

# Artificial Intelligence Regulation in the Areas of Data Protection, Information Security, and Anti-discrimination in Western Balkan Economies

Djordje Krivokapić\*, Ivona Živković\* and Andrea Nikolić\*

\*Faculty of Organizational Sciences, University of Belgrade, Belgrade, Serbia  
djordje.krivokapic@fon.bg.ac.rs

**Abstract** - In order to improve trust related to the implementation of artificial intelligence (AI), European Union (EU) institutions are in the final stages of developing an ethical and legal framework. In the meantime, Western Balkan (WB) economies (Albania, Bosnia and Herzegovina, North Macedonia, Montenegro, Serbia and Kosovo) are pushing for the implementation of advanced information technologies and artificial intelligence, particularly in the public sector. This paper aims to provide an overview of regulatory approaches toward AI in WB economies, which are in process of EU integration but usually do lack institutional capacities and need further strengthening of rule of law. The paper will firstly introduce the concept of regulation and the challenges of the regulability of IT and AI. Secondly, the paper will map key actors and stakeholders in WB and analyze the development of strategic documents, ethical frameworks, and legal regulations in the area of AI. Thirdly the paper will briefly compare the existing regulatory framework of WB economies in the areas of Data Protection, Information Security, and Anti-discrimination and its applicability to the implementation of AI technologies. Lastly, by presenting key principles of the EU approach to the regulation of AI the paper will provide recommendations for Western Balkan economies.

**Keywords** - *Artificial Intelligence; Western Balkan Economies; Ethics; Legal Regulation*

## I. INTRODUCTION

In order to introduce the concept of regulation and challenges of regulability of informational technologies (IT) and artificial intelligence (AI) in Western Balkan (WB) economies, we should provide background information on the use of advanced technologies in WB economies, by presenting existing research conducted by various actors that will be briefly described in rows below. By analyzing existing data and rankings we wanted to get an understanding of how the economies observed rank globally and regionally, and if some conclusions can be drawn - e.g. which economy can be deemed to be the frontrunner and which is continuously ending up at the bottom of rankings, i.e. are there any significant differences in economies' readiness for implementation of AI and advanced technologies.

Unfortunately, most of the existing research excludes at least one economy, usually, it being Kosovo.

Government AI Readiness Index [1] by Oxford Insights draws on 10 dimensions (among which are Digital Capacity, Data Availability and Data Representativeness, presented in graphs below). In total 172 countries are ranked and Kosovo is not included in the ranking. The world average total score is 44.25 and 4 economies from the WB region have lower than average scores - Montenegro (70th place- 43,664), North Macedonia (73rd- 42,995), Albania (85th- 39,991) and Bosnia and Herzegovina (BiH) (100th- 36,250). Only Serbia (46th- 53,431) has a higher than average score. GovTech Maturity Index [2] measures digital transformation in the public sector. By analyzing these criteria we can conclude that Kosovo and Bosnia and Herzegovina are coming at the bottom of the rankings. North Macedonia is not included in the ranking. Network Readiness Index 2021 [3] ranks a total of 130 economies and represents a composite measure of four dimensions - Technology, People, Governance and Impact. Once again Serbia (57th) has the highest rank of all observed economies, right behind is Montenegro (62nd), followed by North Macedonia (64th). The lowest rank among the observed economies is noticeable with Albania (80th) and BiH (86th place). Kosovo is not included in the ranking.

It can be concluded that Serbia seems to be the frontrunner in terms of its readiness for the implementation of advanced technologies. On the other hand, it can be said that differences between other economies included in the research are often very small, and sometimes even non-existent. However, it is important to note that certain economies (usually it being BiH) trail behind and are consistently ranked the worst, while others are often excluded (Kosovo). Overall, when it comes to their readiness for the implementation of advanced technologies, there is much room for improvement.

## II. CONTEXT

In many public sectors tendencies for digitization of activities and services are increasingly present. They are

mostly trying to keep up and go beyond just traditional administrative services offered in digital form (e-government). Economies of WB are following suit not just in implementing e-government, but also in introducing advanced technologies such as artificial intelligence (AI) through existing and new services, often partnering with global ICT giants such as Google or Microsoft. The economies observed in this report show various tech tools being used by public sector actors, with the most impactful on human rights and social processes being the ones used for surveillance, public order and safety and healthcare.

#### *A. Surveillance, public order and safety*

Most governments, either those with a democratic rule or authoritarian regimes, are compassionate when it comes to the advances and proliferation of surveillance technologies, particularly those that rely on the processing of biometric personal data [4]. To provide public peace and order, under the excuse of creating a “crimeless society”, investigating crimes are today more technologically equipped than ever before [5]. In circumstances where democracy is “under siege” and world freedom is in decline for the 15th consecutive year, intrusive surveillance technologies can only intensify these negative trends [6]. When it comes to WB, one of the best examples of dangerous technology in the hands of a non-democratic government is the “Safe Society” project in Serbia, which entails the use of an advanced video-surveillance system [7] in the country’s capital Belgrade, announced in early 2019 [8]. The technical partner for this project is the Chinese tech giant Huawei, as part of wider cooperation between the governments of Serbia and China. There was no prior public debate on whether this kind of surveillance system, most notably with facial recognition capabilities, is needed in Belgrade and what would be the social effects of introducing it. According to documents obtained by SHARE Foundation [9] from the Commissioner for Information of Public Importance and Personal Data Protection, Serbia’s independent data protection authority, the Ministry of Internal Affairs will use 8100 cameras of different types, i.e. pole and vehicle-mounted cameras, eLTE terminal devices and body cams for police officers.

“Thousands of Cameras”, a citizen initiative led by SHARE Foundation, has been fighting the system since it was announced, arguing that there is no legal basis for the use of biometric surveillance technologies [10] in line with Serbian law and that it would have serious implications for freedoms enjoyed in public spaces like streets, parks and squares. In the autumn of 2021, a Draft Law on Internal Affairs [11] was presented by the Ministry of Interior, inter alia to legalize the use of biometric surveillance by the Serbian police. However, after strong opposition from the civil society [12] and the international community, the draft was withdrawn from the procedure [13] because of upcoming elections [14], which are to be held in April 2022. There are more similar cases of governments raising technical capabilities for law enforcement purposes in the Western Balkans region. Another example is the “Safe City”

project in Bosnia and Herzegovina, namely in its Republika Srpska entity, mostly populated by Serbs and with close political ties to Serbia. According to media reports [15] from 2020, local communities across Republika Srpska received a new video-surveillance system for their public spaces. Republika Srpska internal affairs representatives claimed however that the installed cameras allegedly only have “face detection” [16] and not facial recognition capabilities, as well as automatic vehicle license plate [17] recognition for detecting unregistered vehicles.

#### *B. Healthcare*

During the COVID-19 pandemic one of the significant steps made by governments were investing in health infrastructure and implementing tech solutions to help fight the biggest global crisis of the 21st century. In WB economies the pandemic also instigates governments to digitally transform diverse existing healthcare services and offer new ones, such as COVID-19 green certificates. Nonetheless, a variety of events have shown that implementation is not always on the right side of personal data protection and information security standards.

There are several examples where governments have designed mobile apps to reduce the spread of the coronavirus, for example notifying citizens when they have been in contact with an infected person or obtaining other health-related information, such as Koronavirus MK in North Macedonia, or My EU Digital Green Certificate in Serbia. One of the concerns with the usage of technology to undertake the pandemic in the WB was the health data breaches. For instance, the database for pandemic-related data in Serbia [18], was publicly available on a website of a health institution for 8 days. During that time, the page with the published credentials was indexed by Google, meaning that anyone could access it via a simple search. Further investigation of the incident by the Commissioner for Data Protection had shown that the institutions tasked with maintaining and controlling the system lacked even some of the basic data protection measures, for which the Commissioner issued a warning [19] to the Institute for Public Health of Serbia, the data controller of the system. We find a similar situation in Montenegro, where the government published data of people who were given mandatory self-isolation orders to deter them from breaking the quarantine rules [20]. NGO Civic Alliance challenged the practice before the Constitutional Court of Montenegro, which ruled in their favour. The Government deleted the personal data from its website, but some of the citizens who were on the mandatory self-isolation list decided to sue the state for breaching their rights [21].

It seems that the governments of the WB economies are quite willing to procure and implement AI and advanced technologies, however, it is often done with human rights considerations and data protection, information security and anti-discrimination standards as an afterthought. As the digitization of government services and new avenues for exploration of applying technology is going to go further, these issues can only complicate matters, especially in the context of

cross-country merging of information systems, as was recently announced [22] within the Open Balkan Initiative [23] between Serbia, Albania and North Macedonia. Another area with potential dangers for human rights when it comes to applying AI and advanced technologies in the public sector is the judiciary.

### C. *Key actors and stakeholders*

By analyzing strategic documents and AI architectures in WB economies we came to a unifying conclusion: Most economies still haven't developed a solid network of actors and stakeholders who can deal with the implementation of AI systems. However, there are some differences between economies in terms of actors involved in the process of developing AI systems. Most of these actors are representatives of the public sector. To be more specific, the greatest stimulus for the development of these systems comes from national governments and ministries.

In Serbia, most of the actors in charge of this process are related to the Serbian government such as the Ministry of Education, Science and Technological Development, and the Government of the Republic of Serbia. We have also identified the existence of two main R&D Funds in this area: the Science Fund and Innovation Fund. Serbia has also developed AI Architectures such as the State Center for Data Management and Storage, Center for the Promotion of Science, Vojvodina ICT Cluster and Institute for Artificial Intelligence of Serbia.

The greatest efforts in the process of developing and implementing AI and advanced technologies in North Macedonia are also related to the Government and the Fund for Innovation and Technological Development. However, the primary coordinator of all digital-related activities is the Ministry of Information Society and Administration.

The digital agenda in Montenegro is primarily set by the government and its dedicated bodies such as the Ministry of Public Administration, Digital Society and Media, and Ministry of Education, Science, Culture and Sports. Secondly, a part in setting the digital agenda is also played by several Montenegrin ICT companies, mainly through their umbrella body – ICT Cortex, which aims to contribute to and foster the digital development and transformation in Montenegro, and to promote the Montenegrin ICT scene in the international level. Other worthy mentions are the Digital Transformation Committee and the University of Montenegro and master studies of the study program Computers of the Faculty of Electrical Engineering.

In Kosovo among Government actors, we can point out the Agency of Information Society, the Ministry of Internal Affairs and the Ministry of Economy. There are also the Information and Privacy Agency (AIP), TAX Administration Office, Public Procurement Regulatory Commission, and Kosovo Judicial Council.

In Albania, we have also faced a serious lack of information about the process of developing and

implementing AI and advanced technologies in the public sector. Nevertheless, there are several actors in the field of AI that we identified in Albania - the Albanian institute for safe AI, Albania Artificial Intelligence, AADF (AI for Youth program), and the National Agency for Information Society which can be considered a leader in setting the digital agenda in Albania.

Bosnia and Herzegovina hasn't done much in the process of developing and implementing AI and advanced technologies in the public sector and we can't identify any relevant actors or stakeholders. In such a low-level competition, law enforcement is probably a champion as it has occasional updates on the technologies it uses. For instance, legislation on personal data protection and intellectual property rights has been adopted at the state level, while the remainder of the rules is predominately established on the level of entities.

Observing all the analyzed economies and the general situation in them when it comes to mandating to deal with the implementation of advanced technologies, and their capacities, we could say that the greatest efforts have been made by the national governments. In all analyzed economies, except for BiH, governments, relevant ministries and state agencies are responsible for the implementation of changes and processes related to advanced technologies and AI. In Montenegro and Serbia, we have noticed a certain level of cooperation between the private and public sectors. In six out of ten economies we have identified representatives of CSO and the private sector. However, we cannot say that any particular economy has developed a reliable network of actors to deal with the implementation of advanced technologies and AI.

### D. *Analysis of strategic documents*

In a process of analyzing strategic documents we came to the conclusions that Serbia is the only economy from Western Balkan region that has developed National strategy in the area of AI. Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025 [24] assigns priority in areas of education and science, the economy, and the public sector. All other analyzed economies don't have any type of strategic document that regulates the area of AI or advanced technologies. However, certain differences are identified among economies of the WB region. In Montenegro we noticed some positive changes, especially in the last year, mostly initiated by the Government. These changes are primarily in the domain of implementation of new ideas and raising the awareness about the importance of specific regulation of this field. The increase of interest among Government and CSO actors, compared to the previous period, is noticeable in both North Macedonia and Kosovo, but there are still no indications that the development of a strategic document is being considered at all. The most inconvenient situation regarding the beginning of the development of an AI strategy is in Albanian and BIH. Considering the poor network of actors and stakeholders who would potentially be involved in development of such a document, with the complete absence of incentives from

the governments, we can assume that the development of such documents will wait.

#### *E. Ethical frameworks*

Due to the fact that many WB economies, with the exception of Serbia, do not have developed strategic documents in the area of AI, and that most have not taken even pioneering steps in terms of adopting special regulations in this area, they also do not have ethical guidelines for the implementation of AI. As we already mentioned, Serbia is the only economy in WB that has developed strategic documents in the field of AI. As a part of that strategic regulation Serbia has also developed an ethical framework addressing specific ethical issues and the protection of the rights of individuals in the process of developing and applying AI. There are special chapters that pay special attention to the legal framework (3. Link to existing policies and legal framework, 4.3.1 Regulatory framework). In Chapter 4.4 The Individual and Society, a special focus is placed on ethical issues and the protection of the rights of individuals. One of the special goals of the strategy is the ethical and safe use of AI.

### III. REGULATORY FRAMEWORK OF WESTERN BALKAN ECONOMIES IN CRITICAL AREAS

This section will address the existing regulatory framework of WB economies in the areas of Data Protection, Information Security, and Anti-discrimination and its applicability to the implementation of AI technologies.

#### *A. Data Protection Regulation*

Data Protection Legal Framework is very important as every AI project gathers and processes a certain amount of data [25]. Thus, governments must ensure that their data protection regulation is on satisfactory level, meaning that sufficient and quality data is ethically processed by AI if needed.

In both EU countries and WB economies there has been a lot of attention drawn to the area of Data Protection and how personal data is processed. In that sense, progress was made in relation to legal regulation of data protection.

North Macedonia is the only WB economies that has a national data protection strategy currently in place (for years 2017-2022) [26]. In Serbia, a working group is formed to devise a new data protection strategy, because the current one is outdated [27] and corresponds to the previous data protection law from 2008. Also, Albanian data protection authority previously announced that Albanian data protection strategy for years 2021-2023 was to be adopted [28], but this is yet to happen. Although there are no data protection strategies in place, many of these economies' data protection authorities' annual working plans do include certain strategic steps to take and tasks to fill-in.

Further, North Macedonia, Serbia and Kosovo have adopted new data protection legislation which is largely

harmonized with GDPR. On the other hand, a draft of the new data protection law harmonized with GDPR is yet to be adopted in Montenegro [29], while in Albania a consultation process with the goal to adopt a new data protection law is undergoing. Other economies have previous data protection laws in place which were adopted many years prior to GDPR. However, many of these older laws do honor some of the most important GDPR principles but still lack many of GDPR institutes.

Economies that have harmonized their legislation with GDPR have the obligation to adopt a Data Protection Impact Assessment (DPIA) in certain cases of processing and to accordingly adopt guidelines regarding the conduction of DPIA. On the contrary, economies that have not harmonized their national legislation with GDPR (including Albania, Montenegro, Bosnia & Herzegovina) do not have the obligation to conduct DPIA. So, some economies that had the obligation to enact the guidelines, listed the examples in which DPIA is necessary. Such examples mostly include profiling, automated-decision making, using new technologies (such is artificial intelligence) for processing or using possibilities which will serve to analyze or foresee person's economic situation, health, interests, behaviors, location or movement, tracking location or person's behavior in systematic processing communication data generated by using phone, internet or other communication means etc. The issue here is whether the controllers engaging in the processing activities actually possess adequate knowledge to conduct a proper DPIA. For instance, the Serbian Ministry of Foreign Affairs has rendered a DPIA for processing which was to include the installation of facial recognition cameras around Belgrade. The DPIA was submitted to the Serbian data protection authority, which issued an Opinion stating that DPIA did not show the legal grounds for such processing, along with other irregularities.

#### *B. Information security Regulation*

All WB economies have adopted national information security strategies [30], except Bosnia & Herzegovina that only have a national Strategy for Establishment of CERT, adopted back in 2011 [31], which covers some of the information security issues.

Serbia and Albania have adopted information security laws which are mostly harmonized with the EU NIS Directive. However, both of these national laws do have some differences in comparison to the NIS directive. For example, Serbian law applies to a broader scope of entities in comparison to the NIS Directive, and its partial focus is on crypto security and protection from compromising electromagnetic radiation, which are not regulated by NIS directive.

On the other hand, Bosnia & Herzegovina currently does not have an overarching information security law on a national level, but the draft of a new information security law is to be adopted in near future. The similar case is with North Macedonia, which does not have an overarching information security law, but the draft of the future information security law harmonized with NIS

Directive is to be adopted in the near future. As for Montenegro, the matter of information security is divided into three main laws: Law on Information Security, Law on Determining and Protecting the Critical Infrastructure and Law on Data Secrecy, which are partially aligned with the NIS Directive. Kosovo's legislation is not harmonized with the NIS Directive.

### C. *Anti-discrimination Regulation*

All of the WB economies show similar levels of compliance with EU anti-discrimination legislation. Namely, each of the WB economies ratified all major human rights conventions and have adopted their own anti-discrimination laws. However, majority of them does not mention AI in any of discrimination related legislation, while Serbia's Strategy for the Development of AI recognizes the risks of it potentially being discriminatory and the Action Plan [32] for its implementation prescribes certain activities related to preventing discriminatory AI practices.

When it comes to discussing legislation, there are two questions that should be taken in consideration when discussing the readiness of current anti-discrimination legislation for the implementation of AI technologies. The first one is the question of different levels of enforcement of existing laws. The second is the question can the current EU equality directives fully tackle digital forms of discrimination, especially if we are aware of the complexity of human-machine relationship that might bring more confusion around concepts like direct or indirect discrimination. In other words, the main dilemma here is the current EU anti-discrimination legal framework satisfactory and providing enough room for interpretation regarding AI?

TABLE I. Key actors and AI Related Legal Framework in WB economies

	<i>Key actors</i>	<i>AI Related Legal Framework</i>
Albania	Albanian institute for safe AI; Albania Artificial Intelligence, AADF (AI for Youth program); National Agency for Information Society	Lack of any specific legal regulation on AI
Bosnia and Herzegovina		Lack of any specific legal regulation on AI
Kosovo	Agency of Information Society; Information and Privacy Agency (AIP); TAX Administration Office; Public Procurement Regulatory Commission	Lack of any specific legal regulation on AI

Montenegro	Ministry of Public Administration; Digital Society and Media; Ministry of Education, Science, Culture and Sports; ICT Cortex; Digital Transformation Committee University of Montenegro	Lack of any specific legal regulation on AI
North Macedonia	Fund for Innovation and Technological Development; Ministry of Information Society and Administration	Lack of any specific legal regulation on AI
Serbia	Ministry of Education, Science and Technological Development Government of the Republic of Serbia; Science Fund Innovation Fund; State Center for Data Management and Storage; Center for the Promotion of Science; Vojvodina ICT cluster Institute for Artificial Intelligence of Serbia	Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025

## IV. CONCLUSION

Western Balkan economies are obliged to align their national legislations with the EU *acquis communautaire*. Thus, WB economies have the obligation to fully harmonise their personal data protection, information security and anti-discrimination legislation with the EU *acquis* and adapt them accordingly in terms of challenges posed by technological advancements. Some WB economies have already done so, but still have to improve their laws and to strengthen their institutional capacities to improve those laws.

On the other hand, EU member economies seem to be more ready for the implementation of AI/advanced technologies, while WB economies lack capacities for their adequate implementation. However, irrespectable of economies' readiness to successfully regulate AI, there is a real struggle to implement AI solutions in a manner that would not impact human rights negatively of either their own citizens or persons from third countries. Therefore, we will conclude the paper by providing some recommendations for Western Balkan economies concerning AI regulation.

When adopting strategies and policies, governments should have close consultations and cooperation with experts from civil society and academia, in order to map possible solutions to challenges for human rights and especially vulnerable social groups. Also, governments should invest resources into research and development of

domestic technological tools which can provide better services for citizens and solve their actual problems, e.g. by creating scientific and research hubs or clusters.

Technical implementation of government systems which are used for processing citizens' personal data must be done in accordance with the privacy by design and privacy by default principles throughout the life cycle of the system, together with technical and organisational measures which need to be revised and updated in specific time intervals and especially after security incidents. Furthermore, government procurement of advanced technologies needs to be transparent, based on evidence of actual needs and carried out only after a broad public debate with all the relevant stakeholders. In that sense, procurement and application of all technologies for which there is no legal basis in terms of personal data processing and which would effectively cause mass breaches of human rights need to be banned.

Therefore, in order to follow the European path, legal regulation of AI and application of advanced technologies should be developed keeping in mind protection of human rights and possible ethical issues that may arise.

#### REFERENCES

- [1] Government AI Readiness Index by Oxford Insights <https://www.oxfordinsights.com/government-ai-readiness-index-2020>
- [2] GovTech Maturity Index <https://openknowledge.worldbank.org/handle/10986/36233>
- [3] Network Readiness Index 2021 <https://networkreadinessindex.org/>
- [4] E. Jakubowska, Ban Biometric Mass Surveillance: European Digital Rights, 2020. available at: <https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf>
- [5] Privacy international, The Global Surveillance Industry, 2018. available at: <https://privacyinternational.org/explainer/1632/global-surveillance-industry>
- [6] Freedom House, Democracy under Siege, 2021. available at: <https://freedomhouse.org/report/freedom-world/2021/democracy-under-siege>
- [7] B. Perkov, A city with a thousand eyes: mass surveillance in Belgrade, European Voice on Surveillance, 2020. available at: <https://aboutintel.eu/mass-surveillance-serbia/>
- [8] Share Foundation, New surveillance cameras in belgrade: location and human rights impact analysis – “withheld”, 2019. available at: <https://www.sharefoundation.info/en/new-surveillance-cameras-in-belgrade-location-and-human-rights-impact-analysis-withheld/>
- [9] Share Foundation, Kamere bez upotrebne dozvole / procena uticaja 2.0 (Unlicensed cameras / impact assessment 2.0) , 2020. available at: <https://www.sharefoundation.info/sr/kamere-bez-upotrebne-doizvol-e-procena-uticaja-2-0/>
- [10] Share Foundation, Serbian government is implementing unlawful video surveillance with face recognition in Belgrade , 2020. available at: <https://www.sharefoundation.info/wp-content/uploads/Serbia-Video-Surveillance-Policy-brief-final.pdf>
- [11] Share Foundation, Total surveillance law proposed in Serbia, 2021. available at: <https://www.sharefoundation.info/en/total-surveillance-law-proposed-in-serbia/>
- [12] European Digital Rights, Consultation on the proposal for the Zakon o unutrašnjim poslovima, 2021. available at: <https://www.sharefoundation.info/wp-content/uploads/EDRI-Civil-Society-consultation-on-the-proposal-for-the-Zakon-o-unutrašnjim-poslovima.pdf>
- [13] Share Foundation, Draft withdrawal a step towards moratorium on biometric surveillance, 2021. available at: <https://www.sharefoundation.info/en/draft-withdrawal-a-step-towards-moratorium-on-biometric-surveillance/>
- [14] N1 Belgrade, Serbia's Vucic blames himself for withdrawal of law on internal affairs, 2021. available at: <https://rs.n1info.com/english/news/serbias-vucic-blames-himself-for-withdrawal-of-law-on-internal-affairs/>
- [15] M. Matic, MUP RS postavio kamere za prepoznavanje lica: Gdje nas sve snimaju?!(RS Ministry of the Interior has set up face recognition cameras: Where are they filming us all ?!), Buka Magazin, 2020. available at: <https://www.6yka.com/novosti/mup-rs-postavio-kamere-za-prepoznavanje-lica-gdje-nas-sve-snimaju>
- [16] ATV, Postavljene kamere imaju mogućnost detekcije, ali ne i prepoznavanja lica (The installed cameras have the possibility of detection, but not face recognition), 2020. available at: <https://www.atvbl.rs/vijesti/drustvo/postavljene-kamere-imaju-mogucnost-detekcije-ali-ne-i-prepoznavanja-lica-2-8-2020>
- [17] Banjaluka.com, Nove kamere ipak ne prepoznaju lice, pojas, telefon, (However, the new cameras do not recognize the face, the belt, the phone) 2020. available at: <https://www.banjaluka.com/aktuelno/bih/nove-kamere-ipak-ne-prepoznaju-lice-pojas-telefon/>
- [18] Share Foundation, A password pandemic. How did a covid-19 password end up online?, 2020. available at: <https://www.sharefoundation.info/en/a-password-pandemic/>
- [19] Share Foundation, Opomena batutu zbog bezbednosnog incidenta sa licnim podacima gradana (Warning to Batutu due to a security incident with personal data of citizens) 2020. available at: <https://www.sharefoundation.info/sr/opomena-batutu-zbog-bezbednosnog-incidenta-sa-licnim-podacima-gradana/>
- [20] Privacy international, Montenegro publishes personal data of persons in isolation, 2020. available at: <https://privacyinternational.org/examples/3576/montenegro-publishes-personal-data-persons-isolation>
- [21] S. Kajošević, Montenegrins in Self-Isolation Sue State for Publishing Names, Balkan Insights, 2020. available at: <https://balkaninsight.com/2020/09/30/montenegrins-in-self-isolation-sue-state-for-publishing-names/>
- [22] N. Petaković, Otvoreni Balkan uvodi identifikacioni broj, povezuje državne e-uprave (The Open Balkans is introducing an identification number, connecting state e-governments), Nova ekonomija, 2021. available at: <https://novaekonomija.rs/vesti-iz-zemlje/otvoreni-balkan-uvodi-identifikacioni-broj-povezuje-drzavne-e-uprave>
- [23] Euro News Albania, What did Rama, Zaev and Vucic agree to in Skopje?, 2021. available at: <https://euronews.al/en/balkans/2021/07/29/what-did-rama-zaev-and-vucic-agree-to-in-skopje/>
- [24] Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025. available at: <https://www.srbija.gov.rs/tekst/437277>
- [25] The Ada Lovelace Institute (Ada), AI Now Institute (AI Now), and Open Government Partnership (OGP), Algorithmic Accountability for the Public Sector, 2021. available at: <https://www.opengovpartnership.org/wp-content/uploads/2021/08/algorithmic-accountability-public-sector.pdf>
- [26] Strategy on the Implementation of the Right of Personal Data Protection 2017-2022. available at: [https://dzlp.mk/sites/default/files/dzlp\\_strategija\\_mk.pdf](https://dzlp.mk/sites/default/files/dzlp_strategija_mk.pdf)
- [27] Serbian Strategy on Personal Data Protection. available at: <https://www.poverenik.rs/sr-yu/%D0%BF%D0%BE%D0%B4%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D1%81%D0%B>

A%D0%B8-%D0%B0%D0%BA%D1%82%D0%B84/942-strategija-zatite-podataka-o-linosti.html

- [28] Albanian Strategy on Personal Data Protection. available at: <https://www.idp.al/strategjia-2021-2023/>
- [29] Draft of the Law on Data Protection in Montenegro. available at: <https://www.gov.me/dokumenta/2ca5b30b-16ef-4fcf-a043-c05e2afa8fe6>
- [30] For Albania see: Decision No. 1084 On Adopting The National Cybersecurity Strategy And Its Action Plan 2020-2025. available at: [https://www.unicef.org/albania/media/3526/file/Albanian\\_National\\_Cybersecurity\\_Strategy.pdf](https://www.unicef.org/albania/media/3526/file/Albanian_National_Cybersecurity_Strategy.pdf)
- For Kosovo see: Cybersecurity Capacity Review. available at: <https://gcscc.web.ox.ac.uk/files/cybersecuritycapacityassessmentfortherepublicofkosovo2019pdf>
- For Montenegro see: Cyber Security Strategy of Montenegro 2018-2021. available at: <https://www.gov.me/dokumenta/fa4f3ed4-d059-4958-8847-d6111360a477>

For North Macedonia see: National Cyber Security Strategy and Action Plan 2018 – 2022. available at: <https://www.mioa.gov.mk/?q=en/node/2379>

For Serbia see: The Strategy of Development of the Information Society and Information Safety for 2021-2026. available at: <https://mtt.gov.rs/extfile/sr/35314/Information%20Society%20and%20InfoSec%20Strategy%202021-202611.pdf>

- [31] Bosnian National Strategy for Establishment of CERT. available at: <http://www.msb.gov.ba/dokumenti/strateski/default.aspx?id=6248&langTag=bs-BA>
- [32] Action Plan for the Implementation of the Strategy for the Development of Artificial Intelligence in the Republic of Serbia 2020–202. available at: <https://www.pravno-informacioni-sistem.rs/SIGlasnikPortal/eli/rep/sgrs/vlada/drugiakt/2020/81/1/reg>