Rights in the Western Balkans: Mapping Governance and Actors, DCAF- Geneva Centre for Security Sector Governance, 2022, [CybersecurityHumanRightsWesternBalkans\\_EN\\_March2023.pdf \(dcaf.ch\)](#), accessed 18th February 2023

98 Interview with Mentor Vrajolli, 16th March 2023

99 National Cybersecurity Strategies in Western Balkan Economies: Kosovo, DCAF- Geneva Centre for Security Sector Governance, 2021, [NationalCybersecurityStrategiesWB\\_2021.pdf \(dcaf.ch\)](#), accessed 20th March 2023

100 Interview with Mentor Vrajolli, 16th March 2023

they browsing, and they cannot know whether the information flows have been disrupted.<sup>101</sup> As Kosovo does not have a central entry point to Internet traffic, it would very difficult for the government to implement policies that would restrict flow of information online.<sup>102</sup> On the other hand, a Kosovo cybersecurity expert explains that the lack of domain possession makes it possible for media that are based outside of Kosovo to host websites and represent Kosovo media and produce content under Kosovo domains.<sup>103</sup> This also applies to devices physically locally in Kosovo being registered as in Albania or Serbia. This has a spillover effect on processing incident reports, as incident reports concerning addresses in Kosovo are more likely to be administered in Albania or Serbia, rather than in Kosovo. Due to the established cooperation with Albania, they usually forward the incident reports to Kosovo, however, such cooperations is only achieved on a case-by-case bases with Serbia.<sup>104</sup> This makes the system prone to spread of disinformation and misinformation, as this grey zone status complicates its regulation.

Lack of recognition of Kosovo is interconnected with the exercise of digital rights, mainly of the right to be forgotten, as the foundation of this right is set in EU legislation. Right to be forgotten gives

individuals the right to ask to search engines to delete their personal data.<sup>105</sup> Despite Kosovo introducing and adopting corresponding legislation, this right can hardly be exercised without access to international courts.<sup>106</sup>

The Law of Cybersecurity has been processed very rapidly as there was interest to show that a serious progress has been in light of EU accession process. In that process, several key components have been omitted. Law on Critical Infrastructure should be the umbrella law, and all other laws, including Law on Cybersecurity, should be drafted in accordance with the Law on Critical Infrastructure. Implementation of the Law will indicate the contradictions between these two pieces of legislation.<sup>107</sup> One of the shortcomings is that the working group mainly included representatives from public institutions, industry, and foreign experts.<sup>108</sup>

The establishment of the National Cybersecurity Agency is disputed by cybersecurity experts, as there are many institutions that have a certain degree of competence in cybersecurity.<sup>109</sup> One of the proposed options was to expand the jurisdiction of national CERT and to appoint it as the central institution that would coordinate all cyber-related activities. KOS-CERT has only 2 persons employed

---

101 Ibid.

102 Interview with Arianit Dobroshiti, 15th March 2023

103 Interview with Mentor Hoxhaj, 16th March 2023

104 [Cybersecurity Capacity Review Republic of Kosovo 2020, 2020, cybersecuritycapacityassessmentfortherepublicofkosovo2019pdf \(ox.ac.uk\), accessed 20th March 2023](#)

105 Everything you need to know about the "Right to be forgotten", GDPR EU, [Everything you need to know about the "Right to be forgotten" - GDPR.eu](#), accessed 25th March 2023

106 Interview with Mentor Hoxhaj, 16th March 2023

107 Interview with Mentor Vrajolli, 16th March 2023

108 Interview with Arianit Dobroshiti, 15th March 2023

109 Ibid.

at the moment; hence their efficiency is very limited.<sup>110</sup> On the other side, the Agency will address the issue of overfragmentation of the competences among different institutions and will attempt to harmonise all laws and policies in place.<sup>111</sup> Lastly, the efficiency of the Agency solely depends on the human and financial resources that will be allocated to them. Access to data, monitoring of data and involvement of Ministry of Interior and Ministry of Defence in civilian aspects, public administration, should be limited.<sup>112</sup>

The Law on Cybersecurity did not include PPP *ex officio*, and the Councils are usually detached from the practice and might not have the adequate knowledge.<sup>113</sup> Therefore, there is an apprehension that the National Cyber Security Council might not prioritise private-public partnerships (PPP).<sup>114</sup> Private companies and individual experts do have the knowledge and skills to enhance cybersecurity in Kosovo. Institutions are lacking these capacities, and this can be mitigated by establishing PPPs in Kosovo with a focus on including local experts rather than foreign.<sup>115</sup> The pattern of using foreign expertise instead of local was translated to the working group of Law on Cybersecurity and Cyber Strategy.<sup>116</sup>

Despite the shortcomings and potential challenges that might occur, Kosovo government showed serious political will to improve protection in cyberspace by addressing cybersecurity institutionally and systematically. Having a piece of legislation

and institutions whose entire focus is on cybersecurity will improve this area, and harmonisation and other obstacles shall be mitigated accordingly.

### 3.3. Privacy and other challenges

This subchapter will cover privacy and other challenges associated with digital technologies that cannot be covered by cybersecurity. Privacy in this subchapter will be analysed through the lenses of mass surveillance, data leaks and other privacy violations conducted by public institutions, and other targeted data breaches in Kosovo. The findings mainly rely on interviews conducted with various stakeholders as primary sources.

When it comes to surveillance, it was noted that many CCTV cameras are overlooking public spaces have been installed in Kosovo. The law prescribes that every surveilled public area must have a sign indicating that the space is under surveillance. One of the cyberexperts, who is based in Prishtina, noticed that a frequent underpass in Prishtina is under surveillance but the authorities did not put a sign. It was revealed that the camera is owned and controlled by the police, however, regardless of notifying the competent authorities, a sign has not been put to this day.<sup>117</sup>

Another form of privacy violation is

---

110 Ibid.

111 Interview with Erblind Morina, 15th March 2023

112 Interview with Arianit Dobroshit, 15th March 2023

113 Interview with Mentor Vrajolli, 16th March 2023

114 Ibid.

115 Interview with Erblind Morina, 15th March 2023

116 Interview with Arianit Dobroshit, 15th March 2023

117 Interview with Arianit Dobroshit, 15th March 2023

publishing pictures on social media for locating purposes. Namely, there have been cases where the police publicly publish a picture of offenders, usually on Facebook. This has proven to be a method the police utilise to locate the offender.<sup>118</sup> It has been noted that this is the case associated with minor misdemeanours. This is a clear case of violating of data privacy by the authorities. Furthermore, this practice is translated into several media outlets, known for sharing personal information about the latest developments in Kosovo. There are no indications that AIK reacted, as they are continuing with the same practice.<sup>119</sup>

Taking into account that Kosovo is limitedly deploying certain surveillance methods and that it is relying on social media for identification purposes which corresponds to AI regulatory area, Kosovo has not made a stance on AI so far.<sup>120</sup> Nonetheless, some cooperation has been established with social media platforms and Kosovo country code has been added to Facebook.<sup>121</sup> The assessment conducted in 2020 indicated that Kosovo is at a start-up stage in media and social media. It highlights that the discussion about cybersecurity in this area is limited and should be enhanced.<sup>122</sup> Lastly, education and awareness-raising about the relevance of cybersecurity and AI is on a low level in Kosovo. However, SHARE Foundation did not report any breaches

related to blocking and filtering of content.<sup>123</sup> In this way, citizens will be encouraged to report all violations and harassments that occur online and urge the authorities to be more accountable and transparent.

Moving on to cybersecurity and its effects on privacy, it was highlighted by a Kosovar cybersecurity expert that data breach report and comprehensive data incidents reports are two elements to be reiterated in the following period. Despite being prescribed by law, these reports are rarely written and made public. Data breach report covers the details of the occurred breach and provides consequences of that breach for ordinary citizens, whereas the latter would provide deeper analyses of trends, patterns, and expectations.<sup>124</sup> One expert noted that there have been data breaches within public institutions which were not communicated nor announced to the public,<sup>125</sup> with the excuse that the front end was subject to the attack whilst the back end remained secure.<sup>126</sup> Moreover, responsible disclosure as an institute should be foreseen by the new Cybersecurity Law.<sup>127</sup> Responsible disclosure entails that when a bug within a system or network is discovered, it should be immediately reported to the competent institution. The person would receive a recognition and the bug would be able to be fixed in a timely manner. The current legislation does not foresee

---

118 Interview with Mentor Vrajolli, 16th March 2023

119 Ibid.

120 Interview with Arianit Dobroshiti, 15th March 2023

121 Interview with Mentor Hoxhaj, 16th March 2023

122 Cybersecurity Capacity Review Republic of Kosovo 2020, 2020, [cybersecuritycapacityassessmentfortherepublicofkosovo2019pdf \(ox.ac.uk\)](#), accessed 20th March 2023

123 SHARE Foundation database, [SHARE Monitoring \(bird.tools\)](#), accessed 29st March 2023

124 Interview with Mentor Hoxhaj, 16th March 2023

125 Interview with Mentor Hoxhaj, 16th March 2023

126 Interview with Mentor Vrajolli, 16th March 2023

127 Interview with Mentor Hoxhaj, 16th March 2023

this possibility.<sup>128</sup> Lastly, a cybersecurity capacity assessment conducted in 2020 graded this area as formative, which corresponds to an average grade in the assessment methodology.

Several cases of data leaks related to public institutions were observed in Kosovo. BIRN reported about a leak of personal data from website of the Central Election Commission,<sup>129</sup> petition against the Association of Serbian municipalities containing personal data left unsupervised,<sup>130</sup> personal data compromised during a cyberattack on Kosovo Telecom.<sup>131</sup> Reaction of the Commissioner of the Agency for Information and Privacy, AIP, has been assessed as limited. Taking into consideration the recent appointment of the Commissioner, one can expect their work to intensify and to be more proactive.

Share Foundation monitors violations of digital rights in all Western Balkans countries including Kosovo. The database covers the violations that occurred from March 2020 until July 2022 the latest. The chart below demonstrates the affected parties in all registered cases.<sup>132</sup>

In conclusion, the showcased figures show that citizens are the most affected when it comes to breaches online. In 117 out of 178 cases, Share Foundation flagged only citizens as the affected party, whereas public officials and state institutions the affected party in 52 cases. The attackers were online media in 106 cases. These figures support the claim that cybersecurity legal and policy framework should be oriented towards citizens as well, as it is shown that they are the most prone category to be affected by cyberattacks and data breaches. This entire cyber system is interlinked, and all these elements need to be at a satisfying level for Kosovo to have a functioning cybersecurity framework and implementation that is working in favour of national security and individual's security.

---

128 Ibid.

129 BIRN, In Kosovo and Albania, Personal Data Up for Grabs, 2022, [In Kosovo and Albania, Personal Data Up for Grabs | Balkan Insight](#), accessed 15th March 2023

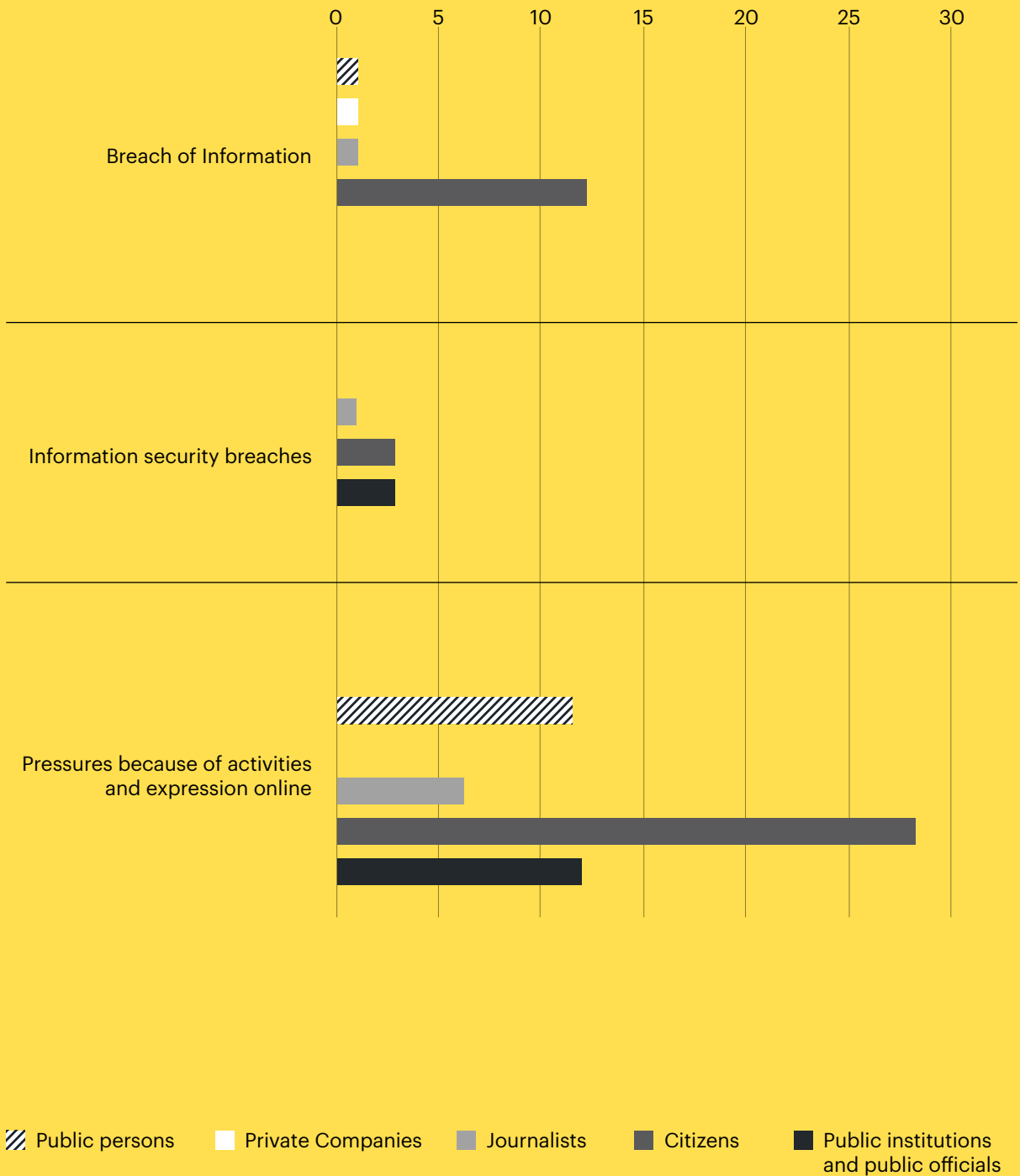
130 i Interview with Arianit Dobroshiti, 15th March 2023

131 BIRN, Kosovo to Establish Agency for Cyber Security Amid Recent Attacks, 2022, [Kosovo to Establish Agency for Cyber Security Amid Recent Attacks | Balkan Insight](#), accessed 15th March 2023

132 SHARE Foundation database, [SHARE Monitoring \(bird.tools\)](#), accessed 29st March 2023



**Figure 1:** Affected parties in monitored cases in Kosovo



## 4. Conclusions

One can argue that there is no ideal solution but only good practices that can mitigate the consequences, due to the complexity of the presented issues.<sup>133</sup> As new technologies are only emerging and the existing ones are advancing, there is no going back from what has been achieved in a technological sense, but we need to learn to mitigate the existing challenges. These must be evaluated and reassessed on an ongoing basis due to their progressive nature. On one hand, these processes include many stakeholders and interests, which are intertwining and potentially conflicting. On the other hand, Internet is a global platform which is accessible worldwide, and many different historical, political, social, linguistic and other contexts must be taken into account. This fragmentation and complexity are also reflected in the attempt of creating international legal regulations. States have the duty to protect, respect and promote human rights and only states can be held accountable for violations of human rights, therefore, the responsibility to protect and enable protection human rights in online spaces lays on the states. Generally enhancing the cooperation of states and Internet intermediaries should be conducted in a manner of legally obliging Internet intermediaries to report on means of operating, but the states also need to set up minimum requirements for transparency and cooperation.

Initiatives already taken, both internationally and nationally, recognised the role social media platforms are playing, as an enabler but also restrictor, thus contributing to the role of the governor of freedom of expression online. They seek to increase accountability and transparency of platforms.<sup>134</sup> Thus far, rules governing algorithmic decision-making are not sufficiently transparent, and states nor users are aware of what criteria are applicable to which situations and why. It is necessary to make available and accessible to the states documentation on models they deploy for content moderation and content curation. Users should be notified that the content available to them was a subject of content moderation and curation, including an option of opting out of automated decision-making.<sup>135</sup>

The research findings indicated that Kosovo is making steady progress in terms of legal and policy frameworks. Despite the significant progress, the level of success of the new Cybersecurity Law depends on its harmonisation with the Law on Critical Infrastructure and other laws that are already in place. The new package consisting of the Cybersecurity Law, Cyber Strategy and Action plan will advance cyber institutions and capacities in Kosovo. It has the capability to centralise this matter and

---

<sup>133</sup> Interview with Bojana Kostić, 07th March 2023

<sup>134</sup> Helberger, N. The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power, *Digital Journalism*, 8:6, 842-854

<sup>135</sup> Bukovska, B. Spotlight on Artificial Intelligence and Freedom of Expression, OSCE, 2020, 40

improve its efficiency. Furthermore, it was emphasised that Kosovo institutions lack capacities to address cybersecurity issues. This issue is expected to be addressed with the establishment of the National Training Centre. Kosovo does not lack cyber experts in private sector, however, the cooperation between private and public sector is limited. The question of PPP should be prioritised and the inclusion of local experts should be increased, hence the reliance of Kosovo on foreign expertise will be reduced. The research findings indicate that the main victims of cyberattacks in relation to privacy are ordinary citizens and that there is space for improvement of accountability and transparency of public institutions in case when a cyberattack occurs. Lastly, challenges that Kosovo is encountering are similar to those encountered in other Western Balkan countries but also worldwide. Despite Kosovo having a legal framework in place, it has been subject to several cyberattacks which has also occurred to other countries in the Western Balkans. Apart from the lack of the domain, Kosovo is in a similar position as the rest of the countries in the region when it comes to risks and challenges related to cybersecurity. Cooperation among the states in the region should be enhanced to increase efficiency in combatting these risks.

In conclusion, cybersecurity, AI, and human rights are two interconnected concepts that require careful consideration and balancing. Cybersecurity measures are necessary to protect against cyber threats, they must not be implemented at the expense of fundamental human rights, such as freedom of expression and privacy. The development and deployment of AI must be done in an ethical way that respects fundamental rights. This includes ensuring a fair and transparent decision-making process, avoiding bias and discrimination, protecting privacy and personal data, and upholding accountability and responsibility. Stable cooperation among governments, private companies and users is necessary to create a digital infrastructure that is secure, safe and respectful of human rights. It is important to reiterate that digital technologies are in place to facilitate our needs and not to restrict human rights, and both can be achieved simultaneously with the right policies and practices in place.

# 5. Recommendations

## **Kosovo government:**

- 🕒 ensure harmonisation of Cybersecurity Law with Law on Critical Infrastructure and other key legislation in Kosovo;
- 🕒 adopt the new National Cybersecurity Strategy and Action Plan that provides policy guidance to cybersecurity institutions, with a special emphasis on implementing a human rights-based approach;
- 🕒 develop and implement incident response plans to respond to any cybersecurity incidents and introduce appropriate sanctions;
- 🕒 improve digital infrastructure in Kosovo, including strengthening its position in cyberspace, introducing advanced programs to process and store data and form its own cloud;
- 🕒 foster a cybersecurity culture that starts from the top of an organisation and runs through all employees can help prevent cyberattacks;
- 🕒 invest in training and education programs for cybersecurity professionals, which can further facilitate the establishment of PPP;
- 🕒 work with other countries to enhance international collaboration in cybersecurity and AI, sharing threat intelligence, knowledge, and best practices;
- 🕒 initiate public awareness and education programs targeted at businesses and individuals should be conducted to promote awareness of cybersecurity risks, best practices, and responsible online behaviour;
- 🕒 promote AI in education, aiming at raising awareness of deploying responsible AI.

## **Private sector:**

- 🕒 support the establishment of PPPs through setting a voluntary exchange network,
- 🕒 liaise with academia and non-governmental representatives to increase their capacities in cybersecurity and AI.

## **Academia and non-governmental sector:**

- 🕒 enhance education on cybersecurity and AI across all levels to promote awareness,
- 🕒 foster collaboration with both private and public sectors, aiming to adopt a comprehensive approach towards cybersecurity and AI,
- 🕒 strengthen the capabilities to oversee public institutions in the domains of cybersecurity and AI.

# 6. Bibliography

## Academic articles

Bromell D, Regulating free speech in a digital age: hate, harm and the limits of censorship. Springer, 2022

Cains, M. et al, Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation, Risk Analysis: an official publication of the Society for Risk analysis, 2021, Author: Cains, Mariana G : Search (wiley.com), accessed 15<sup>th</sup> February 2023

Burton, J. Cyber-Attacks and Freedom of Expression: Coercion, Intimidation and Virtual Occupation, Baltic Journal of European Studies, Tallinn University of Technology Vol. 9, No. 3 (28), 117-132

McCarthy, J. What Is Artificial Intelligence?, Stanford University, 2007

Liaropoulos, A. A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia, Journal of Information Warfare, 14, 4, 2015 (PDF) A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia, Journal of Information Warfare, 14, 4 (2015). (researchgate.net), accessed 20<sup>th</sup> March 2023

Risse, M. The Fourth Generation of Human Rights: Epistemic Rights in Digital Lifeworlds, Carr Center for Human Rights Policy, Harvard Kennedy School, Harvard University, 2021

Helberger, N. The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power, Digital Journalism, 8:6, 842-854

Neuberger, C.. "Meinungsmacht im Internet aus Kommunikationswissenschaftlicher Perspektive." UFITA 82 (1): 53-68, 2018

Pavlova, P. 'Human-rights based approach to cybersecurity: Addressing the security risks of targeted groups', Peace Human Rights Governance, 4(3), 391-418, 2020, PHRG-2020-3-04.pdf (padovauniversitypress.it), accessed 20<sup>th</sup> March 2023

Sekalala,S. et al, Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis, Health and Human Rights Journal, Volume 22/2, December 2020, 7 - 20, <https://www.hhrjournal.org/2020/12/analyzing-the-human-rights-impact-of-increased-digital-public-health-surveillance-during-the-covid-19-crisis/>, accessed 01st March 2023.

Zhou, Y. & Shen, L. Confirmation Bias and the Persistence of Misinformation on Climate Change. Communication Research, 49(4), 500-523, 2022 <https://doi.org/10.1177/00936502211028049>, accessed 07<sup>th</sup> April 2023

## Legislation

Kosovo Draft Cybersecurity Strategy 2023-2027, Draft version v\_0.1 2022-12-30, 2022, [Anglisht-DRAFT-Strategjia-per-siguri-kibernetike V2.0\\_06032023.DOCX \(live.com\)](#)

Law on Cybersecurity, 2023

Universal Declaration of Human Rights, 1948

EU Regulatory framework proposal on artificial intelligence, [Regulatory framework proposal on artificial intelligence | Shaping Europe's digital future \(europa.eu\)](#)

European Commission, The EU Cybersecurity Act, [The EU Cybersecurity Act | Shaping Europe's digital future \(europa.eu\)](#)

Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Surveillance and human rights, A/HRC/41/35, 2019

Parliamentary Assembly of Council of Europe, Need for democratic governance, Resolution 2341, 2020, 1

Convention on Cybercrime: Special edition dedicated to the drafters of the Convention (1997-2001), Council of Europe, 2022, [1680a6992e \(coe.int\)](#)

European Parliament, Artificial Intelligence, 2023, [Artificial intelligence \(europa.eu\)](#)

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 Union legislative acts COM (2021)206, 2020

Written Statement of the Russian Federation to International Court of Justice, 2009, [15628.pdf \(icj-cij.org\)](#), accessed 07th April 2023

Written Statement of the People's Republic of China to the International Court of Justice on the Issue of Kosovo, 2009, [15611.pdf \(icj-cij.org\)](#), accessed 07th April 2023

## News articles

Al Jazeera, Which countries recognise Kosovo's statehood?, 2023, [Which countries recognise Kosovo's statehood? | Infographic News | Al Jazeera](#), accessed 07th April 2023

BBC, Izbori u Srbiji 2020: Šta sve mogu naprednjaci sa dvotrećinskom većinom u skupštini [What can progressive do with a two-third majority in the Assembly], 2020, [Izbori u Srbiji 2020: Šta sve mogu naprednjaci sa dvotrećinskom većinom u skupštini - BBC News na srpskom](#), accessed 20th March 2023

BIRN, In Kosovo and Albania, Personal Data Up for Grabs, 2022, [In Kosovo and Albania, Personal Data Up for Grabs | Balkan Insight](#), accessed 15th March 2023

BIRN, Kosovo to Establish Agency for Cyber Security Amid Recent Attacks, 2022, [Kosovo to Establish Agency for Cyber Security Amid Recent Attacks | Balkan Insight](#), accessed 15th March 2023

Engadget, Police face recognition misidentified 2,300 as potential criminals, 2018, [Police face recognition misidentified 2,300 as potential criminals | Engadget](#), accessed 01st April 2023

Forbes, Facial Recognition Violates Human Rights, Court Rules, 2020, [Facial Recognition Violates Human Rights, Court Rules \(forbes.com\)](#), accessed 01st April 2023

Forbes, The Value Of Search Results Rankings, 2017, [The Value Of Search Results Rankings \(forbes.com\)](#), accessed 01<sup>st</sup> April 2023

Jeremić et al, Facebook, Twitter Struggling in Fight against Balkan Content Violations, BIRN, 2021, [Facebook, Twitter Struggling in Fight against Balkan Content Violations | Balkan Insight](#), accessed 15<sup>th</sup> March 2023

The Atlantic, Facial-Recognition Software Might Have a Racial Bias Problem, 2016, [Facial-Recognition Software Might Have a Racial Bias Problem - The Atlantic](#), accessed 01<sup>st</sup> April 2023

The Guardian, Twitter deletes 20,000 fake accounts linked to Saudi, Serbian and Egyptian governments, 2020, [Twitter deletes 20,000 fake accounts linked to Saudi, Serbian and Egyptian governments | Twitter | The Guardian](#), accessed 01<sup>st</sup> April 2023

The New York Times, One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority, 2019, [One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority - The New York Times \(nytimes.com\)](#), accessed 01<sup>st</sup> April 2023

The Washington Post, Russia's surveillance state still doesn't match China. But Putin is racing to catch up, 2021, [Russia is growing its surveillance state but not everyone is monitored equally - The Washington Post](#), accessed 01<sup>st</sup> April 2023

## Reports

Knockel, J. et al, We Chat, They Watch How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus, CitizensLab, 2020, <https://citizenlab.ca/2020/05/we-chat-they-watch/>, accessed 18th February 2023

Najibi, A, Racial Discrimination in Face Recognition Technology, Harvard University, 2020, [Racial Discrimination in Face Recognition Technology - Science in the News \(harvard.edu\)](#), 07<sup>th</sup> April 2023

Amnesty International, Amnesty International among targets of NSO powered campaign, 2018, <https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/>, accessed 07th April 2023

Human Rights Watch, Rules for a New Surveillance Reality, 2019, <https://www.hrw.org/news/2019/11/18/rules-new-surveillance-reality>, accessed 15th March 2023

Association for progressive communication, Why cybersecurity is a human rights issue, and it is time to start treating it like one, 2022, <https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one>, accessed 01<sup>st</sup> February 2023

Association for Progressive Communications, 2020, [APC policy explainer: A human rights-based approach to cybersecurity | Association for Progressive Communications](#), accessed 01st February 2023

Bukovska, B. Spotlight on Artificial Intelligence and Freedom of Expression, OSCE, 2020

Kostić, B. AI traps and media diversity: mind the loopholes, Media Diversity Institute, 2021, <https://www.media-diversity.org/artificial-intelligence-traps-and-media-diversity-mind-the-loopholes/>, accessed 01st February 2023

## BALANCING CYBERSECURITY, ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS:

Kostić, B. & Sindere, C. Responsible AI, Council of Europe, 2022

Cyberattack on Bank Ekonomik in Kosovo, Cybersecurity Ecosystem Report, Western Balkans: Emerging Cyber threats, PwC, 2022, 30, [PwC-Cybersecurity-Ecosystem-Report-WB.pdf \(isac-fund.org\)](#), accessed 20th March 2023

Cybersecurity Ecosystem Report, Western Balkans: Emerging Cyber threats, PwC, 2022, 30, [PwC-Cybersecurity-Ecosystem-Report-WB.pdf \(isac-fund.org\)](#), accessed 20th March 2023

Cybersecurity and Human Rights in the Western Balkans: Mapping Governance and Actors, DCAF- Geneva Centre for Security Sector Governance, 2022, [CybersecurityHumanRightsWesternBalkans\\_EN\\_March2023.pdf \(dcaf.ch\)](#), accessed 18th February 2023

Cybersecurity Capacity Review Republic of Kosovo 2020, 2020, [cybersecuritycapacityassessmentfortherepublicofkosovo2019pdf \(ox.ac.uk\)](#), accessed 20th March 2023

DataRe portal, Digital 2023: Kosovo, 2023, [Digital 2023: Kosovo – DataReportal – Global Digital Insights](#), accessed 20th March 2023

Human Rights Watch, It's Time to Treat Cybersecurity as a Human Rights Issue : Cyber Heavyweights US and Russia Were Silent on Rights, 2020, <https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue>, accessed 05th March 2023

Digital Guardian, What is Cyber Security? Definition, Best Practices & Examples, 2022, <https://www.digitalguardian.com/blog/what-cyber-security>, accessed 05th March 2023

Everything you need to know about the “Right to be forgotten”, GDPR EU, [Everything you need to know about the “Right to be forgotten” - GDPR.eu](#), accessed 25th March 2023

Freedom on the Net 2022, Countering an Authoritarian Overhaul of the Internet, Freedom House 2023

ICNL, Protesting in an Age of Government Surveillance, 2023, [Protesting in an Age of Government Surveillance - ICNL](#), accessed 25th March 2023

Introduction to digital rights, Share Foundation, 2021

Kosovo Has Undertaken Critical Steps in Cybersecurity, Says New Cybersecurity Capacity Maturity Model Assessment, The World Bank, 2020, [Kosovo Has Undertaken Critical Steps in Cybersecurity, Says New Cybersecurity Capacity Maturity Model Assessment \(worldbank.org\)](#), accessed 20th March 2023

Kostić B, Sindere C, Responsible Artificial Intelligence, Council of Europe, 2022

Kovacs, A, Hawtin, D. (2013) ‘Cyber Security, Cyber Surveillance and Online Human Rights’, Global Partners Digital, [Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf \(gp-digital.org\)](#), accessed 05th March 2023

Leslie, D. et al. Artificial intelligence, human rights, democracy, and the rule of law: a primer. The Council of Europe, 2021

National Cybersecurity Strategies in Western Balkan Economies: Kosovo, DCAF- Geneva Centre for Security Sector Governance, 2021, [NationalCybersecurityStrategiesWB\\_2021.pdf \(dcaf.ch\)](#), accessed 20th March 2023

Pirkova, E. et al, Spotlight on Artificial Intelligence and Freedom of Expression-A Policy Manual, OSCE, 2021

Share Foundation, Regulatory Framework in the Field of Digital Rights Comparative Analysis: Albania, Bosnia



and Herzegovina, Kosovo, Montenegro, North Macedonia, Serbia, 2021, [Digital-rights-legal-analysis\\_EN-1.pdf \(sharefoundation.info\)](#), accessed 25<sup>th</sup> March 2023

UN Development Sustainable Group, [UNSDG | Human Rights-Based Approach](#), accessed 25<sup>th</sup> March 2023

White Paper On Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final

Zuiderveen Borgesius, F. Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, Directorate General of Democracy, 2018 <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decisionmaking/1680925d73>, accessed 05<sup>th</sup> March 2023

## Websites

Apple Inc. Account Requests, <https://www.apple.com/legal/transparency/account.html>, accessed 01<sup>st</sup> March 2023

Freedom Online Coalition website, 2022, <https://freedomonlinecoalition.com/members/>, accessed 01<sup>st</sup> March 2023

Geneva Internet Platform DigWatch, UN OEWG, [UN OEWG in 2023 - DW Observatory \(dig.watch\)](#), accessed 29<sup>st</sup> March 2023

IBM Cloud, <https://www.ibm.com/topics/artificial-intelligence>, accessed 27<sup>st</sup> February 2023

Mass surveillance, Privacy International, <https://privacyinternational.org/learn/mass-surveillance>, accessed 20<sup>st</sup> March 2023

Privacy and data protection, Council of Europe, [Council of Europe Data Protection website - Data Protection \(coe.int\)](#), accessed 10<sup>st</sup> March 2023

SHARE Foundation database, [SHARE Monitoring \(bird.tools\)](#), accessed 29<sup>st</sup> March 2023

UN Office for Disarmament Affairs, Group of Governmental Experts, [Group of Governmental Experts – UNODA](#), accessed 27<sup>st</sup> February 2023

United Nations Mission in Kosovo, [Mandate | UNMIK \(unmissions.org\)](#), accessed 07<sup>th</sup> April 2023



## About the author

**Imane Bellaadem** is human rights defender and activist from BiH. She completed her BA in Law and a MA in human rights and democracy at the University of Sarajevo. Currently, Imane is working on issues concerning civil and political rights in the region, environment for human rights defenders and freedom of expression. Her interests are civil rights, minorities, and environmental human rights.



