A GUIDEBOOK FOR DIGITAL RIGHTS ACTIVISTS IN THE WESTERN BALKANS

2024

The Guidebook for Digital Rights Activists in the Western Balkans was developed by Share Foundation in Serbia, Center for Science and Innovation for Development (SCiDEV) in Albania, and Youth Initiative for Human Rights in Kosovo.

This Guidebook is financed under the Regional Collaborative Project, supported by Open Society Foundation Serbia.

Table of Contents

I. INTRODUCTION

With the rapid advancement of digital technologies, the protection of human rights in the digital spaces is becoming more emergent and critical as ever. Digital rights are human rights in the digital sphere and include rights to privacy and personal data protection, freedom of expression, and access to information. As more of our personal, professional, and social lives are conducted online, the risks of surveillance, censorship, and violations of these rights have intensified, thus, making the protection and exercise of human rights in the digital world a prerequisite for healthy and sustainable development of democratic societies.

This Guidebook is developed to be used by activists and professionals throughout the Western Balkans, that work in safeguarding public interest and human rights in their local communities. It is conceptualized as a tool to guide them into becoming digital rights activists and facilitate mainstreaming of digital rights.
The Guidebook provides an overview of what digital rights are, examples of digital rights violations throughout the Western Balkans, legal and regulatory frameworks in place, a case study of successful activism, and recommendations for effective advocacy.

II. ON DIGITAL RIGHTS

A. WHAT ARE DIGITAL RIGHTS

Digital rights refer to the fundamental liberties that individuals possess in the digital sphere. These rights encompass principles such as freedom of expression, privacy, right/access to information, the right to participate in the digital society without discrimination, and any other human rights in the digital world. They profoundly impact daily life by shaping how people communicate, access information, and interact online.

In the context of democracy, digital rights play a crucial role. They enable citizens to engage in free speech, access diverse viewpoints, and participate in democratic processes through social media, online platforms, and digital communication. Upholding these rights is pivotal for protecting democracy by ensuring transparency, accountability, and equal participation in the digital age. They serve as safeguards against censorship, surveillance, and unfair limitations on information flow, fostering a more open and democratic society.

B. HOW TO UNDERSTAND DIGITAL RIGHTS

i. PERSONAL DATA PROTECTION [1]

The concept of data protection derives from a basic human right – the right to privacy. The right to private life implies control over information about us, that is control over whether and who will know what places we are visiting, what we are buying, where we live and with whom we are corresponding. Privacy is undeniably important for personal autonomy of every individual, and the threats it may face became ever more obvious online.

Protection of Personal Data in the Digital Space

With the development of technology there has been a greater flow and multiplication of data, most of it being personal data, that is information that can be related to a specific, identifiable person. Data protection concerns regulation of data processing (their collection, use and storage) in the service of protecting the privacy of individuals in the digital space. Today, personal data is deemed to be a valuable resource based on which companies make profits and states exercise control over citizens. Thus, maintaining privacy in the digital age is facing additional challenges. If the data is not adequately protected, if it is leaked or misused, our privacy is compromised.

Consequences for the Individual and Society

Dealing with data protection is essential to prevent or at least adequately sanction breaches such as data leaks, illegal surveillance of communications or unauthorized data processing. If situations such as theft of bank card numbers, or surveillance of our conversations on social networks were unregulated, it is clear that we would live in a world dominated by fear, where our freedoms would be significantly diminished. Additionally, the most marginalized among us would be even more threatened, e.g. if companies had an unrestrained right to process sensitive data such as race or gender, that data could be used for discriminatory purposes.

Protection Mechanisms

- The right to be informed: companies and organizations are obliged to explain what data they process, i.e. we have the right to know what data about us is collected and how it is used.
- The right of access: organizations are obliged to issue a copy of the information they have about us upon our request.
- The right to rectification: we have the right to demand correction of inaccurate data or completion of incomplete data.
- The right to erasure, i.e. right to be forgotten: this right is applicable in various cases, such as illegal data processing or when the purpose for data processing no longer exists.
- If a company or an organization wants to process data that is not necessary for the provision of a particular service or it is not prescribed by law, it must obtain our consent for processing, and we can always withdraw that consent.

ii. Freedom of Expression

Freedom of expression is compounded by the:

- Freedom to Hold Opinions: states must not try to indoctrinate their citizens and should not be allowed to distinguish between individuals holding one opinion or another.
- Freedom to Impart Information and Ideas: the freedom to express different opinions and ideas without fear or interference.
- Freedom to Receive Information and Ideas: the right to gather information and to seek information through all possible lawful sources.
- Access to Information: includes free access to information without interference from the state or other entities. However, this right should not be understood as absolute, as it carries both duties and responsibilities, and is subject to restrictions, such as the prohibition of hate speech.

Freedom of Expression in the Digital Space

With the emergence of the internet, the flow of communication between people has increased, especially having in mind that we can communicate with more people at the same time and that they can be located on different continents. In addition, the internet allows us a certain degree of anonymity, e.g. we can create profiles that do not reveal our identity, and because of that, many communicate much more freely in cyberspace, believing that the consequences of online behavior do not have to be the same as in the physical realm. Censorship that occurs through filtering and blocking of content, and is resorted to by various states and corporations, also represents a serious problem, as it prevents us

from freely accessing information. On the other hand, content can be edited not only through censorship, but also its placement can be changed, i.e. algorithms can decide which type of content will be visible to which user. As new ways of communication are created, and the number of ways to restrict them also increases, protecting freedom of expression in the digital context can therefore be particularly challenging.

Consequences for the Individual and Society

The lack of freedom of expression harms the entire society, since it prevents it from accessing various ideas or information that may be of public importance, i.e. which can lead to progress, or point out to certain social problems. On the other hand, freedom of expression also includes the regulation of potential manipulation and dissemination of false information. The restriction of freedom of speech in the form of combating hate speech, threats, belittling, etc., is also crucial, as such speech can provoke or increase the number of acts of violence and discrimination, damage the reputation and dignity, threaten the sense of freedom and security of individuals, silence members of minority groups, and reduce the cohesion of society as a whole.

Protection Mechanisms

- The right to access information: enforceable by law throughout the region, ensuring citizens' access to public information through submission of FOI requests.
- Access to independent bodies protecting freedom of expression: this includes addressing independent institutions like the Commissioner for Personal Data Protection and Access to Information, the Ombudsman, the Anti-Discrimination Commissioner, or the local legal system.
- The internet allows us to be not only users, but also producers of content, and this should be kept in mind when things that can be censored happen in our society (e.g. protests).
- If there is inaccessible content in the country in which we live, we can access them through e.g. Tor browser, which allows us anonymity and free access to the internet.
- If we think certain web pages will be inaccessible or deleted in the future, we can save them using tools like the Wayback Machine. This tool was made by the Internet Archive, a digital library whose goal is universal access to all knowledge.

- If someone insults us, threatens us or threatens our personal rights in another way, we need to inform our community, block and report the person in question to the platform where the attack occurred. If the attacks continue, we should turn to the competent authorities and insist on legal assistance and protection.
- One way to respond to silence is to talk even more. If we are silenced due to some criticism or disagreement, informing the general public about the given problem can give us back a sense of control over the situation.
- If we are a victim of hate speech, i.e. verbal attack based on racial, religious, national, sexual, political, trade union and some other affiliation or personal characteristic, we need to contact a relevant authority such as the police or the Commissioner for the Protection of Equality.

iii. THE RIGHT TO PARTICIPATE IN THE DIGITAL SOCIETY WITHOUT DISCRIMINATION

The Charter of Fundamental Rights of the European Union recognizes the right to access to public services as part of the right to good administration, protected through Article 41. Furthermore, Article 21, recognizes the right to nondiscrimination based on any ground, such as sex, race, color, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. While Articles 25 and 26, respectively, state the rights of elderly to lead a life of dignity and independence and participate in social and cultural life, and the right to benefit from measures designed to ensure their independence, social and occupational integration and participation in the life of the community. While it facilitates access to services for a part of the society, the rapid digitalisation of public service provision also increases the digital divide, risking to leave outside of access to services elderly, less digital literate and those who cannot have access to digital tools.
Furthermore, employment of electronic public consultation platforms, at times being the only way of including the public's opinion in policy making, seriously hinders the capacity of the upper mentioned categories to participate in such processes and express their opinion on laws and regulations that impact their lives.

Consequences for the Individual and Society

One of the immediate consequences of the violation of the right to participate in digital society concerns the exclusion of digitally vulnerable target groups from accessing public services. Also, violations of this right impose an unlawful financial burden on vulnerable groups who will need to pay third parties to facilitate their access to digital public services. Violation of the right to participate in digital society without discrimination impacts democracy by creating barriers of access to consultation processes, with impact citizens' lives.

Protection Mechanisms

- Community leaders/representatives and civil society organizations can approach independent bodies like the Anti-Discrimination Commissioner, or the Ombudsman, to request investigations, and reaction towards institutions that violate this right.
- Approach organizations/foundations that assist citizens to overcome the digital divide and barriers.
- Engage in awareness raising campaigns and advocacy campaigns directed to institutions on providing means and tools to facilitate the participation in the digital society.

C. AN OVERVIEW OF DIGITAL RIGHTS ACROSS WB6 ECONOMIES

Digitalization in the Western Balkans economies have advanced at great strides, offering an increasing myriad of opportunities for its populations, as well as threats. The EU accession process, although with different economies being at different stages, provides fertile ground for the improvement of legal and regulatory frameworks. Nevertheless, implementation of such legal and regulatory frameworks remains a challenge.

In 2024, democracy in the Western Balkans deteriorated, with four economies characterized with democratic decline, and two stagnating[2]. Such deterioration of democracy and vast digitalisation raises concerns regarding the state of digital rights in these economies, and on human rights overall.

Fragmented legislation, weak implementation, and weak independent institutions have led to personal data violations, impediments in access to information, censorship, surveillance, and free speech violations throughout the region.

Balkan Investigative Reporting Network's Digital Rights Violations Annual Report 2022-2023 (Hereinafter, BIRN Annual DR Report) maps digital rights violations across the Western Balkans, Turkey, Croatia, Hungary, and Romania.

In Albania, there were 156 cases of digital rights violations, mostly being computer fraud, destruction and theft of data and programs, and hate speech and discrimination. Personal data leakages in Albania have marked the largest amount of personal data of citizens leaked in the region: data of 910,061 voters of Tirana County, enriched with political behavior data, was leaked online and made available for everyone to download. During campaigns, political candidates use official institutional social media accounts to campaign. Free and independent media is subject to distributed denial-of-service (DDoS) attacks and social media account takeover. Such is the case of Citizens Channel in April 2024, whose website was target of attempted DDoS attacks, followed by a successful in-path attack, where malicious scripts were injected in their server, redirecting their domain first to a porn site, and then to a website which automatically started downloading of malicious content[3].

In Kosovo were noted 191 violations, from misinformation to privacy breaches and scams. In March 2023, a video re-emerged in which a publicly known individual offered a financial reward for identifying protected witnesses testifying against former Kosovo Liberation Army leaders in court in The Hague. This endangered witness safety and constituted a severe violation of digital rights as well as being a criminal offense. The Specialist Prosecutor's Office in The Hague cited this case when denying early release to two defendants. However, the Prosecutor's Office took no legal action against the perpetrator.[4]

In Bosnia and Herzegovina, for 2022-2023, 157 cases of digital rights violations were recorded. In August 2023, Bosnia and Herzegovina was shaken by an unprecedented case of livestreamed femicide, in addition to various attacks on women both offline and online. The case of a teenager from Bijeljina who posted videos on TikTok threatening his Bosniak neighbors also attracted a lot of public attention, as did the case of two female students in Sarajevo who glorified convicted war criminal Ratko Mladic. These cases provoked a large amount of hate speech online and resulted in police action in Bijeljina, and the expulsion of the two students from the University of Sarajevo.[5]

[

103 violations were reported in Serbia, with cases of hate speech, private data breaches, and journalists and activists facing increasing threats. Escalation of violence and threats from the digital to the physical world has been noticed in Serbia. As BIRN Annual DR Report describes, after Sofija Todorovic, the programme director in NGO Youth Initiative for Human Rights in Serbia, called for Kosovo to be given membership of the United Nations, she was attacked on social media and the façade of the building where she lives was defaced with threatening graffiti including her full name and a sexist and misogynistic insult, as well including the letter 'Z', which symbolizes support for Russia's war against Ukraine.

In Montenegro were recorded 177 violations with the most recurrent being insults and unfounded accusations, publishing falsehoods and unverified information with the intention to damage reputation, hate speech and discrimination. BIRN Annual DR Report highlights the 2022 case of threatening Facebook messages sent by an ethnic Montenegrin to the daughter of Sinisa Lukovic, a journalist at Montenegrin daily newspaper Vijesti, warning that her father "will be expelled from the country for supporting Serbian policies". In January 2023, the Basic Court in Kotor sentenced the perpetrator to two months in prison and prohibited any contact with the journalist's daughter.

144 cases were identified in North Macedonia, concerning online scams, data breaches and cybercrimes. The Report raises alarms on the increasing cases of personal data theft, with the authorities struggling to mount an effective response or prevent such incidents. It is stated in the report that: the modus operandi of the attacks involves exploiting stolen data to apply for quick loans online, all without the knowledge or consent of the unsuspecting victims. These victims, including a person with disabilities, a hospital nurse and a local farmer, amongst others, found themselves indebted to quick loan companies operating within the country. The consequences of the frauds committed by unknown perpetrators' actions have been exacerbated by exorbitant interest rates, causing victims' debts to balloon.

A focus on Albania, Serbia and Kosovo

- **Personal data protection (PDP) violations in the region:**

Albania

2021 was marked by serious personal data violation in Albania. A database containing personal data of 910,061 voters of Tirana County, enriched with political behavior data, was leaked online and made available to everyone for download. The database contained sensitive data, like the personal identification number, which is a unique number assigned to every Albanian citizen, foreign citizen, as well as every stateless person, with temporary/permanent residence, with certain economic ties by the civil status service; name and surname; father's name; date and place of birth; phone number; dwelling number; political preferences; voting behaviors; etc. In late 2021, personal data on the salaries of public and private sector employees, and license plate data were leaked. Notably, the personal identification number is present in all the leaked databases, making it easy to track an individual across them, creating threats for their physical and online security.

Low cybersecurity endangers personal data protection

In July 2022 Albania's digital public infrastructure was subject to a massive cyber-attack, which impaired the country's digital infrastructure, inhibited citizens' from accessing digital public services, and facilitated access to personal data of Albanian citizens. The data was then published online by attackers, where sensitive information such as government official emails, embassies' emails, and citizens' phone numbers were made public. Other attacks suffered in the subsequent months, with more data being leaked from other institutions.

Serbia

Multiple incidents in Serbia have revealed severe breaches of privacy and data protection, exposing personal and sensitive information of millions of citizens. In December 2014, a database containing personal information of over 5 million Serbian citizens was inadvertently published on the website of the Privatization Agency. The exposed data included personal identifiers and other sensitive information, and the database was promptly removed following intervention by the Commissioner. The Agency attributed the leak to a hacker attack on their server, filed a criminal complaint against an unknown perpetrator, and the Commissioner initiated a misdemeanor procedure. However, the Privatization Agency was later dissolved, and the misdemeanor procedure became time-barred.

On March 25, 2017, the public became aware of a large database containing detailed economic and political profiles of over 400,000 citizens from across Serbia. This database was reportedly used for political purposes, specifically to influence voting behavior, and was accessible on a public server. The data was meticulously sorted into 222 tables, covering various towns and villages in Serbia, constituting a severe breach of the principle of legality as it was collected and processed without a legal basis.

On June 28, 2021, the "Moja srednja škola" portal, used for final exams and high school admissions, was found to expose student names, attended primary schools, grades, and results through its website code, all linked to unique numerical IDs. This vulnerability allowed unauthorized access to sensitive educational data. The Commissioner for Information of Public Importance and Personal Data Protection announced they would supervise the Ministry of Education, Science, and Technological Development to address this issue and ensure better data protection practices. Additionally, on March 8, 2021, numerous Telegram chat groups were found to be distributing explicit photos and videos of women without their consent, along with solicitations for sexual services. Some of these groups were named after Serbian cities, further identifying the victims and exacerbating the violation of their privacy. This led to a significant outcry and legal action, with a criminal complaint filed with the Prosecutor's Office for High-Tech Crime, and a suspect, believed to be the administrator of these Telegram groups, arrested on March 11, 2021.

Kosovo

Over the past years, businesses and institutions in Kosovo illegally collected and processed personal data of over 30,000 citizens. In 2022, the Information and Privacy Agency discovered 172 cases of data collection without proper consent, including photocopying ID cards and publishing personal information. The Regional Development Agency was fined EUR 30,000 for publishing data of over 20,000 citizens without consent. Other institutions like the Tax Administration and Ministry of Health also violated privacy laws. Private businesses were also found to violate laws, particularly in direct marketing and video surveillance. The Agency listed decisions on privacy breaches, highlighting the widespread issue of data protection violations in Kosovo.

Cybersecurity breaches endanger personal data protection

In September 2022, several public institutions, including the Post-Telecommunication authority, fell victim to cyber-threats. These attacks resulted in the temporary inaccessibility of the internal database and emails for the authority's internal officials. Moreover, the cyber-attack on Kosovo's Central Election Commission website during the parliamentary election on February 14, 2021, was very famous back then. During the attack, the English version of the website displayed ads for Viagra. The report suggests that the attacker(s) were not identified, and it seemed like they wanted to demonstrate how easily they could hack the official government website. Similar attacks continued in 2022. In September 2022, the e-Kosova platform, Kosovo Telecom, the Prime Minister's Office website, some ministries, the Kosovo Police, and many media outlets were targeted. The cyber-attack on Kosovo Telecom forced them to shut down all internet services in the country to handle and resolve the attack. Additionally, online media platforms were attacked too. Telegrafi.com, an online media portal in Kosovo, received an email from someone using the pseudonym "Anon Anterus," stating that the attack was a declaration of cyber warfare. This email was sent to many other institutions and media outlets in Kosovo as well.

- **Freedom of Expression violations**

Albania

Proactive Transparency and Access to Information is an obligation of Albanian Public Authorities according to Law no. 119/2014, an approach that fosters access to information. However, public institutions in the country fail to deliver proactive transparency. As a result, they do not implement the law on the right to information, which inhibits citizens' access to public information that should be readily available to them.

Restricting Freedom of Expression Rights

The 2022 attacks on critical infrastructure in the country led to serious data breaches, among which were data from the Albanian State Police. Hackers uploaded files with such data on a telegram channel, making it available to everyone for download and access. In September 2022, the Prosecutor’s General Office issued an order blocking the publication of any information from the leak, from any written, audiovisual or online media, citing reasons related to national security, citizens’ data protection, and investigative secrecy. Local and international journalists organizations reacted, considering the decision as a threat to freedom of expression and access to information, which also promotes censure on the media and journalists.

Kosovo

The Constitution of the Republic of Kosovo guarantees the right to freedom of expression[6], media freedom[7], and access to public documents[8]. Furthermore, Kosovo has voluntarily committed to upholding international human rights standards by directly implementing various human rights instruments and mandating its judicial system to align with decisions from the European Court of Human Rights[9].

Freedom of expression is further protected through the Civil Law against Defamation and Insult[10], which aims to balance freedom of expression with providing fair compensation to those harmed by defamation or insult. Although defamation was considered a criminal offense until 2012, the Kosovo Supreme Court directed lower courts to treat defamation cases as civil matters that year. Additionally, specific legislation, such as the Law on Access to Public Documents[11] and the Law on Independent Informants[12], provides further details on constitutional guarantees. Newspapers and online media are also subject to self-regulation, which includes obligations, such as prohibiting incitement of hatred.

While there exists a solid legal foundation addressing these matters, there are still reasons for concern. This sentiment is reflected in the 2023 EU Commission Report on Kosovo, which highlights ongoing concerns regarding physical attacks, threats, public smear campaigns, and hate speech. Of particular concern is the notable lack of freedom of expression in the northern part of Kosovo[13]. There were two complaints regarding the government's infringement on freedom of expression on social media platforms. One individual reported that their comments were deleted by the Ministry of Health and they were subsequently blocked from accessing the ministry's social media page in June and July. The second complaint involved a police officer who alleged being suspended from duty after posting on Facebook about the government's purported withholding of overtime pay from police officers to save money.

Serbia

In Serbia, citizens frequently face reprisals and verbal attacks for expressing their views on social media. There have been numerous instances where individuals have been detained or harassed for their online statements, reflecting a concerning trend of suppressing freedom of expression. A notable case involves members from the platform Dasezna!, who faced significant attacks and persecution from tabloids due to their reporting on incidents of police brutality.

This case exemplifies the use of media to discredit and intimidate those who bring critical issues to public attention. Moreover, cyber incidents such as Distributed Denial of Service (DDoS) attacks have been employed to disable websites and online services that promote freedom of expression and report on sensitive topics. For instance, the SOinfo portal experienced numerous DDoS attacks even after reporting them to authorities. These attacks aim to silence voices and restrict access to information, further illustrating the challenges faced by those who strive to maintain freedom of expression in Serbia.

- **The Right to Participate in Digital Society without Discrimination**

Albania

From 1 May 2022 public service offering counters were close and the largest majority of public services in Albania are provided online, creating a barrier to access public services for citizens with no skills and tools to use online services. Since then, a series of privately owned offices have been opened throughout the country, where citizens against predefined fees can get support to access said services. Such decision impairs the right of citizens to participate in digital society, and also puts unnecessary financial burdens on them.

Kosovo

In Kosovo, everyone deserves a fair chance in the digital world, but there are still big hurdles to overcome. While it is true that many of public services now are being offered online, through e-Kosova Platfrom, still many people, especially those in rural areas or with less money, struggle to get online. This makes it hard for them to do things like use online services, learn online, or start businesses online. What's more, some groups face unfair treatment online because of who they are. This could mean being bullied, left out, or treated differently because of their gender, ethnicity, or disability. To fix these problems, we need to make sure everyone has equal access to technology and the internet. This might mean bringing the internet to more places, teaching people how to use tech, and making sure everyone is treated fairly online.

Serbia

The transition to digital loyalty programs of super-market chains has unintentionally discriminated against older citizens in Serbia. As physical cards are phased out and mobile phone applications become mandatory for participation, older citizens, who may not be as adept at using technology, are excluded from these programs. This shift illustrates a digital divide where access to benefits is increasingly dependent on technological proficiency.

Consequently, many elderly individuals miss out on discounts and rewards, highlighting the need for more inclusive solutions that bridge this technological gap and ensure equitable access for all age groups.

III. THE LEGAL AND REGULATORY ASPECTS OF DIGITAL RIGHTS

A. EU FRAMEWORK ON DIGITAL RIGHTS

Taking into consideration the expansion of our daily activity in the digital environment, the European Parliament, the Council and the Commission (hereinafter referred to as the "EU") signed a Declaration on the Digital Rights and Principles to promote a sustainable and human-centric vision for the digital transformation and to ensure that the transition towards digitalization is shaped around the European values.

Accordingly, these principles are shaped around the following 6 topics, namely:

- **Putting people and their rights at the center of the digital transformation**

The scope of this principle is to make sure that technology serves and goes to the benefit of all people and empower them to pursue their aspirations. It should not infringe upon their security or fundamental rights. This principle acquires added value, in the circumstances where the human importance is being emptied and there is a constant risk for the overcome of the human by the technology.

Digital technologies should protect people's rights, support democracies, and ensure that all digital players act responsibly and safely.

When we talk about technology nowadays, we cannot help from thinking about AI and algorithmic solutions. In practical terms this principle stands to ensure that AI does not overcome people but instead be at their service and benefit. Therefore, the focus of the EU, of the CoE or other international organizations is in constant increase towards adoption of appropriate measures aiming to address practical implementation of this principle. For instance, the CoE pays constant attention in this regard, upon adopting Guidelines that can be on their turn adopted or serve as a guideline for domestic institutions of single countries to address this issue.

- **Supporting solidarity and inclusion**

Based on this principle everyone should have access to technology, and this access should be inclusive, and promote EU fundamental rights. In this context, technology should not divide, but instead be inclusive. Everyone should have access to the internet, to digital skills, to digital public services and to fair working conditions.

The Declaration proposes rights in a number of key areas to ensure that nobody is left behind by the digital transformation, making sure that extra efforts are taken to include elderly people, people living in rural areas, persons with disabilities, people in marginalized groups, vulnerable or disenfranchised people and those who act on their behalf.

People living in remote areas or elderly people might be prevented from accessing digital public services due to difficulties of accession to the internet or due to lack of digital skills. The purpose of this principle is therefore to overcome these barriers and ensure equal opportunities for any group of population.

- **Ensuring freedom of choice online**

People should benefit from a fair online environment, be safe from illegal and harmful online content and be empowered when they interact with new and evolving technologies like artificial intelligence. In this context, everyone should be empowered to make their own, informed choices online. This includes when interacting with artificial intelligence and algorithms. The declaration seeks to guarantee this by promoting human-centric, trustworthy and ethical artificial intelligence systems, which are used in line with EU values. And, it pushes for more transparency around the use of algorithms and artificial intelligence.

In this case, the principles promoted by the Declaration on Digital Rights and Principles clearly interact with the provisions of the GDPR (General Data Protection Regulation). Specifically, the GDPR provides for the right of the data subject (note: the term “data subject” is to indicate any person/owner of personal data) not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affecting him or her.

As a response to this right of the data subject, the EU legislator provides that the data controller (i.e., the entity determining modalities, purposes and means of processing of personal data) should implement suitable measures to safeguard

the data subject's rights, freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

Freedom of choice also includes being free to choose which online services we use, based on objective, transparent and reliable information. This in turn involves making sure everyone is empowered to compete and innovate in the digital world.

The right to obtain transparent information is also promoted and regulated in a detailed fashion under articles 12 – 14 of the GDPR, which put the emphasis on the transparency of the information to be provided to data subjects, in connection with the processing of their data.

- **Fostering participation in the digital public space**

Citizens should be able to participate in the democratic processes at all levels and have control over their own data.

This principle involves two constitutional rights and freedoms, recognized respectively by two important pieces of legislation in the international scope, the GDPR and the European Convention of Human Rights (ECHR). These two constitutional rights and freedoms at times are bifold and restrict one another, and the proper interpretation and understanding of the boundaries of the co-existence of these constitutional freedoms and rights are very tricky, in order to achieve the necessary balance between these constitutional rights.

The Right of Access to their own data is explicitly recognized and regulated under article 15 of the GDPR, which explicitly provides that the data subject is entitled to obtain information from the data controller, whether personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject, or to object to such processing;

- the right to lodge a complaint with a supervisory authority, which in the case of Albania is the Commissioner;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling.

In those cases when the processing includes or consists of the transfer of the data towards foreign countries or an international organization, the data subject is entitled to be informed of the appropriate safeguards undertaken by the data controller relating to the transfer.

As regards the right to participation, in the international range, it is recognized by the European Convention on Human Rights, and it is enshrined in article 8, which regulates among others freedom of information. The freedom of information is the instrument that permits citizens to participate in the democratic processes of the country and to build their own standpoint regarding the running of the trust, provided by citizens through vote.

The digital principles also highlight the need to create a digital environment that protects people from disinformation, information manipulation and other forms of harmful content, including harassment and gender-based violence. Also, it supports access to digital content that reflects our cultural and linguistic diversity.

- **Increasing safety, security and empowerment of individuals**

The digital environment should be safe and secure. All users, from childhood to old age, should be empowered and protected.

Everyone should have access to safe, secure and privacy-protective digital technologies, products and services. The digital principles commit to protecting the interests of people, businesses and public services against cybercrime, and confronting those that seek to undermine the security and integrity of the online environment.

The declaration calls for everyone to have effective control over their personal and non-personal data, in line with EU law. It pays specific attention to children and young people, who should feel safe and empowered online. Security of the digital environment occupies an important space in the GDPR, which has inter alia specifically provided thereof in article 32.

- **Promoting the sustainability of the digital future**

Digital devices should support sustainability and the green transition. People need to know about the environmental impact and energy consumption of their devices.
The digital and green transitions are closely linked. While digital technologies offer many solutions for climate change, guarantee must be offered that they do not contribute to the problem themselves. Digital products and services should be designed, produced, and disposed of in a way that reduces their impact on the environment and society.

It is obvious from the picture provided herein above, that the European digital rights and principles complement existing rights, such as data protection, and other rights and freedoms provided under the Charter of Fundamental Rights, including but not limited to freedom of information and freedom of expression. Safety in the digital environment and building an appropriate response to the challenges that emerged due to the rapid development of technology have led to the adoption of the GDPR by the European Parliament, and the Convention 108 + by the Council of Europe. The purpose of the Declaration seems to be addressing these challenges as well.

B. How GDPR can help, if implemented properly.

A short note on the need to push for proper implementation of laws and legal provisions

- **Promoting the sustainability of the digital future**

GDPR serves as a powerful shield for protecting people's privacy and data rights. It gives individuals more control over how their personal information is used. For it to function effectively, companies/organizations/others need to follow its rules, like getting permission before collecting data, being clear about how data is used, and using strong security to prevent data leaks. If done right, this builds trust with users, reduces the risk of data breaches, and helps avoid legal issues.
However, proper implementation of laws and regulations remains an issue throughout the Western Balkans countries, making the effects of legal measures weak. The alignment of the domestic legislation with the GDPR is expected to improve the data protection climate in the region, seen from the investors' perspective, at least from a legal-material point of view.
The new categories of rights introduced by the GDPR (i.e., right to be forgotten and right to data portability) acquire greater importance in the context of the digital reality that we are facing.

Specifically, the right to be forgotten enables data subjects/individuals to ask any data controller (especially when it comes to search engines) to delete any personal data processed in relation to him/her, which is not relevant anymore and which has an adverse impact on his/her personal sphere. Data protection culture is expected to enhance among data controllers and data protection is expected to acquire greater importance, considering the principles of privacy by design and by default introduced by the GDPR.

The GDPR introduces the role of data protection officer as mandatory, in this context job opportunities could be created for young professionals investing for knowledge acquisition in this area. GDPR implementation will require a lot of efforts from public and private institutions, and the support of civil society organizations is highly important.

Directive on the Security of Network and Information Systems (NIS)
Established in July 2016, the NIS Directive aims to boost cybersecurity in the EU. It focuses on enhancing national capabilities, fostering collaboration among member states, and integrating cybersecurity into organizations. The directive applies to essential service operators and relevant digital service providers. While it has positively influenced cybersecurity approaches, challenges and a fragmented approach at the member state level exist. The expanding digital landscape and recent events like the global pandemic and cyber warfare have led to an increased threat landscape and more cyberattacks on organizations and member states.

Directive on privacy and electronic communications
The Directive on privacy and electronic communications, also known as the e-Privacy Directive, establishes regulations for handling personal data and ensuring privacy in electronic communications networks. It outlines rules for securing personal data, reporting data breaches, and maintaining communication confidentiality. Electronic communication service providers are obligated to limit access to personal data to authorized individuals and implement measures to prevent data destruction, loss, or accidental damage.

In cases where there is a heightened risk to the security of the communication network, operators must inform subscribers about the potential risk. Despite security measures, if a breach occurs, operators must report it to the national authority responsible for implementing the directive. In certain situations, operators may also be required to notify individuals about personal data breaches, particularly if the breach could negatively impact their data or privacy.

Regulation No. 45/2001

As the Data Protection Directive could apply only to EU member states, an additional legal instrument was needed to establish data protection for the processing of personal data by EU institutions and bodies. Regulation (EC) No. 45/2001 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community, and on the free movement of such data (EU Institutions Data Protection Regulation) fulfills this task.[14]

Regulation No. 45/2001 mirrors the principles of the general EU data protection regulations, and applies them to data processing by EU institutions. It establishes the European Data Protection Supervisor (EDPS) as an independent authority to oversee its application. The EDPS monitors personal data processing within EU institutions, investigates complaints about potential breaches, and provides advice on data protection matters.

In January 2017, the European Commission presented a proposal for a new regulation on data processing by EU institutions, which will repeal the current regulation. As with the reform of the e-Privacy Directive, the reform of Regulation No. 45/2001 will modernize and align its rules with the new data protection regime, established under the General Data Protection Regulation (GDPR).

C. REGULATORY AND LEGAL FRAMEWORK IN THE WESTERN BALKANS THAT CONCERN DIGITAL RIGHTS

The Western Balkans economies overall have made advancements in developing legal and regulatory frameworks, that protect digital rights and freedoms. The constitutions of all economies, although to different extents, guarantee the right to privacy and freedom of expression.

Serbia is the first economy in the Western Balkans to harmonize its data protection law with GDPR, and passed law "On Personal Data Protection" ("Official Gazette of RS" No. 87/2018). However, the EC, through its EC Serbia 2023 Report[15] recognizes a series of issues regarding the law, highlighting: "... the law is insufficient with regards to penalties and difficult to implement in practice. This is because it does not further elaborate on the principles provided by the GDPR, and the provisions regulating processing of personal data by law enforcement authorities are scattered across a number of articles in the law."

The report further analyses the implementation of the law by highlighting issues related to the low number of appointments of designated data protection officers and court enforcement of this law, following complaints on personal data violations including data leaks to the media, which remain limited.

Access to information in Serbia is regulated by Law on Free Access to Information of Public Importance ("Official Gazette RS" No. 120/04).

The Commissioner for Information of Public Importance and Personal Data Protection is the independent national body that protects the right to free access to information of public importance and personal data protection in Serbia.

Reach out to the Commissioner for Information of Public Importance and Personal Data Protection for issues related to Access to Information here, and Personal Data Protection here.

Serbia has signed and ratified the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223)[16].

In **Albania**, data protection is ensured by law no. 9887, dated 10.03.2008, "On Personal Data Protection", as amended. A new law on data protection, aligned with the GDPR, has been prepared, and still has to be passed in Parliament for approval. Currently, freedom of expression in Albania is safeguarded by law no. 119/2014 "On the right to information", as amended. The 2023 amendments to the law in the country were welcomed, however, concerns remain on its proper implementation. The EC Albania 2023 report[17] highlights "Implementation of the right of access to public information needs to be further strengthened."

The Commissioner on Access to Information and Personal Data Protection is the independent body that protects access to information and personal data protection in Albania.

You can submit a complaint to the Commissioner on Access to Information and Personal Data Protection on the right to information, personal data protection, open data, information reuse and public consultation and announcement through this link.

Albania has signed and ratified the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).

In **Kosovo** personal data protection is regulated by Law N. 06/L -082 On Protection of Personal Data, entered into force in February 2019, which transposes the GDPR.

Access to public documents is guaranteed by Law No. 06/L -081 "On Access to Public Documents". The EC Kosovo 2023 Report[18] highlights that "Despite improvements in the implementation of laws relevant to access to public documents, journalists still encounter some obstacles, in particular due to delays or denials of access by public institutions, including the government."

The Information and Privacy Agency is the independent body that oversees the implementation of personal data protection and access to public information legislation.

You can submit a complaint to the Information and Privacy Agency here.

Bosnia and Herzegovina lags in approximating its personal data protection legislation with the acquis. Personal data protection is regulated by the Law on Protection of Personal Data ("Official Gazette of Bosnia and Herzegovina", 49/06, 76/11 and 89/11).

The Personal Data Protection Agency is the independent body that is in charge of the supervision of the implementation of the Law on personal Data Protection and all tasks resulting from it. However, the agency faces different challenges, as highlighted by the EC's Bosnia and Herzegovina 2023 Report:[19] "The Agency needs to better balance the protection of privacy with the general public interest, notably media freedom, electoral integrity, and the fight against corruption."

Access to information in Bosnia and Herzegovina is regulated by Law on Freedom of Access to Information at the Level of Bosnia and Herzegovina Institutions, of August 2023. The EC's 2023 Report on Bosnia and Herzegovina points out in regard to the upper mentioned law: "The independence of the appeal process still needs to be brought in line with international and European standards..."

"…. Rules on data protection and access to information are still interpreted in a way that protects private rather than public interests and such rights are inconsistently ensured across government levels."

Furthermore, the report emphasizes: "Legislation on freedom of access to information at state and entity level needs to be aligned with international and European standards."

Data holders can find information on how to reach out to the Personal Data Protection Agency here.

Bosnia and Herzegovina has signed and ratified the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).

In **North Macedonia** Law no. 42/20 "On Personal Data Protection" in 2020[20] (Official Gazette of the Republic of North Macedonia, No. 42/20), is aligned with the GDPR.

The Personal Data Protection Agency is the independent body in charge of strengthening, promoting and protecting citizens' data.

Visit this page to learn how reach to the Personal Data Protection Agency and submit a request.

North Macedonia has signed and ratified the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).

The Law on Free Access to Public Information regulates the conditions, manner and procedure for exercising the right to free access to public information in North Macedonia. The EC 2023 Report on North Macedonia[21] notes that "The proactive disclosure of information and datasets on official websites needs to be further encouraged, in particular at local level."

The Agency for Protection of the Right to Free Access to Public Information is an independent body mandated to ensure proper implementation of the law on free access to public information.

To submit a request for access to public information visit this link.
To submit a complaint to the Agency visit this link.
An e-portal is also available to citizens, to submit requests, browse through requests for public information and institution's responses or submit complaints. To use the portal you have to set up a user profile.

In **Montenegro**, the law governing personal data protection is the Law on Personal Data Protection ("Official Gazette of Montenegro", no. 079/08 dated 23.12.2008, 070/09 dated 21.10.2009, 044/12 dated 09.08.2012, 022/17 dated 03.04.2017). A new law in line with GDPR has still to be passed.

Montenegro still has to align the law on access to information with the acquis, although the preparation and consultation process has already taken years, as the EC 2023 Report on Montenegro[22] states.

The Agency for Personal Data Protection and Free Access to Information is the independent body responsible for proper implementation and oversight of data protection and access to information laws and regulations.

Reach out to the Agency for Personal Data Protection and Free Access to Information for issues related to Access to Information here, and Personal Data Protection here.

D. AI AND DIGITAL RIGHTS: A LIGHT REFLECTION ON AI ACT IMPLICATIONS FOR THE WESTERN BALKANS

Defining Artificial Intelligence precisely poses a challenge, but it is generally understood as a diverse set of technologies and approaches. It encompasses automation, machine learning, algorithmic decision-making, and neural network processing. AI relies on input from both machines and humans to generate processes and outcomes that contribute to decision-making[23].

On Friday, December 8, 2023, following months of intense trilogue negotiations, the European Parliament and Council reached a political agreement on the European Union's Artificial Intelligence Act ("EU AI Act"). This groundbreaking Act, praised by European Commission President Ursula von der Leyen as a "global first," marks a historic milestone, positioning the EU at the forefront of AI regulation. It is hailed as the "very first continent to set clear rules for the use of AI."

With this significant legislation, the EU aims to establish a broad and comprehensive legal framework for the regulation of AI systems throughout the EU. The primary objectives include ensuring the safety of AI systems and upholding fundamental rights and EU values, while also fostering AI investment and innovation in Europe. Following the finalization of the consolidated text in the coming weeks, the majority of the EU AI Act's provisions will take effect two years after its entry into force.

To maintain competitiveness, the six governments of the Western Balkans countries need to narrow the disparity with developed nations, by establishing legal, technological, and industrial frameworks for the effective integration of artificial intelligence. While there have been initial efforts by these governments to adopt regulations and devise strategies for AI implementation, the practical execution of these initiatives has been somewhat limited.

In the Western Balkans region, the utilization of AI in public services is still in its early stages. Developing robust capabilities is essential, not only for technological advancement but also as a fundamental prerequisite for the responsible deployment of AI that respects human rights. Given AI's heavy reliance on personal information, there is a significant risk to privacy rights. Technologies like biometrics, especially facial recognition, have the potential to continuously track individuals. In the absence of well-defined regulations, the deployment of AI and biometrics could worsen societal inequalities, placing certain communities, particularly racial minorities, at an increased risk of rights' violations.

Consider, for instance, public surveillance cameras equipped with facial recognition, scanning everyone on the streets without their knowledge, creating a constant record of people's movements. Without proper regulations, these scenarios underscore the potential for AI and biometrics to infringe upon individual rights and amplify existing societal disparities. Or, imagine smart computers making decisions that could incorrectly affect your taxes or claim you owe money when you do not. They might also wrongly label innocent people as troublemakers, causing problems in court or immigration. It is as if these programs identify certain areas as suspicious and label individuals as high-risk, even when they are not. This can infringe on people's rights. Moreover, social benefits could be denied due to biased information processed by the system. In essence, it is like AI acting as judge and jury, disrupting jobs, benefits, and fairness. Definitely not a cool scenario![24].

E. Fighting the silencing through SLAPPs

SLAPP stands for Strategic Litigation Against Public Participation. It acts as a legal weapon used by powerful individuals or companies to silence human rights defenders, activists, journalists, or anyone voicing criticism on matters of public interest. The goal of these proceedings is not to obtain a legal victory, which rarely materializes, but to incur procedural costs and to threaten disproportionate damages, in order to silence the critical voice of activists and to have a broader “chilling effect” on the work of journalists, NGOs, and civil society.[1]

Determining and characterizing these legal actions involves evaluating specific conditions[27]. Firstly, it is essential to inquire whether the legal proceedings are initiated by a private party. This distinction is crucial, as it sets apart these cases from traditional censorship, which typically involves governmental entities rather than private individuals or organizations. Secondly, one should investigate whether the legal action revolves around activities of public participation. Lastly, it is important to differentiate whether the lawsuit aims to silence, close down, or discourage such acts of public participation. By addressing these three questions, one can effectively define and pinpoint SLAPPs. If the response to all these questions is affirmative, it becomes highly probable that the legal action qualifies as a SLAPP lawsuit.

In the digital world, SLAPPs become even more tricky. What makes these legal threats particularly powerful is the global reach and ease of communication present in the digital sphere. Activists and journalists can quickly communicate their messages worldwide, which poses a challenge to those in power who may want to control the narrative or avoid scrutiny. Faced with the prospect of expensive legal proceedings, activists, human rights defenders, or journalists may opt to remove their content or refrain from expressing their opinions to avoid legal consequences. This fear of legal repercussions can lead to self-censorship, where individuals may hesitate to discuss crucial issues openly. This, in turn, hinders the free exchange of ideas and information that is vital for a healthy and informed society.

Recognizing the EU's lack of adequate legislation to tackle this matter, on the 27th of June 2023, the Legal Affairs Committee (JURI) of the European Parliament adopted its report[1] on the proposal for a directive concerning the protection of journalists and human rights defenders from SLAPPs. The main changes that the JURI report sets out include the introduction of a minimum

harmonization clause, expansions of the definitions of abusive court proceedings and public participation, and a wider scope for the cross-border element, necessary to trigger the directive.

In conclusion, these legal maneuvers, often wielded by powerful entities against those who dare to speak out on matters of public interest, strike at the very heart of democratic principles. SLAPPs serve as a tool to suppress dissent, muzzle whistleblowers, and intimidate journalists, activists, and human rights defenders into silence. The absence of robust legal protections against SLAPPs not only undermines freedom of speech and expression but also wears down the foundation of a transparent and accountable society. Legislation specifically addressing SLAPP lawsuits is imperative to ensure that individuals and organizations can engage in public discourse without the fear of facing harmful legal battles designed to bankrupt them into submission. By enacting legislation to curb SLAPPs, governments can safeguard the essential pillars of democracy, protect the integrity of public debate, and uphold the fundamental rights of citizens to participate in shaping their communities and holding power to account.

IV. RESEARCH AND ADVOCACY FOR DIGITAL RIGHTS

A. RESEARCHING DIGITAL RIGHTS

In the age of digital activism, the ability to effectively research and advocate for digital rights issues is crucial. The following chapter will guide young activists on utilizing various tools and techniques such as Freedom of Information (FOI) requests, Open-Source Intelligence (OSINT), and more to amplify their voices and drive change.

Section 1: Freedom of Information (FOI) Requests
Understanding FOI
FOIA or the Freedom of Information Act, is a federal law in the United States of America that provides individuals with the right to request access to records and information held by the federal government. The purpose of the FOIA is to promote transparency and accountability by allowing the public to access government documents and information.

Under the FOIA, government agencies are required to disclose requested information, with certain exceptions for classified or sensitive information. The process typically involves submitting a written request to the relevant government agency, specifying the records or information requested.

On a European level, the right to access information is protected by Article 15 of the Treaty on the Functioning of the European Union[28] which states that all citizens of EU countries have the right to access documents of the European Parliament, the Council, and the European Commission. This right encompasses the public's access to an array of public documents including legislative information, official documents, historical archives, and meeting minutes and agendas.

Considering that transparency is one of the EU's key principles, it requires the EU to disclose information on policy-making and spending, and to uphold the principle of freedom of information. The EU upholds this principle in its databases, namely through the "EUR-Lex" database, where you can search for treaties, legal acts, international agreements, law-making procedures, summaries of EU legislation, and case law. Through the "transparency register", you can search for organizations or register your own. The register includes information on interests being pursued, by whom, and with what budgets at the EU level. Also, "DORIE" can be used to access documents on EU, issued from the year 1946 to the present day. This includes legal instruments adopted by the EU institutions, minutes of meetings held by institutions and bodies, press releases, newspaper articles, speeches by European leaders, and internal Commission notes.

On a national level, the Government of Kosovo, based on Article 65 (1) of the Constitution of the Republic of Kosovo[29] adopted Law No. 06/L-081 on Access to Public Documents[30]. This law guarantees the right of every individual to access public documents produced, received, maintained, or controlled by public institutions, as well as the right to re-use public sector documents. Access to public documents shall be possible upon request. The request needs to be written clearly and concisely and be submitted either in person, in writing, orally, or electronically. There is no need to justify the reasoning behind the use of requested public documents whilst the decision for granting such a request needs to be made seven (7) days after receiving the request.

Submitting a Freedom of Information (FOI) request can be a straightforward process, but it is essential to ensure that your request is clear and complies with the relevant laws and guidelines. Here are some tips for submitting an effective FOI request:

1. Research the Process
Before submitting a request, familiarize yourself with the FOI process in the relevant jurisdiction. Each country or region may have its own rules and procedures, so make sure you understand the requirements specific to your area.

2. Identify the Correct Recipient
Determine the correct agency or department to which your FOI request should be addressed. Ensure that you have the right contact information, including the correct office, mailing address, and email.

3. Use Clear and Concise Language
Draft your request using clear and simple language. Be specific about the information you are seeking, and avoid unnecessary jargon. This helps ensure that your request is easily understood and processed.

4. Provide Sufficient Details
Include relevant details such as names, dates, and any other information that might help the public body locate the records you are requesting. The more precise your request, the easier it will be for the agency to fulfill it.

5. Check Timeframes
Be aware of any deadlines or timeframes associated with FOI requests in your jurisdiction. Some places may have specific time limits for responding to requests and knowing these can help you follow up appropriately.

6. Specify the Format
Indicate your preferred format for receiving the information, whether it's in electronic or paper form. This can help expedite the processing of your request.

7.Check for Fees
Some jurisdictions may charge fees for processing FOI requests. Be aware of any potential charges, and if applicable, inquire about the cost before submitting your request.

8. Provide Contact Information
Include your contact details in case the agency needs to get in touch with you for clarification or to provide the requested information.

9. Follow Up
Keep track of the status of your request. If you haven't received a response within the specified timeframe, follow up with the relevant agency to inquire about the status of your request.

10. Understand Exemptions
Be aware of any exemptions or limitations on the information you can request. Some information may be exempt from disclosure due to privacy concerns, national security, or other legal considerations.

Section 2: Open-Source Intelligence (OSINT)
OSINT, or Open Source Intelligence, is the act of gathering and analyzing publicly available information that is open to all individuals. This information can be obtained from a variety of sources, including websites, social media platforms, public documents, articles, and more. Individuals, corporations, and government agencies frequently utilize it to gain intelligence and insights about a variety of topics, including people, organizations, events, and activities. It entails the systematic collection, analysis, and interpretation of publicly available data to produce actionable intelligence. OSINT is useful for a variety of applications, including security assessments, threat analysis, investigations, and decision-making. Therefore, it is vital to clarify that OSINT is based on information gathered lawfully and ethically from publicly accessible sources, and therefore does not entail hacking or any illegal activity.

How does open-source intelligence (OSINT) work?[31]
OSINT gathering involves collecting publicly available information from a wide range of sources, including social media, articles, government reports, research papers, and commercial databases. This procedure can be carried out manually by looking for and examining sources, or by using automated technologies that seek and collect information. Once the data has been acquired, it is processed, in order to remove duplicate, irrelevant, or incorrect information. This stage involves filtering and categorizing data based on relevance and importance.
The processed data is then examined to look for trends, patterns, and linkages. This may entail applying data visualization tools, data mining, and natural language processing to derive useful insights from the data.

The final step in the OSINT process is to disseminate intelligence to decision-makers. This can take the form of reports, briefings, or warnings, depending on the needs of the company.

Common OSINT techniques[32]

Open-source intelligence encompasses a wide range of techniques for collecting and analyzing publicly available information. Listed below are some OSINT techniques:

1. Search Engines

Search engines, such as Google, Bing, and Yahoo are valuable tools for gathering open-source intelligence. By using advanced search operators, analysts can quickly filter and refine search results to find relevant information.

2. Social Media

Social media platforms, such as Twitter, Facebook, and LinkedIn are valuable sources of OSINT. By monitoring and analyzing social media activity, analysts can gain insight into trends, sentiment, and potential threats.

3. Public Records

Public records, such as court documents, property records, and business filings are valuable sources of OSINT. By accessing these records, analysts can gather information on individuals, organizations, and other entities.

4. News Sources

News sources, such as newspapers, magazines, and online news outlets are valuable sources of OSINT. By monitoring and analyzing news articles, analysts can gain insight into current events, trends, and potential threats.

5. Web Scraping

Web scraping involves using software tools to extract data from websites. By scraping data from multiple websites, analysts can gather large amounts of data quickly and efficiently.

6.Data Analysis Tools

Data analysis tools, such as Excel, Tableau, and Rare are valuable for analyzing large datasets. By using these tools, analysts can identify patterns, trends, and relationships in the data.

B. ADVOCATING FOR DIGITAL RIGHTS

Section 1: What Does Advocacy for Digital Rights Mean?
At its core, advocacy is the embodiment of empowerment. It is the manifestation of a collective voice that resonates beyond individual capacities. It is about amplifying the concerns and rights of those who might otherwise go unheard. When engaging in advocacy for Digital Rights, one assumes the role of a guardian, not of a city, but of the expansive and complex digital world. The mission involves safeguarding the ethical and secure utilization of the internet.

In the context of Digital Rights, advocacy assumes the role of a digital watchdog, navigating the vast and sometimes treacherous landscapes of the online world. It entails not only raising awareness but actively participating in the ongoing dialogue surrounding the ethical, legal, and just use of digital platforms.

Section 2: Crafting a Strategic Approach
Initiating the path of advocating for Digital Rights extends beyond mere enthusiasm; it calls for the development of a well-thought-out Advocacy Plan. This plan serves as a detailed roadmap and it consists of the following elements:

1. Define Your Goal
Begin by clearly defining your advocacy goal. Do you seek legislative changes, policy improvements, or a heightened awareness of digital rights issues? Be specific, this clarity sets the foundation for your entire advocacy strategy.

2. Know Your Audience
Identify the primary recipients of your message. Whether it's government bodies, the general public, or specific organizations, understanding your audience helps tailor your communication approach.

3. Research Findings
Arm yourself with the data gathered through Freedom of Information requests (FOI), Open-Source Intelligence (OSINT), and/or others. This information becomes your weapon – use facts and evidence to fortify your case. A well-informed advocate is a powerful advocate.

Section 3: Tools for Advocacy

1. Social Media
Harness the power of platforms like Twitter/X, Instagram, and TikTok to disseminate your message widely. Just as superheroes signal for help, your social media channels serve as examples, drawing attention to the cause.

2. Petitions
Create online petitions to amass backing from citizens who support your cause. The more signatures you gather, the more substantial your voice becomes.

3. Infographics and Videos
Visual storytelling is a powerful advocacy tool. Develop infographics and videos that portray your cause. These visual aids simplify complex issues, making it easier for people to understand and rally behind your efforts.

4. Collaborate with Media
Reach out to news outlets by sending well-crafted press releases. This outreach includes newspapers, blogs, as well as influential figures in the digital space. Collaborating with media outlets will amplify the reach of your advocacy.

5. Team Up with Other Activists
Embrace a collaborative approach by partnering with fellow activists. Each person brings distinctive skills and perspectives, forming an actual force for driving change. The effectiveness of this collaborative effort comes from unity, magnifying the impact of advocacy initiatives.

CASE STUDY: THE MAKING OF AN ANTI-BIOMETRIC MASS SURVEILLANCE CAMPAIGN

The case study was written by Filip Milošević, SHARE Foundation. It depicts the work of a large team of experts, activists and citizens, gathered around the common aim of protecting and safeguarding their rights.

Background

In 2019, the government of Serbia bought a smart surveillance system from the Chinese company Huawei, which would consist in deploying 8,000 smart cameras around the city of Belgrade. Such decision was based on the argument that, through the employment of this technology, the city would become safer, and the cameras would contribute to fighting organized crime and terrorism.

This smart surveillance system was being set up in a climate of extensive government control, oppression of free speech and independent media, and an overall deteriorating democracy. Facial recognition of citizens without their knowledge and consent would further instill control on citizens and strengthen autocratic practices of the government.

Experts at SHARE Foundation, started asking questions to themselves, wondering what was the real purpose of the surveillance system? Why there was no prior public discussion? Was such mass surveillance system legal in Serbia? How would it affect the society? And how would those who cared, stop it?
Facing such reality, experts at SHARE Foundation, decided to engage in a broad-based campaign to rally citizens, help them understand the threats and risks of such system, and counter the attempts of the government in conducing large-scale surveillance of its citizens.

SHARE Foundation, a Belgrade based non-profit organization, working towards advancing human rights and freedoms online and promote positive values of an open and decentralized internet, as well as free access to information, knowledge and technology. SHARE Foundation's primary areas of activities are freedom of expression online, data privacy, digital security and open access to knowledge. SHARE Foundation extends its area of work beyond Serbia, to the Western Balkans, and European level as well.

1. Context analysis and research

To fully understand the extent of the smart surveillance system, SHARE Foundation sent FOI requests to the Ministry of Interior (MOI) of Serbia requesting: locations of the cameras, including the analysis based on which these locations were determined, details of the public procurement process and other relevant legal procedures.

A month later, the Ministry replied: the procurement documents were protected as "confidential." They did not provide any information on locations and analysis as asked through FOIs.

MOI not providing the exact information requested by SHARE Foundation was valuable information, and a key issue to present to the public.

Facing the silence of institutions, SHARE Foundation continued its research with publicly available information sources on similar projects worldwide, and found that Huawei, had published on their website a case study on the supplying of surveillance cameras to Serbia, with detailed information about their features and deployment. After analyzing and publishing the information found on Huawei website, the case study was removed from the latter. However, the SHARE Foundation team managed to retrieve a snapshot of the website from Archive Today and the Wayback Machine.

2.Communication with interested stakeholders

Reaching out to the community

The SHARE Team identified local stakeholders with interest in privacy, security and surveillance, and organized a small initial gathering, to raise awareness on the identified issue. From an initial small group of 15 people, they reached out to 30 more people.

Set up of campaign

After creating the first small group to reach out, the team created an initial campaign that consisted in:

-Creating a small micro-site

-Choosing a website name and registering a domain

-Running an initial social media push to build an organic community around the topic and campaign.

The initial microsite included information that was easy to read, links so people could read more, and a link to a form where people could say what they think, offer support, help, and establish contact. A link to a Telegram channel was also provided, so people could get in touch and learn more.
The site was called www.hiljadekamera.rs / #hiljadekamera ("thousands of cameras" in Serbian).

Street marketing
The team engaged in street marketing by printing out stickers to be disguised into official ones, so they could help citizens understand that they were under surveillance. A QR code was added to the stickers, to lead people to their website.

Explaining surveillance
To understand how citizens would react to being under surveillance, and explain it, the team joined an open art festival in Belgrade. They implemented a small installation and space intervention in order to embody the "chilling effect" among festivalgoers, by putting them under intrusive surveillance at times when they wanted to relax.

Engaging the community
The team decided to prepare a more comprehensive website to reach out to wider audiences, and asked community members to engage such process. They had over 50 submissions, and thus continued with creating a collaborative, sprint like writing and design event.

Reaching beyond the bubble
With the new website functioning https://hiljade.kamera.rs, with content in English, media picked up the stories, ensuring media appearances, and reaching out wider audiences.

Multimedia and public relations
Multimedia products were developed, such as a podcast, a short video documentary and a live-stream event. Different products ensured reaching out to different audiences. The team reports that the short video documentary was a huge success.

3. Outcomes

In 2021, the Ministry of Interior announced the new Draft Law on Internal Affairs, one that, among other things, contained provisions for legalizing a massive biometric surveillance system, and launched a consultation of the law on its website. SHARE joined a discussion event, sent their comments to the Ministry, and alerted international and community media. A heated debate followed the announcement of the law.

Four days after the deadline and with strong public opposition, an unexpected press release was issued by the Minister himself, stating that the withdrawal of the draft law on massive biometric surveillance system.

ANNEX 1: LEARN TO PROTECT YOUR DIGITAL RIGHTS

I. PRIVACY: AVOID SURVEILLANCE AND HARASSMENT (PRIVACY & CYBERSECURITY)

Privacy refers to a person's ability to keep aspects of their life private, away from public view. It stems from the fundamental right to be left alone and is considered a natural entitlement, forming the basis for legal protection. In many democratic societies, the right to privacy is enshrined in their constitutions, ensuring legal protection. Privacy holds significance because it is essential for other rights, like the right to freedom and personal autonomy. There exists a close link between privacy, freedom, and human dignity. Respecting someone's privacy means acknowledging their right to freedom and recognizing them as an independent individual.

While countries generally acknowledge data privacy as a fundamental right of citizens, there is often disagreement, especially when it comes to balancing privacy with national security interests. Widespread surveillance measures are sometimes justified in the name of national security, leading to tensions between safeguarding individual privacy and ensuring public safety. This conflict makes it challenging to establish universally accepted guidelines on data privacy and surveillance practices at the international level.

For example, the mayor of Pristina, announced plans to install security cameras equipped with advanced artificial intelligence at the start of this year. These cameras will be monitored by the Kosovo Police. He stated that the cameras will assist in identifying individuals engaged in activities such as littering, parking on sidewalks, or occupying prohibited areas. Furthermore, the system will aid in identifying individuals involved in thefts, assaults, and other criminal activities. The Information and Privacy Agency announced that the data recording system to be installed in the capital will not involve processing biometric characteristics. Instead, the Kosovo Police will manage the cameras and work on identifying individuals suspected of committing public order breaches and criminal offenses based on the images captured. The request for the purchase and placement of cameras in public spaces was initiated by the Police.

II. BASIC CYBER HYGIENE PRACTICES

Staying safe online is essential in today's digital world. Here are some practical tips to help you maintain good cyber hygiene and protect your personal information.

Create Strong, Unique Passwords for Each Account
Use a mix of letters, numbers, and symbols to create passwords that are hard to guess. Avoid using the same password for multiple accounts to keep your information secure.

Keep Your Devices Updated
Regularly update your operating system, apps, and software. These updates often include security patches that protect you from the latest cyber threats.

Install Antivirus Software
Equip your devices with reliable antivirus software to detect and remove malicious programs. This software acts as a shield against viruses, malware, and other cyber threats.

Beware of Phishing Attempts
Be cautious with emails and links, especially if they seem suspicious or come from unknown sources. Phishing scams trick you into revealing personal information by pretending to be legitimate messages.

Secure Your Home Wi-Fi
Protect your home network with a strong, unique password. This prevents unauthorized users from accessing your internet and potentially your personal information.

Back Up Important Data Regularly
Keep copies of your important files on an external drive or a cloud service. This ensures you don't lose valuable information if your device gets lost, stolen, or compromised.

Enable Two-Factor Authentication (2FA)
Use 2FA for an extra layer of security on your accounts. This requires a second form of verification, such as a code sent to your phone, in addition to your password.

Manage Your Social Media Privacy Settings
Adjust your privacy settings on social media platforms to control who can see your posts and personal information. This helps you maintain control over your digital footprint.

Be Cautious with Public Computers and Wi-Fi
Avoid accessing sensitive information, like bank accounts, on public computers or unsecured Wi-Fi networks. These can be less secure and more susceptible to hacking.

Use a Virtual Private Network (VPN)
A VPN encrypts your internet connection, making it more difficult for hackers to intercept your data. Use a VPN, especially when connected to public Wi-Fi, to keep your online activities private and secure.

Stay Informed About Cyber Threats
Keep up-to-date with the latest cybersecurity news and trends. Knowledge is power, and staying informed can help you recognize and avoid potential threats.

Be Mindful of Artificial Intelligence (AI) Tools
Be aware of how AI tools collect and use your data. Always review the privacy policies and permissions before using AI applications and ensure they come from reputable sources. AI can be used both for enhancing security and for malicious purposes, so stay informed about the tools you are using.

III. DIGITAL SECURITY AS A GATEKEEPER FOR DIGITAL RIGHTS' PROTECTION

We can approach security as an extremely important aspect in the lives of individuals, as it represents a form of resistance to an event or the behavior of others that can be threatening, i.e. it represents a certain protection against things that can harm us. In addition to the fact that security can be discussed in an individual context, for example, whether members of a sexual minority can walk freely on the street without fear of physical violence, security can also be discussed at the level of an organization or state.

Security in the Digital Space

Cyber attacks and cybercrime are becoming more and more present, with the prospect that their number and sophistication will only grow in the future. This requires dealing with security in the digital context, and it is necessary to constantly work on building the resilience of information systems and resistance to potential attacks and damage. Many basic activities of states and companies have spilled over into cyberspace. If we acknowledge that entire sectors such as transport, energy, health, etc. are dependent on digital technologies, it is clear that this makes them more fragile in one way – that is, the whole society and economy are exposed to attacks that can now also be of digital nature. Individuals can also be the target of cyber attacks. For example, if we are denied access to our accounts on different platforms, it may be a sign that our privacy and access to personal data is under threat, i.e. that someone has come into possession of our passwords. The Internet can also additionally expose us to potential harassment or stalking, which can be done through fake or anonymous accounts.

Consequences for the Individual and Society

If we do not work on strengthening digital security, both at the individual and organizational level, the effects of malicious attacks can cause increasing damage to individuals and entire societies. As many of the processes that take place in cyberspace affect a large number of people, the consequences of attacking them are potentially more far-reaching. Although we can all be under threat from cyber attacks, when we talk about cyber, i.e. digital security, just as when it comes to security in the physical space, some members of society are more vulnerable than others. Members of special categories – e.g. journalists who handle sensitive information, are a frequent target of cyber attacks. By attacking these journalists and removing content or stealing various data, hackers affect not only the representatives of this group, but also the wider society they work to inform.

Mechanisms for Protection

- In order to protect yourself from malware, a type of software that can steal or lock data, in addition to installing software which can identify it, it is crucial not to open emails from suspicious addresses, not to install unverified programs and not to trust unreliable sites.
- It is necessary to have a different password for each account, and it should be long and consist of different characters and symbols.
- Two-level authentication for accounts is a double verification of identity and represents an additional barrier for hackers.
- It is important to use reliable applications and update them regularly.

ANNEX 2: AN EXTENDED OVERVIEW OF REGULATORY AND LEGAL FRAMEWORKS IN ALBANIA AND KOSOVO ON DIGITAL RIGHTS

Albania

The right to data protection of a citizen (i.e., data subject) is explicitly provided for under article 35 of the Albanian Constitution, where it is unequivocally stated that the processing of personal data is based on consent of the data subject and/or law.

According to this constitutional provision, the processing of personal data (i.e., their collection, use and public disclosure) is carried out upon the informed consent of the data subject, unless otherwise provided for by specific letter of law.

Protection and processing of the personal data within the territory of the Republic of Albania is regulated under the provisions of the Data Protection Law, along with sublegal acts issued by the Information and Data Protection Commissioner, which is the competent authority that monitors and supervises the compliance of data controllers and/or data processors with the legislation in force.

The provisions of the Data Protection Law apply to the processing carried out through automatic means, or through other means, of personal data stored in a filing system, or which are intended to be part of a filing system.

The scope of the law includes inter alia, data controllers established in the Republic of Albania, as well as data controllers not established in Albania, but who make use of equipment situated in this country.

Pursuant to point 1 of article 31 of such law, it is considered as “personal data” any information relating to an identified or identifiable natural person directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that natural person.

By way of example, personal data are, without limitation, a person's name, surname, address, image/photograph/video footage, age, fingerprint, voice, phone number, email, curriculum vitae (CV), internet protocol (IP), or social media account, etc., of a data subject/individual.

The processing of personal data includes, but is not limited to, the collection, registration, organization, retention, adaption or change, transmission, disclosure, erasure or destruction of personal data, etc. Each of these actions constitutes a personal data processing in itself. Personal data processing is performed by the data controller and/or the data processor.

A data controller is a natural person or legal entity that determines the scope and manner of personal data processing, in accordance with the legislation in force, being bound to comply with the provisions of such legislation.

A data processor is any natural person or legal entity that processes personal data in the name of a data controller.

Article 5 in The Data Protection Law lays down the main principles of data protection, to be honored in any processing activity carried out by any data controller/processor; namely:

'**Lawfulness and fairness**': Lawful processing of personal data means that a controller may process personal data only under a specific legal basis. That might be the consent of the data subject, the conclusion of a contractual relationship, a legal obligation, legitimate interest, etc. (i.e., see letters (a) to (f) below).

Special emphasis when coming to the lawful processing of the personal data has to be put on the legal basis of processing sensitive data, as well as children's data; they enjoy special protection in legislation.

On the other hand, fair processing of personal data means taking into account the privacy expectations of the data subjects while collecting/processing their data, without misleading them to such an end, or by collecting/processing personal data in a way that causes unjustified harm to the data subject/individual. This means the controller must ensure that data subjects are treated fairly when they seek to exercise their rights (these include right to access, block, correct, erase, object processing, etc.).

‘**Purpose limitation**’: This principle implies that the collection of personal data should be done for specific purposes that are clearly determined and lawful, as well as the (further) processing in compliance with such purposes. For example, if personal data are processed within the ambit of a journalistic purpose (during an interview, etc.), these data cannot be further processed if the new purpose differs from the first one (i.e., for direct marketing purpose) – the so-called “function creep”.

If the new purpose is not compatible with the previous one, the further processing of data should be based again on a new legal basis (i.e., consent, legitimate interest, etc. – see letters (a) to (f) below).

By providing transparency about the purpose behind the use of personal data, individuals can gain a clear understanding of the intentions and actions surrounding their information. This clarity empowers them to make informed decisions, including on whether or not to share their data with you. Moreover, it enables individuals to exercise their rights and exert greater control over the handling of their data.

‘**Data minimization**’: This principle means that in order to achieve the purpose of processing, the controller should process only those personal data that are sufficient to such an end. Such personal information/data should relate to the purpose of their processing and not be excessive in relation to it. If you collect personal data beyond what it necessary to fulfil your intended purpose, individuals may exercise their right to request the deletion of their data (right to erasure). Conversely, if you hold insufficient data, you may face challenges in obtaining a comprehensive understanding of the relevant facts. In such cases, individuals have the right to request completion of any incomplete data (right to rectification).

‘**Accuracy**’: The accuracy principle means that personal data should be accurate, complete and, where necessary, kept up-to-date; every reasonable step must be taken to erase, complete or rectify any inaccurate or incomplete data, having regard to the purposes for which they are collected or for which they are further processed. Apart from being a crucial legal principle for data protection purposes, the accurate exploitation of data is crucial for any processing purpose.

‘**Storage limitation**’: Personal data should be kept in a form that permits the identification of individuals for no longer than it is necessary for the purposes for which the data are collected or further processed.

Apart the case of video surveillance, where the time limit is provided by the relevant instruction regulating the specific area, the data protection legislation does not provide explicit time limits for different categories of data. It is therefore incumbent on the controller to assess the purpose for which they are processing personal data and reasonably determine the appropriate period for retaining that data. When deciding on a suitable retention period, it is essential to consider the specific purpose behind the processing of the personal data. By conducting a thorough assessment, you can determine a reasonable time frame for retaining the data that aligns with your purpose and ensures compliance with data protection principles.

In order for the processing of personal data to be considered lawful, according to article 6 of the Data Protection Law, it should be carried out only in accordance with the legal criteria below:

(a)If the data subject has granted his/her consent to personal data processing;

(b) If the personal data processing is substantial for the fulfilment of a contract entered into by the data subject, or for the purpose of discussions or amendments to a project/ contract on the proposal of the data subject;

(c)To protect the vital interest of the data subject;

(d)To fulfil a legal obligation of the data controller;

(e)For the performance of a legal task of public interest or exercising an authority of the data controller, or third party, to which the personal data have been disclosed;

(f)If the personal data processing is substantial for the protection of legitimate interest of the data controller, data receiver or other interested persons, provided that such legitimate interest is not overridden by the data subject's right to the protection of their personal and private life.

A special treatment is reserved to the processing of sensitive data, as set out under article 7 of the Data Protection Law. This comprises any information related to an individual concerning his/her racial or ethnic origin, political opinion, membership of a trade union, philosophical belief or religion, criminal background, as well as data related to health and sexual life. The processing of sensitive data might take place, inter alia:

- if the data subject has granted his or her written consent;
- if it is in the vital interest of the latter or of another person (where the data subject is physically or mentally incapable of giving consent);
- if it is authorized by the competent authority for reasons of public interest;
- if it relates to personal data manifestly made public by the data subject or is necessary for the exercise or defense of a legal claim;
- or if it is required for purpose of preventive medicine, healthcare, etc.

Especially important in the context of personal data processing are the rights of the data subject, as laid down under articles 12-18 of the Data Protection Law. They include:

1. **Right of access.** Data subjects are entitled to obtain, free of charge, from the data controller (upon written request), confirmation of whether their personal data are being processed, information on the purposes of processing, as well as on the categories of processed data and the recipients to whom personal data are disclosed/disseminated. However, this right is not absolute and may be subject exercised, in line with the constitutional freedoms of information, the freedom of expression/press and professional secrecy. In addition, the right to access may be restricted if it could harm the public security interests, foreign policy, the country financial and economic interests and the criminal prevention or proceeding. When denying right of access, the controller should within 30 days explain the reason of such a denial and inform the data subject about his/her right to file a complaint to the Commissioner, who is entitled to check (on request of the data subject) whether the access denial is justified by the aforementioned reasons;

2. The right to request blocking, rectification or erasure of data. The data subject has the right to request blocking, rectification or deletion of his or her data, free of charge, whenever he or she becomes aware that data relating to him or her are inaccurate, false and incomplete, or have been processed in violation of the law's provisions;

Moreover, according to Article 18, when collecting personal data, the data controller is obliged to inform the data subject about, among others: the name of the controller; the purpose of personal data processing; the person that will process the personal data and the means of such processing; the persons or categories of persons to whom the personal data will be transmitted/disclosed; their right to access and rectify the personal data; the personal data retention period, etc. The right of information of the data subject corresponds to the obligation of the controller for information. The information of the data subject precedes his/her consent to personal data processing (i.e., informed consent).

However, considering the target group to whom this Guidebook is addressed, the use they make of social media and the volume of data they transmit through this channel of communications, it is worth to be mentioned that pursuant to letter b) of point 4 of article 4 of the Data Protection Law, any processing of personal data carried out exclusively for domestic and personal purposes, is exempted from the scope of the law.

Moreover, it is to be noted that the Data Protection Law has in its scope and focus the behavior of controllers and processors towards compliance with their obligations set out by the data protection legislation in force. To this effect, any administrative investigation shall be undertaken towards controllers/ processors.

Having said this, the Data Protection Law does not apply in the cases of unlawful use of data transmitted through social media, towards the person practicing this illicit behavior, as far as the latter is a natural personal and the processing is done merely for domestic or personal purposes.
In such cases, the Criminal Code will apply and will serve the purpose to restore the right to private life of the citizen, as it will be indicated herein below.

Nonetheless, the Data Protection Law may be invoked to address the platform or platforms where the unlawful processing/transmission of data is carried, search engines or any other controller to cease/processing/publication/ transmission and any other form of illicit processing of the data (i.e., pursuant to point 5 of article 3 of the law, “controller” means any natural or legal entity, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data in line with laws and sub legal acts regulating the specific area, and is liable/ accountable for fulfillment of the obligations arising out of the Law on Personal Data Protection).

The authority in charge to monitor and supervise implementation of the Data Protection Law is the Commissioner. Pursuant to article 30 of the Data Protection Law the Commissioner is entitled to:

- conduct administrative investigations and access any processing of personal data, as well as collect the entire necessary information for the fulfillment of its duty;
- issue blocking, erasure, destruction orders or suspend the illicit processing of personal data;
- issue instructions before any processing takes place and ensure publication thereof. In case that, in the course of the administrative investigation, the Information and Data Protection Commissioner observes that the specific contravention constitutes criminal offense, the case is transmitted to the law enforcement authorities for further steps.

As regards the level of approximation of the Data Protection Law with the acquis Communautaire, the Data Protection Law is fully approximated with Directive 95/46/EC.

On the other hand, the IDP Commissioner has already 'transposed', in virtue of its sublegal acts (i.e., instructions), several novelties introduced by GDPR, such as the mandatory position and the role of the data protection officer, the data impact assessment, the information security policy, the certification mechanism, etc.

Moreover, since November 2021, the Commissioner has filed with the Ministry of Justice the new draft law "On personal data protection" fully aligned with the GDPR. The draft has passed through the process of public consultation since July 2022 and is now in the process of review/consultation with the European Commission. Pursuant to the National Plan for European Integration, the draft is expected to be approved by the end of this year.

The draft was prepared in the framework of a twinning project, financed by the Delegation of the European Commission in Albania and technically assisted by the consortium of the Italian Supervisory Authority, Ludwig Boltzmann Institute for Human Rights, Austria and CSI Piemonte.

Based on the foregoing, considering the current direction of the Albanian legislation vis-à-vis GDPR, a brief overview on the GDPR and the main novelties it will introduce compared to the existing legislation in place is needed.
GDPR is the legal instrument that governs the processing of personal data in the European Union. As a regulation, it is a binding legislative act that is directly applicable and enforceable in its entirety across the EU. It represents the most important piece of legislation for each member state for guaranteeing data protection and the privacy rights of data subjects.

GDPR applies to controller/processors situated in the EU, as well as those situated outside of the EU that fulfills one of the following conditions:

- they offer goods or services to data subject in the EU; or
- monitor the behavior of data subjects in the EU.

Though widely misunderstood, GDPR does not protect only the data protection/privacy rights of EU citizens, but also those of non-EU citizens situated/residing in the EU.

In other words, if a controller, established/situated in Albania, monitors (i.e., interacts with or processes personal data unilaterally) the behaviors of a data subject situated/residing in the EU, that controller must comply with GDPR rules (extraterritoriality principle).
GDPR has repealed former Directive 95/46/EC, with which the Data Protection Law is fully aligned with, thus bringing data protection requirements to a considerably higher-quality level.

Some of the most important novelties of GDPR vis-à-vis Directive 95/46/EC (i.e., and also: the Data Protection Law) include the following:

- Extraterritoriality principle (as explained above).
- Principle of accountability. This is the core principle of GDPR, according to which any controller should not only comply with GDPR provisions (i.e., principles of lawfulness, accuracy, minimization, storage limitation, etc.), but bears also the burden of proof to demonstrate and evidence compliance therewith.
- Dedicated provisions/rules regarding the processing of personal data of minors (i.e., including the criteria for consent).
- Introduction of new categories of sensitive data (i.e., biometric and genetic data).

- Introduction of new categories of rights of data subjects (i.e., the right to be forgotten and right to data portability).
- Augmentation of the requirements of information obligations of the controller (i.e., for data processed directly by data subjects and those processed through third parties).
- Introduction of principles of privacy by design and by default. These principles mean that any system of personal data processing should be designed to address any personal data protection issue (i.e., data protection by design), including encryptions/pseudonymizations, and that these systems should be by default (i.e., automatically) data protection compliant/friendly and, therefore, not process data more than it is necessary to achieve the processing purpose (i.e., data minimization principle).
- Introduction of self-regulatory mechanisms, such as certification mechanism, codes of conduct, and binding corporate rules that apply only to international transfer of personal data to countries without adequacy level.
- Introduction of the obligation to carry out a data protection impact assessment before any processing activity, and/or whenever it changes.
- Introduction of the obligations to keep records of data processing activities.
- Introduction of the mandatory role of the data protection officer.
- Tightening the rules for international transfers.
- Increase administrative sanctions up to a maximum of EUR 20 million, or 4 per cent of the annual global turnover of a controller, whichever is higher.

Kosovo

The potential for EU integration has been a successful mechanism for standardizing legislation in all areas, as the countries aiming for EU accession, are anticipated to synchronize their data protection laws with the EU General Data Protection Regulation. Before Kosovo declared independence in February 2008, there was virtually no established legal and policy framework for cybersecurity. The development of such a framework started in the initial years of independence and is an ongoing process, evolving over time. Since joining the EU Digital Agenda for the Western Balkans in 2018, Kosovo has demonstrated a commitment to digitalisation through various strategies and initiatives.

The Ministry of Economy leads the implementation of the Digital Agenda. Starting in 2013, Kosovo embarked on a comprehensive Digital Agenda Strategy spanning 2013 to 2020. In 2023, a new strategy focused on boosting digital transformation in the ICT sector was introduced, emphasizing internet accessibility and robust infrastructure.

The Ministry of Economy, in collaboration with stakeholders, developed the Kosovo Draft Digital Agenda 2030 and its Action Plan. Approved in 2023, this strategic framework outlines five key objectives for shaping Kosovo's digital future: advanced and secure digital transformation, digital transformation of businesses, digitalization of public services, fostering digital skills and innovation, and strengthening the cybersecurity system.

Kosovo's Constitution ensures the right to privacy, as outlined in Article 36, which guarantees protection for personal data. While it is important to note that Law No. 04/L-145 on Government Bodies for the Information Society designates responsible bodies for developing information society services in Kosovo, outlining competencies, responsibilities, and the establishment of the AIS (Agency for Information Society). This law consolidates functions related to Information and Communication Technology (ICT) within Kosovo institutions. While, the Law no. 06/L-082 on Protection of Personal Data safeguards individuals' rights, privacy, and outlines responsibilities and punitive measures related to personal data processing. In compliance with the EU's General Data Protection Regulation (GDPR), it designates the Agency for Information and Privacy for monitoring data processing legitimacy.

According to the Law on Personal Data Protection a "data controller" is any person or entity, whether public or private, that decides how and why personal data is processed. On the other hand, a "processor" is a person or entity that processes personal data on behalf of the data controller. Overall, the law grants individuals rights such as accessing, correcting, and deleting their personal data. This law aims to ensure the protection of personal information in Kosovo.

However, as technology has advanced in Kosovo, concerns about data privacy have arisen due to limited awareness, underdeveloped institutions, and potential misuse of data. To address these issues, Kosovo's Assembly established the Information and Privacy Agency (IPA) in June 2021. The IPA oversees personal data protection and freedom of information, reporting to the National Assembly.

Additionally, the Kosovo government is developing its e-Government Strategy 2027, which prioritizes cybersecurity. Experts are contributing to this strategy, which is set for consultation and approval in 2023. This strategy aims to enhance cybersecurity measures across Kosovo.

REFERENCES

[1] The organization of information in this section follows the structure, and is based on a 2021 Publication of SHARE Foundation: Introduction to Digital Rights.

[2] Freedom House. (2024). Nations in transit 2024: Digital booklet. https://freedomhouse.org/sites/default/files/2024-04/NIT_2024_Digital_Booklet.pdf

[3] SCiDEV Center. (2024, April 10). The limited recount of cyberattacking media freedom. https://scidevcenter.org/2024/04/10/the-limited-recount-of-cyberattacking-media-freedom/

[4]https://birn.eu.com/wp-content/uploads/2023/12/01-BIRN-Digital-Rights-Violations-Annual-Report-2022-2023.pdf

[5] Balkan Investigative Reporting Network. (2023). Digital rights violations annual report 2022-2023. https://birn.eu.com/wp-content/uploads/2023/12/01-BIRN-Digital-Rights-Violations-Annual-Report-2022-2023.pdf

[6] Article 40, Constitution of the Republic of Kosovo, 15 June 2008, available at http://www.assembly-kosova.org/common/docs/Constitution1percent20ofpercent20thepercent20Republicpercent20ofpercent 20Kosovo.pdf

[7] Article 42, ibid.

[8] Article 41, ibid.

[9] Article 53, Ibid

[10] Law No. 02/L-65

[11] Law No. 04/L-044

[12] Law No. 04/L-137

[13] European Commission. (2023). Kosovo 2023 report (SWD(2023) 692 final). https://neighbourhood-enlargement.ec.europa.eu/document/download/760aacca-4e88-4667-8792-3ed08cdd65c3_en?filename=SWD_2023_692%20Kosovo%20report_0.pdf

[14] Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ 2001 L 8.

[15]European Commission. (2023). Serbia 2023 report (SWD(2023) 695 final). https://neighbourhood-enlargement.ec.europa.eu/document/download/9198cd1a-c8c9-4973-90ac-b6ba6bd72b53_en?filename=SWD_2023_695_Serbia.pdf
[16] Read more here: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=223
[17]European Commission. (2023). Albania 2023 report (SWD(2023) 690 final). https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_690%20Albania%20report.pdf
[18] European Commission. (2023). Kosovo 2023 report (SWD(2023) 692 final). https://neighbourhood-enlargement.ec.europa.eu/document/download/760aacca-4e88-4667-8792-3ed08cdd65c3_en?filename=SWD_2023_692%20Kosovo%20report_0.pdf
[19]European Commission. (2023). Bosnia and Herzegovina 2023 report (SWD(2023) 691 final). https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_691%20Bosnia%20and%20Herzegovina%20report.pdf
[20] Amended and supplemented in 2021, with "Law on Amending and Supplementing the Law on Personal Data Protection" (Official O.Gazette of the Republic of North Macedonia, No. 294/21)
[21]European Commission. (2023). North Macedonia 2023 report (SWD(2023) 693 final). https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_693%20North%20Macedonia%20report.pdf
[22] European Commission. (2023). Montenegro 2023 report (SWD(2023) 694 final). https://neighbourhood-enlargement.ec.europa.eu/document/download/e09b27af-427a-440b-a47a-ed5254aec169_en?filename=SWD_2023_694%20Montenegro%20report.pdf
[23] OECD, Artificial Intelligence in Society (Summary in English) (2019); Australia Human Rights Commission, Human Rights and Technology Final Report (2021) (Hereinafter Australia Human Rights Commission Report), p. 17.
[24]Report of the UN High Commissioner on The Right to Privacy in the Digital Age, paras 22-33.
[25] 9 R Abrams, 'Strategic Lawsuits against Public Participation (SLAPP)' (1989) 7 Pace Environmental Law Review 33.
[

[26]https://www.the-case.eu/slapps/
[27]
https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733668/EPRS_BRI(2022)733668_EN.pdf
[28]https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF
[29]https://gzk.rks-gov.net/ActDetail.aspx?ActID=3702
[30]https://gzk.rks-gov.net/ActDetail.aspx?ActID=20505
[31] Ibid
[32] Ibid

OPEN SOCIETY FOUNDATIONS
WESTERN BALKANS

SHARE FOUNDATION

scidev

YiHR