INTRODUCTION TO DIGITAL RIGHTS

SHARE FOUNDATION

DECEMBER, 2021.

CONTENT:

INTRODUCTION

Human rights apply equally on the internet and in the physical space.

Digital technologies have opened many new and interesting ways for expressing ideas, exchanging information, associating, protesting and other similar free citizens' activities, recognized as fundamental rights of all people. These rights enjoy universal protection and they belong to everyone, regardless of their background, status and other personal distinctions.

At the same time, the digitalization of our communication and daily affairs has also enabled the development of means for abuses and violations of rights. Intentionally or out of ignorance, driven by commercial interests or intent to establish control, various actors – states, corporations, political and other organizations – are often the perpetrators of censorship, privacy violations and discrimination on various grounds.

Although most of us today know how to use smart devices and download and publish content on online platforms, it may not always be clear which of these activities belong to the domain of protection, or in which cases we can talk about violation of rights. Do likes on Twitter, shares on Facebook or Google Search metadata constitute personal information? When does restricting access to a site turn into censorship? What fundamental human rights are threatened during the mass processing of biometric data in smart systems? Can the process of automated algorithmic decision making be discriminatory?

In order for citizens and civic organizations to be able to answer these and many other questions that await us with the wider application of even more complex technologies, they need more knowledge about digital rights – human rights in the digital environment. This handbook presents some of the basic concepts in this field, illustrated with practical examples from the Western Balkans region.

PERSONAL DATA PROTECTION

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 precisely 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.

EXAMPLES OF RIGHTS VIOLATIONS:

- A file with personal data of over 5 million citizens of one country has started circulating on social networks. The supervisory process determined that the data file was originally publicly available on one state agency's website from which it was downloaded. The agency in question defended itself by claiming that this occurred through unauthorized access to their server.
- Data such as names, phone numbers and locations of over half a billion accounts from one social network leaked to a hacker forum. However, it turned out that this leak was not a matter of error, but that the data was intentionally extracted with the help of a special software, which was made possible due to the social network's systemic failure.
- An international human rights organization had received lists of more than 50,000 mobile phones that were suspected of being the targets of potential espionage with the help of software that compromises the phone, extracts all data and activates a microphone to record conversations.
- Tens of thousands of men from the region exchanged intimate contents, i.e. pictures, videos and photos of women, including minors, via Telegram app. The members of the groups received the content either from their past partners or simply "downloaded" it from social networks and sent it to the groups, often with the disclosure of women's personal data.

- The media in one country published the details from a large database containing personal data of more than 910,000 voters. The list also included journalists, activists and other well-known individuals. Allegedly, these data were given to one political party to use during the election campaign.

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 where fear would reign and where we would all be less free. 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.

At this link you can view our short video on data protection.

DIGITAL SECURITY

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, 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.

EXAMPLES OF RIGHTS VIOLATIONS:

- A website was hacked a few hours after publishing an analysis that a state official's PhD dissertation was plagiarized. The attacks on the site continued over the following week, and site administrators informed the public that they had been under cyber attacks for years due to their politically inappropriate content.
- One municipality issued a statement that their archive was attacked by a virus that locks documents, i.e. prevents access to them. The virus was cited as the reason why the municipality could not issue any documents to the citizens and the problem was resolved within a few days, however, it is not clear whether the data were stolen in the meantime.
- The day after elections a website of one country's election commission was the target of a hacker attack for three hours. The attack did not cause major systemic damage, but it delayed the announcement of election results.
- Several thousand infected computers attacked the servers of portals that published the news about the privileges of the National Bank governor's daughter in one country. The pages on which the news was

published showed a 404 Not Found error, which indicates that the requested content does not exist at the given web address.

- An anonymous person registered a profile on a social network under the name and surname of a professor who is well known and respected in his local community. Then, through this profile, financial donations were requested. After the professor pointed out that someone had stolen his identity on this social network, the profile in question was suspended.
- The mayor of one city could not access his profile on a social network for days, so he informed the customer support about a possible hacker attack.
- The fraudsters used the name and photograph of a large bank's director to promote cryptocurrency-related services, attributing to him quotes he never said.

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, as they are working in order to inform the wider society.

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.
- We need to use reliable applications and update them regularly.

At this link you can access our short video on digital security.

For more tools that can strengthen digital security, you can visit this site.

FREEDOM OF EXPRESSION

Freedom of expression implies the freedom to express different opinions and ideas without fear or interference, but also 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, 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.

EXAMPLES OF RIGHTS VIOLATIONS:

- A journalist from an online media outlet was arrested in her own home over an article in which she wrote about poor working conditions and the lack of protective equipment for medical workers during the COVID-19 pandemic. She was detained for 48 hours, and the hospital announced that the journalist was spreading false information and upsetting the public.
- The administrators of a Facebook group, in which a picture of a flock of sheep captioned "Municipal Councilors" was posted, were fined after the court ruled that the post was insulting and humiliating.
- The MP of one country insulted certain politicians with sexist and vulgar messages on Twitter, called for the rape of an official and threatened to shoot his political opponents.
- After a human rights activist defended a person who was exposed to chauvinistic attacks, she herself became a victim of threats and attacks through social networks. Due to the feeling of not being safe she filed several criminal charges, however, the reaction of the authorities was absent, and the threats continued.
- One social network announced that it had deleted thousands of fake,

so-called "bot" accounts that served to promote the ruling parties in several countries.

- Several online media outlets' identities were stolen and copied by creating sites with almost identical domains and designs, which were then used to promote the work of the ruling party and confuse regular readers of authentic media outlets.

CONSEQUENCES FOR THE INDIVIDUAL AND SOCIETY:

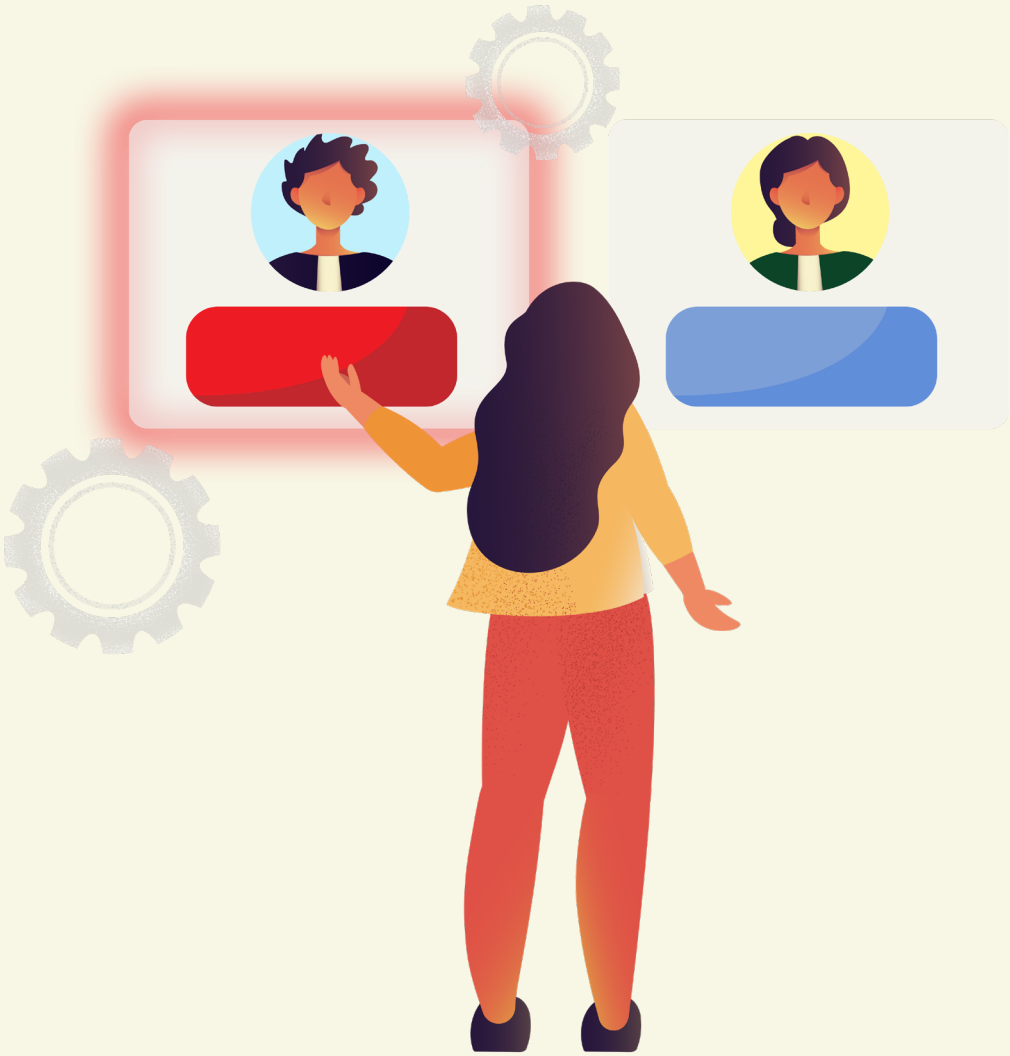
The lack of freedom of expression harms the entire society since it prevents it from accessing various ideas or information that may be of public importance, i.e. which can lead to progress or point out to certain social problems. On the other hand, freedom of expression also includes the regulation of potential manipulation and dissemination of false information. 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 or 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 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 are inaccessible contents 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 would 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 and block and report the person in question to the platform where the attack occured. 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.

At this link you can access our short video on freedom of expression.



DIGITAL RIGHTS IN THE REGION

The SHARE Foundation has established permanent monitoring of the rights and liberties of citizens in the digital environment, and publishes annual reports of its findings. This process of monitoring and documenting violations of digital rights SHARE began in Serbia in 2014, and in 2019 the scope was expanded to the region in cooperation with BIRN, currently covering Bosnia and Herzegovina, Croatia, Hungary, North Macedonia, Romania and Serbia. In addition to allowing us to warn and mobilize the public, the monitoring also empowers us to actively participate in advocating for new and critically analyzing existing legal proposals that concern regulating the lives of individuals, which are now taking place in both physical and digital spaces.

You can access the database of digital rights violations in these 6 countries at this link.

At this link you can find a study on regulations in three areas covered by this guide, covering six countries in the region: Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia.

USAID
FROM THE AMERICAN PEOPLE

B | T | D The Balkan Trust for Democracy
A PROJECT OF THE GERMAN MARSHALL FUND