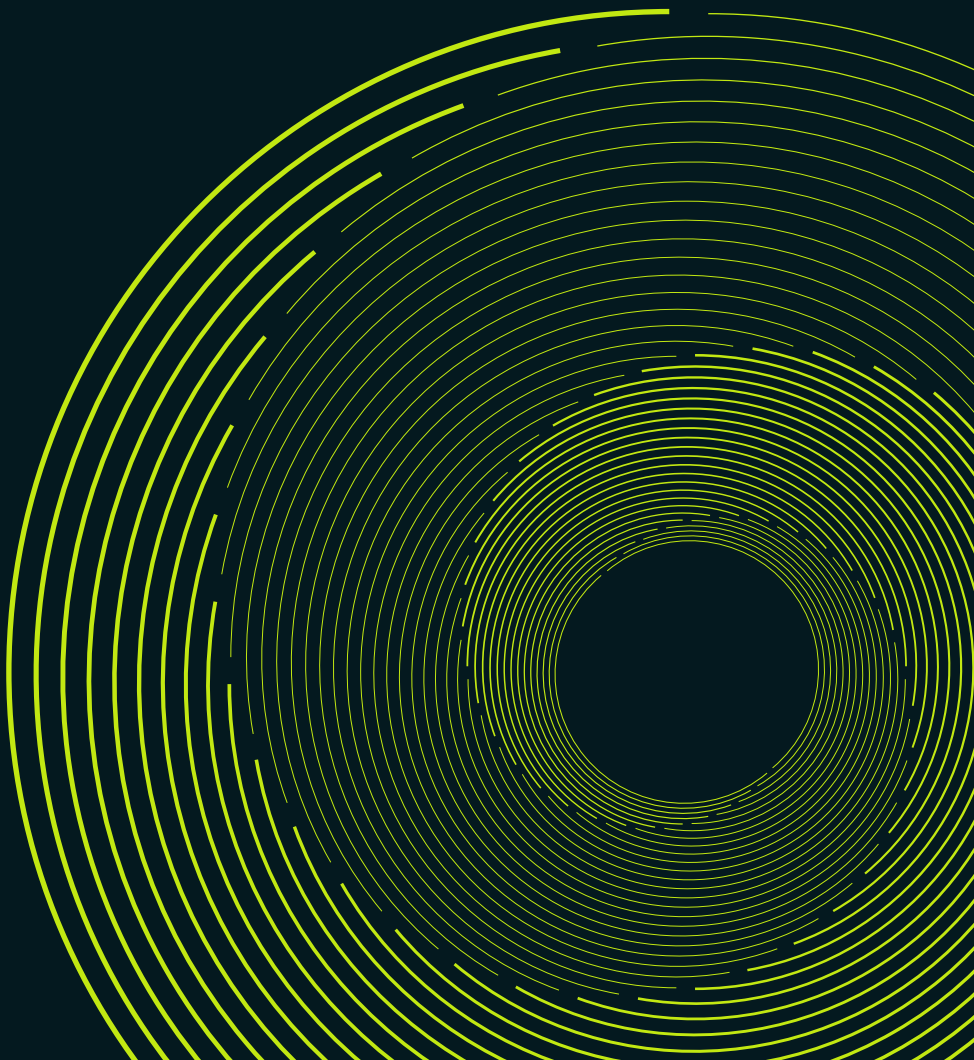
# AI IN SOUTHEAST EUROPE

COMPARATIVE READINESS OVERVIEW



# CONTENTS

# Intro

This research aims chiefly to provide information on governments' capacities for the implementation of AI and advanced technologies in ten countries of the Southeast Europe: Albania, Bosnia and Herzegovina, Croatia, Greece, Hungary, Kosovo, Montenegro, North Macedonia, Serbia and Slovenia. Motivated by the importance and urgency of this issue and at the same time the lack of any in-depth insight that would cover all its important aspects in this region, the authors conducted this study to provide a more holistic overview of governments' readiness to implement AI and advanced technologies, as well as to point out the main problems arising.

### Main hypothesis of the research

The governments of the ten countries in Southeast Europe have a significant lack of capacities for adequate implementation of AI and advanced technologies.

## Methodology

The research consisted of collecting and analysing both primary and secondary data.

1. A preliminary desk research was done by collecting countries' rankings and conclusions from relevant studies concerning the implementation of advanced technologies, and by gathering information on existing regulatory framework on AI, Data Protection, Information Security and Anti-discrimination.

2. The key actors and stakeholders for each country were mapped.

3. Concise summaries of findings on each country were sent to our local partners so they could verify collected or add missing information.

4. A questionnaire for regional experts was designed and distributed through our local partners in order to get additional information and a more nuanced insight.

5. The gathered data was examined using the thematic analysis, mapping areas in which the implementation of AI/advanced technologies seems to be the most prominent and searching for recurring answers in our experts' questionnaires.

# Overview

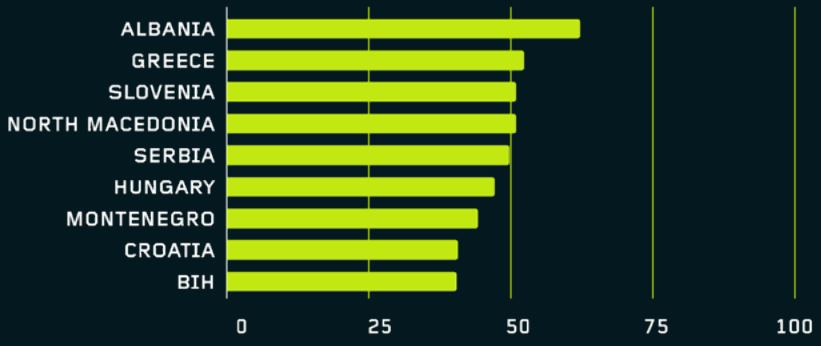
In order to provide background information on the use of advanced technologies in Southeast Europe (SEE), existing research conducted by various international actors will be briefly described in this section. By analysing existing data and rankings we wanted to understand how the observed countries rank globally and regionally, and if some conclusions can be drawn - e.g. which country can be deemed a frontrunner and which is continuously ending up at the bottom of rankings, i.e. are there any significant differences in countries' readiness for implementation of AI and advanced technologies. Most of the existing research excludes at least one country out of the observed 10, usually it being Kosovo.

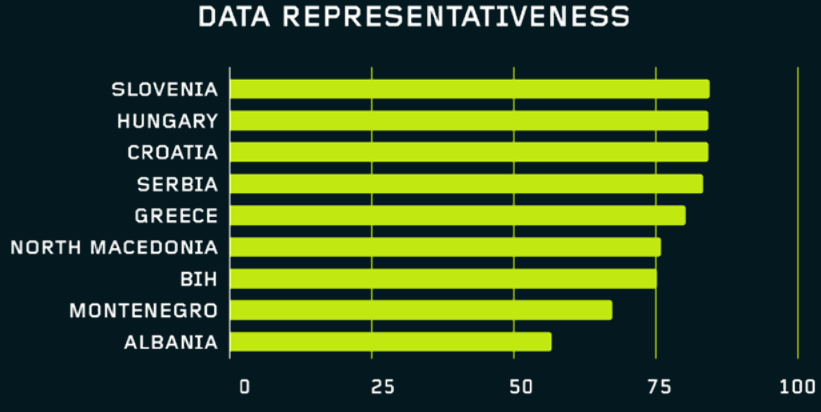
## Existing research

Government AI Readiness Index is compiled by Oxford Insights drawing on ten 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. World average total score is 44.25 and four countries included in our research scored lower than average - Montenegro (70th place), North Macedonia (73rd), Albania (85th) and Bosnia and Herzegovina (100th). Out of all non-EU countries, only Serbia (46th) has a higher than average score and ranks better than two EU countries - Croatia (58th) and Greece (61st). Slovenia is ranked the highest (39th), followed by Hungary (41st place). It can be concluded that EU countries have overall better scores in most dimensions, with an exception of Serbia which continuously has good scores when compared to other countries included in our research.

## GOVERNMENT AI READINESS INDEX


## DIGITAL CAPACITY




The Global AI Index evaluates AI development in 62 countries through three dimensions of analysis: investment, innovation, and implementation. It includes only three out of ten observed countries, all of them being EU members. Slovenia takes 29th place with a score of 25.19 out of 100 (the U.S. have a score of 100 for comparison), Greece takes the 40th place with a score of 17.33 and Hungary is 42nd with a score of 17.

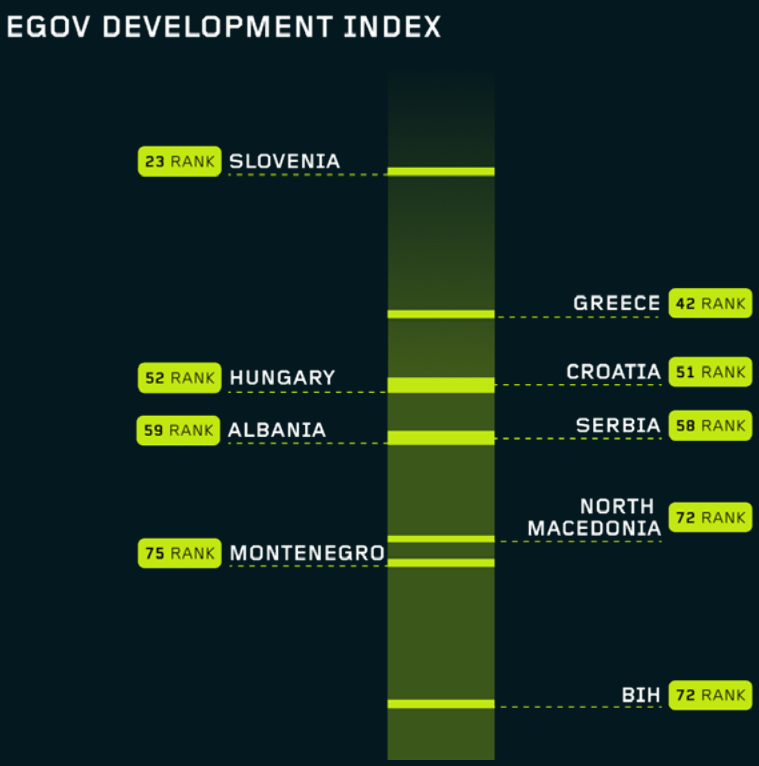
Global Open Data measures openness of government data, i.e. which governments readily publish data and in which spheres datasets are rarely published. Among countries in the research, Slovenia ranks the best and takes 28th place. Next comes Greece on 35th, Serbia on 41st, Croatia on 44th, Albania on 47th, Montenegro on 49th, North Macedonia on 52nd, and lastly Kosovo and BiH share the 58th spot. Hungary is not included in the research. It is important to note that the last available datasets and ranking is for 2015. Once again, EU members are ranked higher, followed by Serbia.

GovTech Maturity Index measures digital transformation in the public sector. North Macedonia is not included in the ranking. Three of the EU members from our research are deemed to be GovTech leaders. Kosovo and Bosnia and Herzegovina are once again ranked at the bottom of the list.

| Rank | Countries |
|---|---|
| A - GovTech leaders | Croatia, Greece, Slovenia |
| B - significant focus on GovTech | Albania, Hungary, Montenegro, Serbia |
| C - some focus on GovTech | BiH, Kosovo |
| Not included | North Macedonia |

EGov Development Index measures to which extent governments provide public services through information and communication technology. It draws on three dimensions: provision of online services, telecommunication connectivity and human capacity. Slove-

nia is once again ranked the highest (23rd), followed by three other EU members. Serbia (58th) comes closely after Hungary (52nd), Bosnia and Herzegovina once again ranks the lowest (94th), while Kosovo is not included.




Network Readiness Index 2021 ranks a total of 130 economies and represents a composite measure of four dimensions, Technology, People, Governance and Impact. Slovenia ranks the highest (26th), followed by other EU members (Hungary - 37th, Croatia - 41st and Greece - 46th). Serbia comes after the EU members

(57th), followed by Montenegro (62nd), North Macedonia (64th), and Albania (80th), BiH ranks the worst (86th place), while Kosovo is not included in the ranking.

## Conclusion

**It can be concluded that EU members are continuously ranked better than non-EU countries,** while Slovenia appears to be the regional frontrunner in terms of its readiness for the implementation of advanced technologies. Other than that, EU membership seem to have small or no impact on most levels achieved by the observed countries' while differences among them appear inconsistent (e.g. Serbia sometimes ranks higher than some EU countries). However, it is important to note that certain countries, usually BiH, trail behind and are consistently ranked the worst, while others are often excluded (Kosovo). Overall, **none of the countries in question can be seen as leaders on the global level** when it comes to their readiness for the implementation of advanced technologies and there is **much room for improvemen**t.

The answers of the regional experts from questionnaires mostly align with conclusions drawn from the existing body of research, with most of them seeing **the lack of experts in the field and the lack of adequate funding as the biggest challenges** in implementing AI/advanced technologies in their respective countries.

# Context

As digitisation of jobs and services takes an increasingly important role in our societies, the public sector is trying to keep up and go beyond traditional administrative services offered in digital form (e-government). While most countries may lag far behind Estonia, considered as the European "digital state" champion, the SEE countries 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 public sector in the observed countries use various tech tools, the most impactful on human rights and social processes being the ones used for **surveillance, public order and safety, border control and management, and healthcare**.

## Surveillance, public order, and safety

The advances and proliferation of surveillance technologies, particularly those that rely on processing of biometric personal data have been welcomed by governments in the observed countries regardless of the perceived levels of democracy. While promises of a "crimeless society" are far-fetched, government entities tasked with maintaining public order and safety, and investigating crime are more technologically equipped today than ever before. In circumstances where democracy is "under siege" and global freedom is in decline for the 15th consecutive year, intrusive surveillance technologies can only exacerbate these negative trends.

One of the most prolific examples of dangerous technology in the hands of a hybrid regime in SEE is the "Safe Society" project in

Serbia, which entails the use of an advanced video-surveillance system in the country's capital Belgrade, first announced in early 2019 as a part of a wider cooperation between the Serbian and Chinese governments. Technology partner in this particular project is the Chinese tech giant Huawei. There was no prior public debate on whether this kind of surveillance system, most notably with facial recognition capabilities, was actually needed in Belgrade and what would be the societal ramifications of introducing it. According to documents obtained by SHARE Foundation 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.

A citizen initiative led by SHARE Foundation, #hiljadekamera, has been fighting the proposed surveillance system since its announcement, arguing that Serbian law provides no legal basis for the use of biometric surveillance technologies and that it would have serious impact on freedoms and liberties enjoyed in public spaces. In the autumn of 2021, a Draft Law on Internal Affairs was presented by the Ministry of Interior, inter alia with the aim of legalising the use of biometric surveillance by the Serbian police. However, after strong opposition from the civil society and the international community, the draft was withdrawn from procedure. The issue is expected to reopen after the presidential, parliamentary and local elections held in April 2022.

In January 2022, the Commissioner for Information of Public Importance and Personal Data Protection conducted an oversight procedure within the Ministry of Interior on suspicion that the facial recognition technology was used by the police to identify citizens

who participated in environmental protests and roadblocks in late 2021 and issue them misdemeanour charges. However, the Commissioner's Office did not find any evidence of facial recognition usage for that purpose.

There are more similar cases of governments advancing 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 which has close political ties to Serbia. According to media reports in 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 have only "face detection" and not facial recognition capabilities, as well as automatic vehicle licence plate recognition for the purpose of detecting unregistered vehicles. One expert from Bosnia and Herzegovina also noted that body cameras were introduced for police officers in the Sarajevo Canton, i.e. the region of the country's capital. In Hungary, there were announcements of a centralised CCTV system, dubbed "Dragonfly", which would consist of approximately 35,000 cameras monitoring public spaces and a central facility to store the collected recordings. Although not yet confirmed, it is likely that this system would also include facial recognition capabilities, as Hungarian law enforcement already uses a face recognition search engine provided by Japanese vendor NEC.

Facial recognition tools are increasingly embraced by the law enforcement, despite numerous human rights risks associated with the use of this technology. For example, automated facial recognition has been used in criminal investigations in Slovenia since 2015 (VeriLook and Face Trace as tech solutions) while there are

indications that the Slovenian police used this technology as early as 2014. Croatia, another EU Member State, has two databases used for facial recognition which are owned by the Ministry of Internal Affairs: ABIS, which stores data from crime suspects and offenders, and the image repository of civil documents (ID cards, travel documents, and driver licences). In both of them, the search engine used for facial recognition searches is IntellQ supplied by IntellByte, a Croatian company.

One of the most worrying developments surrounding these issues was the discovery that the Hungarian government used Pegasus, an advanced spyware designed to infect smartphones and sold by Israeli surveillance equipment vendor NSO Group. In July 2021, journalistic collective Forbidden Stories broke the story of how Pegasus was used for targeted surveillance of about 50,000 people from across the world, including journalists, activists, academics, and high ranking public officials. Until now, information emerged that phones of investigative journalists, the President of the Hungarian Bar Association, and even people close to the former President of Hungary Janos Ader have been infected with Pegasus, along with many more people from Hungary also suspected of being targets. Citizen Lab, a tech investigative team working at the University of Toronto, also reported on implications that Serbia's Security Information Agency (BIA) has been a customer of Circles, another surveillance company linked to NSO Group. In December 2021, Citizen Lab reported on indications that Predator, an advanced spyware tool with capabilities similar to Pegasus, could have been used in Serbia.

## Border control and management

The so-called 2015 European migrant crisis that has sparked deep

political divisions across the continent, has largely influenced the ways in which EU Member States govern the entry into the Schengen space and control its borders. Expectedly, Schengen border countries, particularly Greece and Hungary in the context of this research, experience considerably higher pressure when it comes to the migrant path to Western Europe.

Although the EU already has a vast infrastructure of border management, such as "smart borders", some emerging technologies and associated practices observed in recent times are quite problematic in terms of inhumane treatment of persons from third countries, most notably refugees and asylum seekers. Moreover, it is unlikely at this point that the governments in question would so easily apply such technology in dealing with the domicile population. An article in The Guardian highlighted a whole new form of "Fortress Europe" emerging in countries such as Greece, Hungary, Croatia, or Poland that are being equipped with very advanced military-grade technologies used to deter and push back refugees from crossing into the EU. Ranging from drones, sensors, cameras and AI-powered "lie detectors" to a sound cannon capable of firing blasts of up to 162 decibels used by Greece to deter people from crossing its border with Turkey, these tools are a terrifying glimpse into a techno-dystopian future, with vulnerable and disadvantaged people caught on the testing grounds.

In January 2021, the Border Violence Monitoring Network submitted a report to the UN Special Rapporteur on contemporary forms of racism, xenophobia, and related intolerance displayed by the Croatian police using technology to conduct illegal push-backs of refugees to Serbia and Bosnia and Herzegovina. The report lists cases where drones, helicopters outfitted with searchlights and electro-optical/infra-red turrets, scanners for human detection

inside vehicles, and night/thermal vision equipment were used to chase and hunt down people as they moved across Croatian territory.

Greece, which is planning to implement a biometric border management system with facial recognition and fingerprinting, has also procured numerous technologies when it comes to tech-policing and border control in the context of migrations towards Europe. According to Homo Digitalis, an organisation advocating for digital rights and freedoms in Greece, the Greek police have procured smart devices with facial recognition and automated fingerprint identification, which are the size of a smartphone and can be used to collect facial image and fingerprint data and compare them to data in existing identification databases. There are fears that these devices will primarily be used to check the status of people presumed to be illegally residing in Greece, therefore impacting the migrant community. Police drones, which were previously mandated for monitoring forests and motorway traffic only, were approved for use in policing and border management by a new Presidential Decree passed in 2019. However, as Homo Digitalis experts have warned, there were no provisions in the Decree pertaining to personal data processing through the use of drones. Also, the Decree uses vague language in terms of drones, which opens a lot of opportunities for abuse by the police.

Asylum seeker facilities in Greece are also problematic in terms of intrusive technology being used on people in a vulnerable position. Based on information provided to our research team by Homo Digitalis, these facilities have a vast surveillance ecosystem which includes advanced technologies primarily targeting movements and behaviour of asylum seekers. One example is IPERION, a system which will be used to track entry and exit of asylum seekers to

the reception facilities with the use of special ID cards. Fingerprints will also be taken for automated biometric authentication purposes. The ID cards will be used by the asylum seekers for receiving food, clothing, and other supplies in the facilities, as well as for moving from one facility to another. Another system to complement IPERION is KENTAYROS, set up within the facilities and in their perimeter, consisting of different technologies such as drones and smart CCTV equipped with AI behaviour analytics algorithms. It is possible to use such tools to constantly monitor and analyse people's behaviour, giving them a false sense of security while they can't challenge the use of the system in any way.

An important step in the battle against IPERION and KENTAYROS was taken in February 2022 when Homo Digitalis, together with the Hellenic League for Human Rights, HIAS Greece and Dr Niovi Vavoula, a Lecturer at Queen Mary University of London, submitted a request to the Hellenic Data Protection Authority to launch an investigation of the two systems. Prompted by the request, the Hellenic Data Protection Authority started an investigation into the Ministry of Immigration and Asylum in March 2022 and stated that it also received a request for information from the European Parliament's Civil Liberties, Justice and Home Affairs Committee regarding surveillance technologies generally used for border control in Greece.

## Healthcare

With the COVID-19 pandemic entering its third year and still wreaking havoc on the economic and healthcare systems in most of the world, one of the significant steps made by governments was investing in health infrastructure and implementing tech solutions to help fight the biggest global crisis of the 21st century. The pandemic

prompted governments in Southeast Europe to digitise various existing healthcare services and offer new ones, such as COVID-19 green certificates. However, a number of incidents have shown that implementation was not always on the right side of personal data protection and information security standards.

To provide citizens with a familiar user experience, governments have designed various mobile apps to help curb the spread of the coronavirus by notifying users when they have been in contact with an infected person, or to obtain other health related information. There are numerous examples in the observed countries, such as Koronavirus MK in North Macedonia, #OstaniZdrav and zVem in Slovenia, VirusRadar and the Home Quarantine System in Hungary, Covid Free Gr Wallet in Greece, Stop COVID-19 and EU Digital Covid Passport in Croatia or My EU Digital Green Certificate in Serbia. Another similar example is Andrija, a digital assistant on WhatsApp designed to help citizens of Croatia detect if they had symptoms of coronavirus infection. Andrija bot was officially presented to the Croatian public in April 2020 and was active until June 2021. This tool was highlighted by an expert we reached out to as the most prominent example of advanced technologies usage by the public sector in Croatia.

In 2020, there was controversy in Slovenia as the government tried to impose an obligatory contact tracing app by bundling the provisions into a massive bill, which contained other public services such as unemployment subsidies and government compensations for businesses affected by the pandemic. As Slovenian digital rights activist Domen Savič wrote in an op-ed, "the Minister of Public Administration went on to explain that the provisions of the law stating the app will be obligatory are not going to be used in practice. The coronavirus tracking app will therefore be completely voluntary".

Another issue concerning the use of technology to tackle the pandemic in the SEE region were the health data breaches. For example, access credentials for Information System COVID-19, the database for pandemic-related data in Serbia, were publicly available on a website of a health institution for 8 days long enough to get indexed by Google, meaning that anyone could access it via a simple search. Further investigation of the incident by the Serbian 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 to the Institute for Public Health of Serbia, the data controller of the system.

In Montenegro, the government intentionally published data of people who were given mandatory self-isolation orders to deter them from breaking the quarantine rules. NGO Civic Alliance challenged the practice before the Constitutional Court of Montenegro, which ruled in its 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. In December 2021, the Government of Montenegro decided to compensate more than 2.700 citizens affected by the personal data breach with 300 Euros, given that courts have already ruled in citizens' favour in some cases.

In February 2021, with the start of the first vaccine rollouts, the Croatian Ministry of Health set up a COVID-19 vaccination appointment website without a privacy policy, contrary to data protection regulations. The system was only accessible for three hours and Health Minister Vili Beroš stated it was a test version, claiming that more than 4000 people already entered their personal data into the system.

The COVID-19 pandemic also presented an opportunity for countries to try out machine learning and big data analytics in healthcare. In Greece, a machine learning algorithm nicknamed Eva was provided pro bono to the government by a group of scientists. Eva was used to provide an assessment as to which incoming travellers should be tested for COVID-19 based on data they provided in a questionnaire they had to fill out before entering Greece. In terms of big data analytics and combating the pandemic, it was discovered that Greece signed a pro bono agreement with Palantir, a company with a history of providing technology for intrusive purposes, most notably for immigration enforcement in the USA. In January 2021, the Greek government announced that it has partnered with PwC Greece to receive consultancy services in relation to big data analytics and the pandemic.

## Conclusion

It seems that the governments of the Southeast European countries 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 digitisation of government services and new avenues for exploration of applying technology are 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 within the Open Balkan Initiative 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: an expert from North Macedonia highlighted the issues with the country's automatic court case allocation system (AKMIS). In 2017,

a working group of the Ministry of Justice discovered that the Criminal Court in Skopje and the Supreme Court, arguably the most important courts in North Macedonia, were allocating cases manually. A former President of the Criminal Court in Skopje was given a prison sentence in 2021 directly in connection with the abuses of the case allocation system. Use of AI in courts, or "predictive justice", was also announced in neighbouring Serbia, but with no specific implementation plans as of late.

When it comes to instances of AI implementation which would have the highest impact on society and citizens in their countries, the **regional experts mostly highlighted public administration services, education, and healthcare as areas where considerable benefits are possible**. In terms of highest social risks, experts from Serbia and Greece for example pointed to biometric data processing through video-surveillance of public spaces or biometric identification tools used during police stops. The experts mostly named **privacy, personal data protection, freedom of expression and information, and rights to assembly and equal treatment as the rights most likely to be impacted** by application of AI and advanced technologies.

# Regulatory Framework

## AI Framework

Three out of ten countries analysed have developed strategies in the field of AI (Serbia, Slovenia, and Hungary), two have their strategies under development (Croatia and Greece) and five countries have not yet developed strategies in the field of AI (Montenegro, Bosnia and Herzegovina, North Macedonia, Albania, and Kosovo).

Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025 assigns priority in areas of education and science, the economy, and the public sector. Within the strategy, there are 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 particular goals of the strategy **is the ethical and safe use of AI**.

Hungary's Artificial Intelligence Strategy for the period 2020-2030 assigns priority to the possibility of supporting specific sectors that could be developed by AI-based applications most effectively: manufacturing, agriculture, health care, public administration, logistics, transport, and energy. A separate chapter (4.1.6 Regulatory and Ethical Framework - "Reliable, regulated use") is focused on the ethical and legal framework for the usage of AI.

National Strategy for the Development and usage of AI in the Re-

public of Slovenia in effect through to summer of 2025 assigns priority in areas of economy, public sector, public and state administration, and society. Special chapters deal with legal and ethical aspects of AI usage. One of the specific objectives of this strategy is also to provide an appropriate legal and ethical framework.

## Data Protection Framework

All of the countries observed have made progress in data protection, including the ones outside the EU.

A great majority of the countries did not adopt a national data protection strategy, except for North Macedonia, which has its strategy currently in place (for years 2017-2022). Serbia's Data Protection Commissioner announced that the data protection strategy for the period 2022-2023 is currently in the works, but has not been adopted yet. The current strategy is outdated and corresponds to the previous Data protection law from 2008. Also, Albanian data protection authority previously announced that Albanian data protection strategy for years 2022-2024 was to be adopted and 'published soon', but this is yet to happen. Although there are no data protection strategies in place, many of the observed countries' data protection authorities' annual working plans do include certain strategic steps to take and tasks to fill-in.

Three of the EU-member states (namely, Croatia, Greece, and Hungary) have transposed GDPR to their national legislation by adopting separate data protection laws. Slovenia has yet to adopt a national law which would harmonise the national legislation with GDPR – currently, there is only a draft data protection law which mostly follows GDPR and amends only a few aspects of systemic and procedural nature.

As for the non-EU states, some of them have actually adopted new data protection legislation which is largely harmonised with GDPR. This is the case with North Macedonia, Serbia, and Kosovo. As for Montenegro, there is a draft of the new data protection law harmonised with GDPR which is yet to be adopted, although rendered back in 2019. The similar is currently happening in Albania – its data protection authority is undergoing a consultation process with the goal to adopt a new data protection law. Other countries have previous data protection laws in place which were adopted many years prior to GDPR, however, many of these older laws do honour some of the most important GDPR principles but still lack many of GDPR principles.

One of the important GDPR concepts is the obligation to conduct a Data Protection Impact Assessment (DPIA) in certain cases of processing. Majority of countries which have harmonised their legislation with GDPR have adopted guidelines regarding the DPIA. Such guidelines followed by the examples in which DPIA is necessary were adopted by national data protection authorities. Such examples mostly include profiling, automated-decision making, using new technologies (such is artificial intelligence) for processing or using possibilities which will serve to analyse or foresee person's economic situation, health, interests, behaviours, location or movement, tracking location or person's behaviour in systematic processing communication data generated by using phone, internet or other communication means etc.

For example, Greek data protection authority in their DPIA guidelines specifically mention the obligation to conduct DPIA when the processing activity includes data collected or generated by means or devices, especially through 'internet of things' applications (smart TVs, smart appliances, toys, smart cities etc.), innovative

use or application of new technological or organisational solutions, which can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms, like the combined use of fingerprint and face recognition for improved physical access control, or m-health applications, or other "smart" applications from which user profiles are generated, or artificial intelligence applications as well as publicly accessible blockchains that include personal data.

The question is whether the controllers engaging in the processing activities actually possess adequate knowledge to conduct a proper DPIA. For instance, 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.

Countries which have not harmonised their national legislation with GDPR (including Albania, Montenegro, Bosnia and Herzegovina) do not have the obligation to conduct DPIA, therefore, there are no specific guidelines regarding this.

Experts included in the research were asked to rate their government and state bodies' capacity to comply with relevant standards when implementing AI/advanced technologies with data protection in their respective countries on a scale of 1 to 5 (1 being the worst, 5 the best). Out of 17 experts, two of them were unable to give specific scores but emphasised there is room for improvement. The average score of the other 15 is 2 out of 5, indicating a significant space for improvement.

## Information security Framework

All of the observed countries have made progress in relation to information security regulations, including the ones outside the EU.

Except for Bosnia and Herzegovina, all countries have adopted national information security strategies. However, Bosnia and Herzegovina does have a national Strategy for Establishment of CERT, adopted back in 2011, which covers some of the information security issues.

All EU country member-states (Croatia, Greece, Hungary, and Slovenia) have transposed the EU NIS Directive in their national legislation by adopting separate laws. As for the other non-EU countries, some of them do have separate information security laws which are mostly harmonised with the NIS Directive. This is the case with Serbia and Albania, although 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.

Bosnia and 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 harmonised with NIS Directive is supposed to be adopted in the near future (not clear when, the first draft announcement came back in 2019 and since then several versions were published). 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 harmonised with the NIS Directive.

On a scale of 1 to 5 (1 being the worst, 5 the best) experts participating in the research were asked to rate their government and state bodies' capacity to comply with relevant standards when implementing AI/advanced technologies with information security in their respective countries. Three of them were unable to give scores, and the average score of the rest was 2.2.

## Anti-discrimination Framework

Greece, Croatia, Hungary, and Slovenia as members of the European Union are obliged to transpose its Racial Equality Directive and the Employment Equality Directive in their national legislation. All non-EU countries included in the research ratified all major human rights conventions and have their own anti-discrimination laws. It should be noted that there is no mention of AI in any of discrimination related legislation in any of the countries in question. However, Serbia's Strategy for the Development of AI recognises the risks of it potentially being discriminatory and the Action Plan for its implementation prescribes certain activities related to preventing discriminatory AI practices.

Each country also has at least one national equality body that is a part of European network of institutions that deal with discrimination - Equinet, which has had different activities related to the connection between technology and discrimination. As they are all part of Equinet, all national equality bodies should be aware of its reports and be present at events that deal with discrimination and technology, so it can be concluded that they are all at least aware

of this topic and its urgency. Even though none of the institutions have their own concrete activities related to this, Croatia's Ombudswoman can be pointed out as the institution which is showing the highest level of awareness, covering reports and participating at various events related to AI.

Out of 17 experts from the region who answered our questionnaire, two said they cannot answer the question: How would you rate the capacity of the government and state bodies to comply with relevant anti-discrimination standards when implementing AI/advanced technologies? (from 1-5, 1-worst, 5-best). The average rating of the other 15 was 2.6 out of 5, which implies that there is a perceived significant room for improvement when we talk about capacities of governments to comply with anti-discrimination standards when implementing advanced technologies.

Only three out of ten countries analysed have developed strategies in the field of AI (Serbia, Slovenia, and Hungary), and two more (Croatia and Greece) strategies are expected to be drafted in the near future. All other countries still haven't developed national strategies in the field of AI.

When it comes to countries' capacities regarding data protection, **they largely vary depending on the country**. EU countries and some non-EU countries included in this report (such as Serbia and North Macedonia, amongst others) have harmonised their legislation with GDPR, and others (such as Albania, Montenegro, and Bosnia and Herzegovina) still have not, however, many of those are currently in the harmonising process, therefore, have the intention to harmonise in future. There is progress in the data protection field in the majority of these countries and practices of their respective data protection authorities, however, there is still much room for improvement.

As for information security, it is comforting to know that information security is a relevant topic in each of the observed countries. All but Bosnia and Herzegovina have an information security strategy in place and the majority of the countries have harmonised their national legislation with the NIS directive, although there are differences between these national laws and NIS. Some of the countries (North Macedonia, Bosnia and Herzegovina) still do not have overarching information security laws.

## Conclusion

Overall it could be concluded that **all of the countries in question show similar levels of compliance with EU anti-discrimination legislation**. However, when it comes to discussing legislation, there are two questions that should be taken in consideration when assessing 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 of the ability of the current EU equality directives to 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 question is whether the current EU anti-discrimination legal framework is satisfactory and if it provides enough room for interpretation regarding AI?

# Key Actors and Stakeholders

Hungary, Serbia and Slovenia are the countries with the most developed network of key actors and stakeholders in the field of AI. Among other analysed countries we have noticed the lack of actors and stakeholders involved in this process. Regardless, we can point to some systematic efforts in Greece and Montenegro to deal with the implementation of advanced technologies and AI.

## Hungary

In **Hungary**, the mandate to deal with the implementation of advanced technologies and AI is largely entrusted to the government and institutions under its jurisdiction. However, we are also noting an excellent example of cooperation between the public and private sectors through the development of Artificial Intelligence Coalition. The Coalition was founded upon the initiative of the Ministry of Innovation and Technology under the Digital Success Program as an expert and consultation forum of the local AI ecosystem. There are also some AI architectures that we recognise such as AI Innovation Centre, National Laboratory for Autonomous Vehicles and PwC which supported the creation of an AI Innovation Hub and AI Strategy for Hungary.

## Serbia

In **Serbia** most of the actors in charge of this process come from the public sector, i.e. institutions related to the Serbian government such as the Ministry of Education, Science and Technological Development, and Institute of Artificial Intelligence. There are also several representatives of the private sector that we can identify

such as Continental Automotive Serbia. We have also identified the existence of two main research and development Funds in this area: Science Fund and Innovation Fund. Among the representatives of the CSO we point out to Digital Serbia, Serbian AI Society and Wonderland AI Summit 2021. Serbia has also developed AI Architectures such as State Centre for Data Management and Storage, Centre for the Promotion of Science, Vojvodina ICT cluster, and Institute for Artificial Intelligence of Serbia.

## Slovenia

In **Slovenia** we can single out actors from both public and private sectors who have the mandate to deal with the implementation of advanced technologies and AI of which we should firstly mention the Ministry of Public Administration, namely the Information Society Directorate that has been a driving force of digital transformation in the public sector. In January 2022 the Directorate was to be integrated into the newly established Government Office for Digital Transformation. Beside these institutions there are also the International Research Centre on Artificial Intelligence (IRCAI) and Jožef Stefan Institute as relevant actors in this process. Other than those, we should bring up the ICT Association of Slovenia (ZIT), Chamber of Commerce and Industry of Slovenia (CCIS), Slovenian Artificial Intelligence Society (SLAIS). There are also a couple of stakeholders worthy of mention: Strategic Research and Innovation Partnerships on Smart cities (SRIP CS&C), Factories of the future (SRIP FoF), and civil society through the Slovenian Digital Coalition (SDC). According to the Slovenian AI Strategy report the current Open data platform for data sharing (OPSI) remains the central hub for further development of data sharing infrastructure and practices. The first EuroHPC world-class supercomputer Vega

remains the main computational infrastructure for further adaptation to AI use. On the other hand, Edge-AI infrastructure has been developed for the Factory of the Future (FoF) digital twin demonstration centre at the Faculty of Mechanical Engineering (University of Ljubljana) within the FoF Strategic Research and Innovation Partnership. SPIRIT Slovenia in cooperation with the Embassy of the Republic of Slovenia in Tokyo and Sumitomo Mitsui Banking Corporation prepared a web conference for Japanese companies interested in investing in Central and Eastern European countries.

## Albania

In **Albania** we have 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 - Albanian institute for safe AI, Albania Artificial Intelligence, AADF (AI for Youth program), and National Agency for Information Society which can be considered as a leader in setting the digital agenda in Albania.

## Bosnia and Herzegovina

**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 of technologies it uses. For instance, legislation on personal data protection and intellectual property rights has been adopted on the state level, while the remainder of the rules is predominately established on the level of entities.

## Croatia

In **Croatia** we can identify several Government bodies which we can say are relevant actors in this field such as the Ministry of Economy and Sustainable Development of the Republic of Croatia, Central state office for Digital Society Development, and the Ministry of Tourism. Worth mentioning are also Croatian Regulatory Authority for Network Industries HAKOM, Croatian Personal Data Protection Agency AZOP, University of Zagreb - University Computing Center SRCE, and Central Finance and Contracting Agency SAFU. Worth mentioning is also Croatian Artificial Intelligence Association which created the first ever Croatian AI Landscape that lists all stakeholders in the artificial intelligence ecosystem in Croatia, including companies, startups, educational and research institutions, and other relevant organisations.

## Greece

Although **Greece** hasn't developed a national strategy in the field of AI, the country has developed Digital Transformation Bible (DTB), the flagship policy report that drives the digital transformation in Greece. Among key actors from the segment of competent authorities we can identify Hellenic Ministry of Digital Governance as the most prominent player in this field. Nevertheless, each ministry has a leading role in its respective sector. For example, the Ministry of Justice has put in place a special working group assessing the benefits and drawbacks from using AI tools in the justice field (mostly applications related to e-justice, digitisation of documents, etc).

## Kosovo

Among Government actors in **Kosovo** we can point out the Agency of Information Society within the Ministry of Internal Affairs, and Ministry of Economy. There are also Information and Privacy Agency (AIP), TAX Administration Office, Public Procurement Regulatory Commission, Kosovo Judicial Council, Municipality of Prishtina, Property Tax Payment, Ministry for Internal Affairs and Public Administration, Assembly of Kosovo, Ministry of Education, Science, Technology and Innovation etc. Among local CSO actors we have identified Open Data Kosovo, BIRN Kosovo, Innovation Centre Kosovo, STIKK, FLOSSK.

## Montenegro

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 a number of Montenegrin ICT companies, mainly through their umbrella body – ICT Cortex, that aims to contribute to and foster the digital development and transformation in Montenegro, and to promote Montenegrin ICT scene on the international level. Other worthy mentions are Chamber of Commerce of Montenegro, Association of Managers of Montenegro, Union of Employers of Montenegro, Council of Foreign Investors of Montenegro, AmCham Montenegro, Crnogorski Telekom (owns a department for digital transformation), Telenor Montenegro, M: tel Montenegro, Digitalizuj.me, DevClub.

It is important to mention the contribution of the University of Montenegro in this area, and master studies of the study program Com-

puters of the Faculty of Electrical Engineering.

## North Macedonia

The greatest efforts in the process of developing and implementing AI and advanced technologies in **North Macedonia** can be observed among representatives of 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.

Apart from them, worth mentioning are the North Macedonia CIRT agency (MKD-CIRT), Agency for Personal Data Protection, and the Agency for Electronic Communications (regulatory body). Others are the Ministry of Education and Science, The Bureau for Public Procurement, Public Revenue Office, the Customs Administration (which is under the Ministry of Finance), to name a few. We should also mention the Metamorphosis Foundation as a representative of CSO.

## Conclusion

We have included answers of 17 experts from the region who we asked the question: How do you see the capacity of your government to implement AI/advanced technologies in the public sector? All experts had a similar answer to the presented question: **- Low or non-existent capacity tied with low capability**. However there is a slight difference between analysed countries. In some of them, like Slovenia, there are examples of successful implementation of AI and advanced technologies in the public sector. Other than some isolated examples of successful implementation of AI

and advanced technologies in the public sector in specific country, all interviewed experts agreed that their **countries are dealing with the lack of systematic approach to implementation of AI and advanced technologies in the public sector**, without a clearly defined agenda with specific details about capacity and mandate aspects and entrust actors for the process. In almost all countries analysed we have also identified a **problem with human capacities for implementation of AI/advanced technologies in public sector** since there are no incentives for the young people with proper education to get a job in the public sector, while on the other hand, already employed staff do not have the knowledge and skills to engage in this process.

Overall we can conclude that in all the countries analysed, with the exception of Bosnia and Herzegovina, there is a **certain number of actors that have a mandate to deal with the implementation of AI/advanced technologies**. Especially in those with developed strategies in the field of AI/advanced technologies. However, it seems that **their mandate is only formally determined, and that very few actors are really involved in this process**. One of the main conclusions of the experts is that the **capacities of individual countries in this area are very scarce**, and that additional investment in the process of implementation of AI/advanced technologies in the public sector is much needed.

Observing all the analysed countries and the general situation in them when it comes to mandate 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 analysed countries, 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 Hungary, Montenegro, Slovenia, and Serbia, we have noticed a certain level of cooperation between the private and public sectors. In six out of ten countries we have identified representatives of CSO and private sector. However, **we cannot say that any particular country has developed a reliable network of actors to deal with implementation of advanced technologies and AI**.

# Final Remarks

All countries included in our research lack capacities for an adequate and successful implementation of AI/advanced technologies. Some countries are in a better position compared to others, most notably EU members seem to be more ready for the implementation of AI/advanced technologies. However, by mapping examples of use of advanced technologies and analysing them in more detail, we can conclude that none of the observed countries are ready for implementing such solutions in a manner that would not impact human rights negatively of either their own citizens or persons from third countries. Moreover, governments have not developed a reliable network of actors to deal with implementation of advanced technologies and AI. It seems that, even though most of them have necessary legislation that is observed to be a good basis for the implementation of AI/advanced technology, none of the countries have the capacities to use this technology in a way that would not at the same time be damaging for their citizens, especially vulnerable groups, or citizens of other countries.

Based on the findings in this report, the following recommendations can be provided:

1. Countries on the path of joining the EU should 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.

2. Strategies and policies in the areas of AI and application of advanced technologies should be adopted with realistic goals for implementation in mind, and with questions of ethics and

human rights taken into consideration.

3. When implementing 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. Stockpiling technology and equipment with known negative effects on human rights and freedoms, especially those which could lead to militarisation of law enforcement agencies, needs to be stopped.