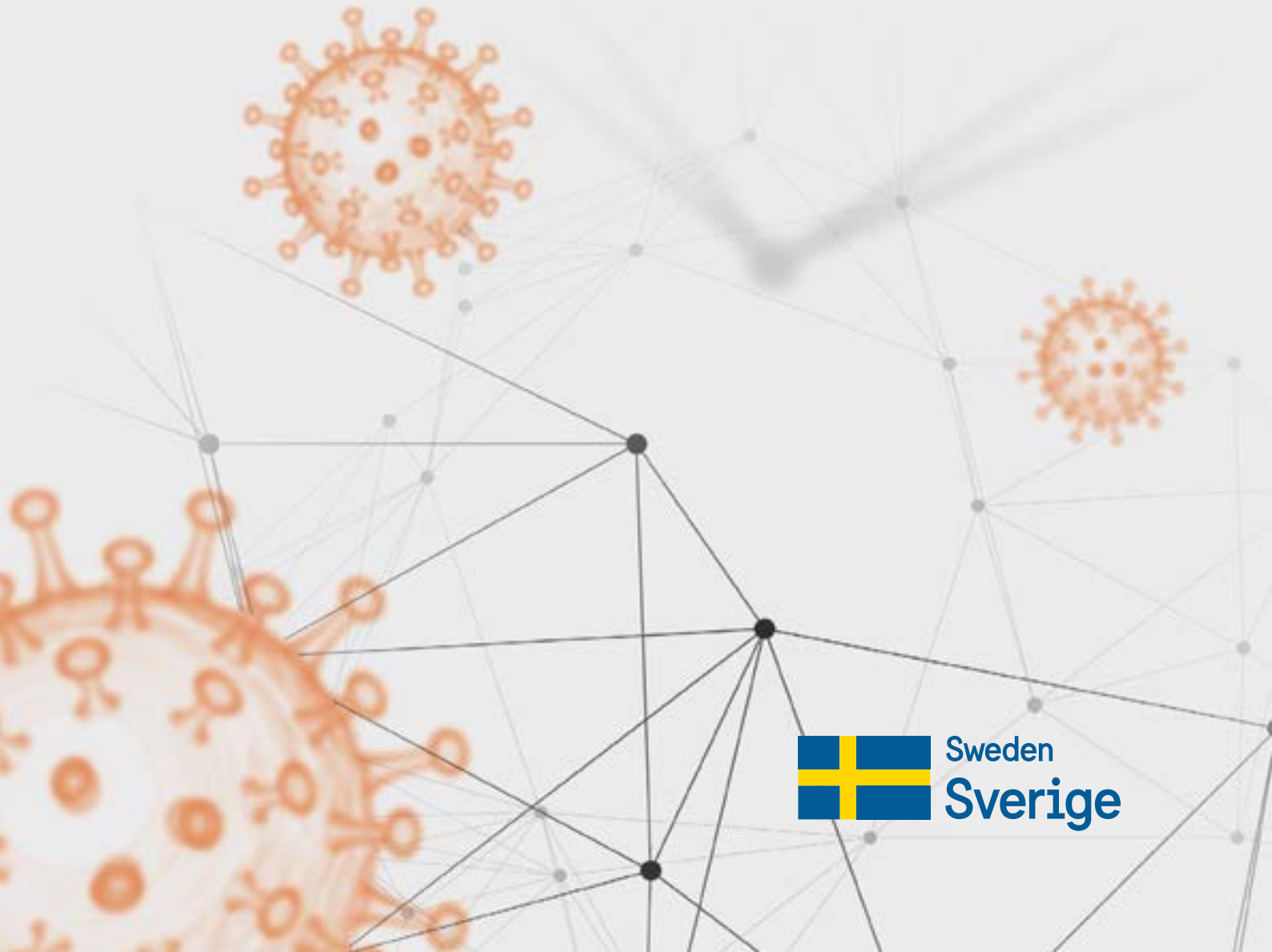
CIVIL RIGHTS DEFENDERS

HUMAN RIGHTS IN A PANDEMIC



Sweden
Sverige

IMPRESSUM

Published by
Civil Rights Defenders

For Publisher
Goran Miletic

Authors
SHARE Foundation

Bojan Perkov
Kristina Cendic
Filip Milosevic
Andrej Petrovski
Milica Jovanovic

Editor
Neda Mirkovic

Design
Marko Kovachevski

HUMAN RIGHTS IN A PANDEMIC

HUMAN RIGHTS IN A PANDEMIC

Amplifying existing pressures on human rights and their defenders throughout the world, the COVID-19 pandemic has brought major challenges to communities that already suffer inequalities and injustices in the states of their residence, many of which have resorted to extraordinary measures to contain the outbreak. “Inform, empower and listen to communities”, warned WHO’s Director-General back in August, addressing the states’ response and the “damage COVID-19 has caused socially, economically and politically”.[1]

As Civil Rights Defenders’ Executive Director Anders L. Pettersson put it in May: “Some measures may be necessary, but others are clearly not – and all must be removed once this is all over. Furthermore, using the pandemic to harass human rights defenders or abuse the rule of law for political gains, which we have been already witnessing, is simply unacceptable.” He also emphasized the role of human rights organisations in the process of monitoring and demanding accountability from authorities whenever the line is crossed between what is actually necessary in a democratic society and the misuse of power.[2]

The region of the Western Balkans has shared similar experiences. As authorities in many Balkan countries framed their response to the pandemic in militaristic terms, issues of public health gave way to the discourse of state security where dissenting opinions and questions are viewed as signs of sedition.

While in some countries the traditional media space for dissent was already very limited, the imposed full or partial lockdowns and curfews moved most of the social and political activities to the online sphere. Pressure on human rights defenders followed suit.

Official measures implemented in order to combat the pandemic often involved increased surveillance and use of motion tracking technology. Such circumstances have gravely affected the privacy of the work done by human rights defenders in every field possible. Journalists, lawyers and activists concerned with human rights have also faced difficulties in relocating their community activities, such as workshops, protests and conferences, to the online sphere while maintaining communication security.

In addition to sampling digital rights violations and describing visible trends in restraining the work of human rights defenders in several Southeast European countries, this publication offers a chance to rethink online services and tools used in daily operations. There are ethical and safe digital tools available that can replace the big data-hoarding complexes of Facebook, Google, Amazon and other global IT giants and can help us avoid government censorship, surveillance by intelligen` ce agencies and technical attacks from cybercriminals and malicious hackers.

1 WHO Director-General’s opening remarks at the media briefing on COVID-19 - 3 August 2020, World Health Organization, 3 August 2020
2 COVID-19 is no excuse for governments to abuse human rights, Anders L. Pettersson, The Globe Post, 1 May 2020.

A REGIONAL OVERVIEW

SHARE Foundation has been monitoring digital rights violations in Serbia since 2014, expanding the scope of work as of last year in partnership with the Balkan Investigative Reporting Network (BIRN) to keep track of such incidents also in Bosnia and Herzegovina, Croatia, Hungary, North Macedonia and Romania.[3] The first joint effort inadvertently coincided with the global pandemic, uncovering worrisome events and trends in the region.

The process of monitoring is based on tracking various types of breaches in line with the defined methodology,[4] and sorting the cases into specific categories. In the methodology, there are seven different categories of digital rights and freedoms breaches:

A. Information security breaches: cases of information systems breaches, e.g. unauthorised access, DDoS (Distributed Denial-of-Service) attacks to disable access to certain content, theft and data destruction, etc.

B. Information privacy and personal data breaches: cases of data leaking, illegal data processing or interception of communications.

C. Pressures related to expression and activities on the internet: these breaches refer to honour and reputation, endangering security, discrimination and hatred, freedom of expression in the workplace, and pressures on individuals on the basis of their publication of information on the internet.

D. Manipulation and propaganda in the digital environment: these breaches include different forms of content dissemination and online manipulation with the objective of achieving certain goals – which often turn out to be economic goals.

E. Holding intermediaries liable: these breaches refer to pressures on internet providers, such as hosting providers, content removal requests and service refusals, by means of legal threats, punishments, or blocking.

F. Blocking and filtering of content: in these cases, certain content is technically blocked at national or organisational level, or blocking or suspension of legitimate content by platform algorithms (e.g. video parody).

G. Other: other breaches of digital rights and freedoms not included in the categories defined so far.

In addition to the above-mentioned categories, the monitoring process also provides information on attackers and affected parties. They may include journalists, public figures, state officials, citizens, activists and others. If possibly identifiable, descriptions of cases also contain the means of attack used. This could be technical (malware attacks, code injection, reconnaissance attacks, interception attacks, access attacks, flooding/denial of service attacks) or legal (private lawsuits, criminal complaints, arrests and detentions, important judgments, confiscations and searches, misdemeanour complaints). Outcomes of cases are also monitored, i.e. the monitoring covers any legal and other measures taken regarding a case, and whether a final court judgment has been reached or not.

This report presents findings for four countries - Albania, Bosnia and Herzegovina, Kosovo and Serbia - and is based on the data retrieved in the period from 31 January to 30 November 2020.[5]

3 SHARE Foundation and BIRN digital rights monitoring database: https://monitoring.bird.tools/
4 More details about the SHARE Foundation and BIRN digital rights monitoring methodology can be found at: https://monitoring.bird.tools/methodology
5 Please note: data for Kosovo was provided by Balkan Investigative Reporting Network (BIRN), while data for Albania was based on information provided by CRD Albania staff and "The Right to Information during Natural Disasters in Albania 2020" publication, authored by Dorian Matlija with the support of Res Publica center staff.

CATEGORY OF VIOLATION	Serbia	Bosnia and Herzegovina	Albania	Kosovo
A. Information security breaches	4	1	1	0
B. Information privacy and personal data breaches	8	5	2	4
C. Pressures related to expression and activities on the internet	30	9	2	3
D. Manipulation and propaganda in the digital environment	15	6	2	4
E. Holding intermediaries liable	0	1	0	0
F. Blocking and filtering of content	0	0	1	0
G. Other	0	0	0	0
TOTAL	**57**	**22**	**8**	**11**

Over the observed period, 98 pandemic-related violations of digital rights were recorded in Serbia, Bosnia and Herzegovina, Albania and Kosovo, ranging from arrests of journalists and citizens over information they shared online and seizures of devices to leaks of personal data. Apart from targeted incidents, there has been a rising number of cases involving improper handling of sensitive health-related data of citizens and intentional unlawful releases of such data to the public.

The most prevalent type of violations in the observed period - about a half of all recorded instances - were those concerning pressures related to expression and activities on the internet, such as insults, threats, publishing falsehoods with the intention to defame, etc.

According to a policy brief on the Western Balkans,[6] in some countries the pandemic exposed long-term problems and served "as an accelerator to pre-existing trends, such as the crisis of democracy and nationalism". In others, it was soon accompanied by election campaigns causing "disbelief and anger directed at the authorities and the state, revealing a deeply rooted distrust towards the latter". Freedom of expression suffered in all observed countries.

During the lockdown, political pressures on media sectors in these countries resulted in serious consequences such as centralisation of information, spread of fake news and persecution of those of contrasting views, including both professional journalists and citizen journalists. At the same time, media outlets close to the governments did not refrain from spreading fake news themselves. In some cases, authorities had such a strong grip on information that they attempted to introduce legislation which would make anything but the official information illegal. In this manner, they exercised their power and hindered democratic procedures in these countries even more, curbing human rights under the pretext of fighting the pandemic.

6 Policy Brief: The Western Balkans in Times of the Global Pandemic, Balkans in Europe Policy Advisory Group (BiEPAG), April 2020

STATE RESPONSES TO COVID-19

In March 2020, administrations in some of the countries observed in this report resorted to declaring a state of emergency. In Serbia, it was introduced on March 15 and lasted until May 6; in Bosnia and Herzegovina it lasted from March 17 till May 29 in the Federation and from March 28 until May 21 in Republika Srpska; and in Albania from March 25 until June 23. In Kosovo, a state of emergency for public health, supervised by the Ministry of Health, came into force on March 16. The citizens of the four countries faced similar prohibitions and challenges during the pandemic, and although all restrictions provoked a louder public outcry, the human rights activism had to rely on the internet more than ever. The state of emergency in **Albania** lasted longer than in any other country covered in this report. Authorities insisted on the necessity to protect public health, but the respect of citizens' rights became questionable, especially when it came to freedom of expression on the internet. During the crisis, the government tightened its grip on information, especially information on the spread of the virus, which raised numerous concerns. Public discourse was revolving around warlike phrases, stoking fears among citizens with a number of armoured vehicles in the streets.[7] Much like in other countries, Albanian citizens were also confused by the measures introduced. There was a Technical Committee of Experts established to decide on anti-pandemic measures but "the Committee's work was marked by limited public information on its competences and the extent to which its recommendations were converted into political decisions. Until early May, the name of the Committee's chairperson was not even disclosed". On one occasion, Albania's counter-terrorism police force asked for criminal charges to be raised against about ten people stating that they had used Facebook to spread fake news.[8]

The police was apparently monitoring Facebook posts and comments and found out about the statements in question in this manner. The monopolisation of information turned out to be one of the biggest problems that Albania faced during the crisis. The Prime Minister was very active on social networks, too, in addition to his dominant presence on state television. In fact, it was reported that "only in the first month of the lockdown, the Prime Minister published 407 Facebook posts (13 per day) and 47 hours of videos, thus creating Albania's first experience of governance via social media."[9] It was rather problematic to see that "most decisions were first published on the Prime Minister's Facebook account and only later in the Official Gazette, while the 'press conferences' were actually closed for journalists." The access to accurate public information was, therefore, hindered and "national media had limited opportunities to provide additional information to the public and contrast the information offered by the government."[10]

Bosnia and Herzegovina had no consistent official strategy for fighting the pandemic due to its administrative divisions. Each of the separate entities, the Federation of Bosnia and Herzegovina, the Republika Srpska, Brcko District and the ten cantons in the Federation of Bosnia and Herzegovina introduced various measures to contain the pandemic. Such a situation was particularly confusing for the citizens of Sarajevo, with the entity border line cutting through the city and restrictions and measures varying from one street to another.[11] During the crisis, the public in Bosnia and Herzegovina including human rights defenders faced issues such as disinformation on a medicine being produced locally, the lack of tests, virus-spraying airplanes flying over cities, etc. The protection of personal data was also under threat: authorities disclosed the names of people disobeying self-isolation orders and they even considered making the names of infected people public. The authorities of Konjic and Canton 10 published the list of people put in self-isolation and then withdrew it after the Data Protection Agency declared it a breach.[12] The protection of human rights in Bosnia and Herzegovina was mostly hindered when the entity of Republika Srpska adopted a decree banning the spread of panic and disorder through alleged fake news.[13] Since it was criticised as harmful to freedom of expression by local human rights defenders and international actors, the decree was soon abandoned, but only after several citizens were already arrested or fined.

In addition to the pandemic, **Kosovo** also faced a political crisis as the government received a no-confidence vote, which only contributed to the overall insecurity and distrust of citizens. Just like in other countries, authorities insisted on people wearing masks and keeping a physical distance; they also introduced restrictions of movement. In relation to the latter, BIRN Kosovo and a local software development company, KUTIA, created a platform "90 Minutëshi yt" ("Your 90 Minutes") which enabled citizens to check at what times they were allowed to leave their homes, by entering their second-to-last number of their personal ID number or passport number.[14] However, during the crisis citizens were much more concerned with the chilling effect caused by the arrests of those who spoke about matters of public interest. An editor from Mitrovica was arrested, which constituted great pressure on freedom of expression.[15] The chilling effect in Kosovo was further intensified when the Kosovo police investigated a case of a person who allegedly shared a text message inviting citizens to get tested for coronavirus at the Kosovo University Clinical Center (UCCK), claiming that persons of certain blood types were more prone to catching the disease.[16] In addition to this, the Sinjali news portal published the names, addresses and dates of birth of 210 citizens put in quarantine in North Mitrovica and other cities, which was assessed as a violation of privacy.[17] After a strong reaction from the Association of Serbian Journalists in Kosovo and the OSCE Mission to Kosovo, the personal data was blurred.

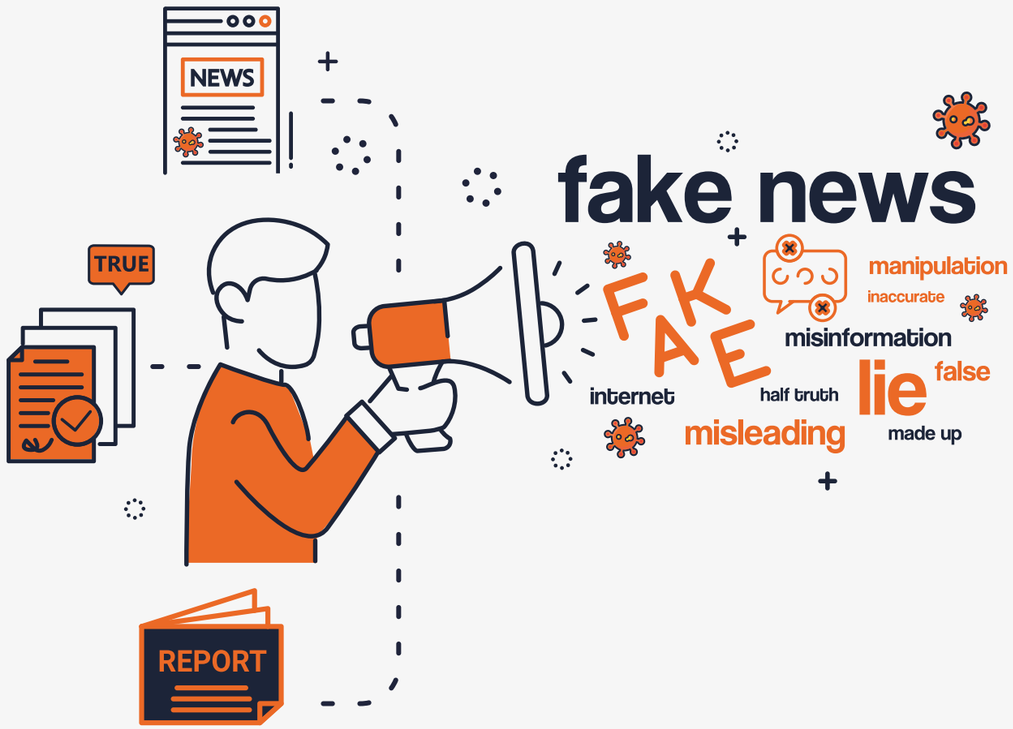
In **Serbia**, the Covid-19 outbreak and the introduction of the state of emergency resulted in problematic measures taken by the authorities to combat the pandemic. This can be seen in the attempts to control the flow of information, favouring pro-government media, hostility towards independent media outlets and human rights defenders and violations of personal data protection. Due to the situation caused by the pandemic, various actors shifted their activities online more than ever, which made them even more exposed to digital threats and attacks. One of the most serious incidents referred to a data leak incident of COVID-19 information system log-in credentials appearing online.[18] These credentials used to access the system processing sensitive pandemic-related data of citizens were publicly available on the website of a healthcare institution for eight days. Despite the username and password being removed after the civil society alerted the authorities, eight days were enough for Google to index the information and make it available in its search results. Additionally, the Serbian government tried to centralise the pandemic-related information by introducing a decree according to which only information coming from the authorities is reliable, turning all the others into the sources of alleged fake news. Journalists, civil society activists and even citizens who spoke about issues such as medical equipment shortage, gas shortage, etc. were accused of spreading panic and some of them even arrested.

7 G. Madhi, Albania: public information becomes a casualty of COVID-19, OBC Transeuropa, 11 June 2020
8 G. Emiri, Albania's War on 'Fear Mongers' Leaves Rights Activists Uneasy, BIRN, 29 July, 2020
9 G. Madhi, Albania: public information becomes a casualty of COVID-19, OBC Transeuropa, 11 June 2020
10 Ibid.
11 G.Sandić-Hadžihasanović, Entities and pandemic: On one side of the street one rule, on the other another, Radio Free Europe/Radio Liberty, 14 May 2020
12 Bosnia and Herzegovina and Montenegro to Respect Right to Privacy of Citizens in Self-Isolation, CRD, 25 March 2020
13 M. Milojević, Preventing the spread of panic or 'disciplining' doctors and journalists, Radio Free Europe/Radio Liberty, 12 April 2020
14 S. Todorović, BIRN Platform to Help Kosovars Follow COVID-19 Restrictions, BIRD, 16 April 2020
15 OSCE Media Freedom Representative concerned about pressure on KoSSev online portal and its editor-in-chief in Kosovo, Organization for Security and Co-operation in Europe, 12 April 2020
16 Calling for coronavirus testing by false messages, Kosovo online, 31 March 2020
17 COVID-19: political interference in the media in Kosovo, European Federation of Journalist, 4 April 2020
18 A Password Pandemic. How did a COVID-19 password end up online?, SHARE Foundation, 24 April 2020

Impact of Anti-COVID Measures

FREEDOM OF EXPRESSION

The pandemic had a substantial impact on freedom of expression around the world. When public health is in danger and when countries introduce a state of emergency there can be certain restrictions imposed on citizens, however these measures must not be excessive. According to Article 19, it seems that many governments used the pandemic to further entrench repressive measures and to restrict freedom of expression and information.[19] Western Balkans countries introduced restrictions which threatened freedom of expression and affected the work of activists and journalists to a great extent.



Digital technologies changed the way in which we exercise our right to free expression and enabled numerous actors to take up roles of journalists, as well. Therefore, we increasingly rely on media actors and citizen journalists, all of whom participate in debates on matters of public interest. More than ever, the pandemic brought these debates into the online environment, but along with this shift, pressures on those either exercising their freedom of expression or reporting on issues of public interest on the internet intensified. Professional journalists and other traditional media actors are not the only targets. According to the UN Plan of Action on the Safety of Journalists and the Issue of Impunity and General Comment no.34 of the Human Rights Committee, "the definition of media actors has expanded as a result of new forms of media in the digital age. It therefore includes others who contribute to public debate and who perform journalistic activities or fulfil public watchdog functions."[20] However, in the Western Balkans, we have witnessed threats and insults directed at those who spoke against the information given by the officials or expressed their views on the pandemic, whereas in some cases we saw arrests and fines imposed.

19 Coronavirus: Impacts on freedom of expression, Article 19
20 Recommendation CM/Rec(2016) of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors, Council of Europe, 13 April 2016

One of the first steps that some countries took after they proclaimed state of emergency was the attempt to control the flow of information. The public has the right not only to exercise their freedom of expression, but also to receive information. However, on March 28 the Serbian government made a decision forbidding anyone outside its Crisis Headquarters to provide any pandemic-related information, proclaiming that any information from other sources would be considered incorrect and unverified. More specifically, those who would share such information could be held accountable and suffer legal consequences for spreading disinformation in a state of emergency.[21] We have witnessed similar occurrences in Bosnia and Herzegovina, when its entity of Republika Srpska adopted a decree which prohibited spreading panic and disorder; it referred also to social networks and media outlets.[22] Such a decree had a restricting effect on the right to free expression - therefore local human rights defenders, as well as international actors, urged authorities to revoke it as soon as possible. The decree was soon revoked, but by that time, some of the citizens were already either arrested or fined. Fines stipulated for violation of this decree amounted to 500–1,500 EUR for natural persons and 1,500-4,500 EUR for legal entities.

One of the most serious cases causing a chilling effect was that of Ana Lalic, a journalist who was arrested for her article about the state of the hospital in Novi Sad, Serbia. Ana was arrested on April 1, only hours after her text entitled "The Clinical Centre of Vojvodina at its breaking point: no protection for nurses" was published. In the article, she spoke about matters of public interest, namely the lack of protective equipment, such as masks and gloves, at the Clinical Center of Vojvodina. The hospital filed a criminal complaint against her claiming that the article damaged their reputation and upset the public with unverified information. After the arrest, Ana's laptop and phones were seized and she was taken into custody. This arrest provoked a very strong response from both local and international actors demanding her release as soon as possible. Ana Lalic was released the next day after being interrogated and the charges against her were dropped at the end of April. This incident did not only cause a possible chilling effect among citizens and those who spoke about certain matters of public interest, it also triggered a smear campaign against Ana Lalic led mainly by the pro-government media. Also, Civil Rights Defenders called upon the government of Serbia to provide journalists with an adequate space within which they could get information and inform citizens about ongoing Covid -19 developments. "We believe there is no justification for the suspension of the right of journalists to ask questions in an open and public forum, considering the possibilities that modern technology offers for such interaction without a necessary physical presence", they stated.[23]

Overall, journalists and activists were often targets of insults on the internet during the pandemic. The insults came from other media, public officials, sometimes from anonymous actors, as a result of which the exercise of the right to freedom of expression in Serbia stooped to a low level. In addition, out of the four countries covered by this paper, Serbia already has already had the lowest ranking according to Reporters without borders (93rd) and it has been assessed as unsafe for journalists.[24] In another incident, Albanian journalist Sonila Meço suffered online abuse after she had posted a comment on Facebook criticising comments made by a doctor referring to a group of Albanian nationals which were stuck at the border with neighbouring Greece and were not allowed entry to the country.[25] In mid-March, Albanian citizens received an unexpected voice message through the Vodafone mobile operator, in which Prime Minister Edi Rama advised them to wash their hands as a way of fighting the coronavirus and to "protect themselves from the media".[26]

But it was not only in Serbia and Albania that activists, journalists and citizens were punished upon expressing themselves in the online sphere. In Bosnia and Herzegovina, there were cases of citizens being fined in line with the disputed decree, mainly because of their posts on social networks.[27] For example, a doctor was fined for saying that hospitals did not have enough equipment, a person from Gradiska allegedly "caused panic and disorderly conduct during an emergency situation," and offended public bodies of the entity of RS, etc.

21 T. Curcic, J. Tomic, D. Djordjevic, Government Attempts to Restrict Reporting on Coronavirus, Center for Investigative Journalism of Serbia, 1 April 2020
22 M. Milojevic, Preventing the spread of panic or 'disciplining' doctors and journalists, Radio Free Europe/Radio Liberty, 12 April 2020
23 Serbia's Authorities Must Respect Media Freedoms and Citizens' Rights to be Informed, Civil Rights Defenders, 11 April 2020
24 Reporters without borders, Serbia
25 Albania: journalist Sonila Meço receives torrent of abuse after Facebook post, Mapping Media Freedom, 7 April 2020
26 G. Erebara, Rama Takes his War on Media to Albanians' Phones, Balkan Insight, 13 March 2020
27 Digital Rights in the Time of COVID-19, BIRD

SURVEILLANCE

As Freedom House noted in their recent report, the worrying trends related to measures taken during the Covid-19 crisis include sweeping collection of very sensitive personal data and the rollout of intrusive technologies for monitoring citizens such as predictive policing, facial recognition or thermal scanning.[28] To make things worse, these measures were often implemented without adequate protection mechanisms aimed at the prevention of human rights abuses.

Due to the Covid-19 pandemic, Western Balkans states also resorted to increased surveillance measures, as the prevailing atmosphere was implying that the spread of the disease can only be prevented and kept under control through strict oversight over citizens' behaviour. Restrictions of movement and lockdowns, sometimes spanning to several days, were also intended to keep under control large gatherings and crowds.

For example, Albanian citizens were required to obtain a permit on the E-Albania portal to be allowed to go out of their homes in order to buy groceries or walk their pets.[29] Only one family member could obtain the permit on a daily basis and it was valid for two hours. The police also used drones in the Albanian capital Tirana to keep track of how lockdown measures are respected.[30]

28 A. Shahbaz, A. Funk, False Panacea: Abusive Surveillance in the Name of Public Health, Freedom House, 2020
29 M. Brändle, T. Brankovic, A. Dyrmishi, Democracy and the State of Emergency, Friedrich Ebert Stiftung, 18 May 2020
30 Albanian Police Use Drones to Enforce Lockdown, Voice of America, 16 April 2020

In Serbia, a national state of emergency was declared in mid-March and lasted until early May. The President of Serbia warned citizens at a press conference held soon after state of emergency was announced that "Italian phone numbers are being tracked", referring to mobile phone location tracking of the many Serbian citizens returning to the country from abroad and being sent to mandatory self-isolation.[31] He also noted that there is "an alternative method" of motion tracking of those who leave their phones behind in an attempt "to trick the government", but did not explain what that method was.

Increased surveillance measures, mostly concerning the movement of citizens, hinder the work of journalists, activists and human rights defenders, particularly in public spaces, which are becoming increasingly turned into areas of dystopian control.[32] Who is to say that when the pandemic is eventually over, advanced technological tools for surveillance introduced to contain the coronavirus will not be used for other purposes - among other things, to stifle dissent and criticism of the government?[33]

A massive video surveillance system installed in Belgrade, the capital of Serbia, consisting of thousands of cameras with facial recognition capabilities, is a serious warning for social activism and public interest work as the coverage of the streets of an entire city with smart video surveillance changes the very fabric of society.[34]

Restricting rights and liberties disproportionately and indiscriminately, the system of smart video surveillance has been installed in Belgrade against national and international legal standards and regulations. Its purpose has not been clearly defined, nor has there been set a clear and strict legal framework for the use of the smart surveillance system by the police in public places prior to its implementation. The "Smart City", a joint project of Serbian public authorities and Chinese company Huawei, is being developed in a non-transparent way, withholding information on the conditions of the partnership and the price of the entire system. There has been no public debate on possible social and political impact of these extremely intrusive technologies.[35] Intrusive video surveillance was also reported in Republika Srpska, one of the entities of Bosnia and Herzegovina. According to media reports, the Ministry of Interior of Republika Srpska has acquired more than 300 cameras, out of which 66 have facial recognition capabilities.[36]

31 Government responses to COVID-19 adversely affect digital rights in the Balkans, International Freedom of Expression Exchange, 4 April 2020
32 Ban biometric mass surveillance!, European Digital Rights, 13 May 2020
33 The day after the pandemic: are we moving towards a dystopia of surveillance, SHARE Foundation, 2 April 2020
34 Thousands of Cameras website: https://hiljade.kamera.rs/en/home/
35 It is against the law and harmful for society to introduce the system of smart surveillance in Belgrade, Thousands of Cameras
36 The Ministry of Interior set up facial recognition cameras: Where all we are being surveilled?, Istok, 28 July 2020

REMOTE WORK

As societies switched to the online sphere more than before, digital rights defenders came across several obstacles in their work. On several occasions, journalists faced serious problems in performing their role of a watchdog, because this role cannot be entirely performed online - it requires field reporting, as well. Therefore, associations of journalists insisted on journalists being exempted from the curfew. In Serbia, the Association of Independent Journalists of Vojvodina requested that the authorities clarify the conditions under which journalists can move during the lockdown at the very beginning of the state of emergency.[37] Ultimately, professional journalists were allowed to report from the field if they applied for such permits. However, this change did not cover citizen journalists, bloggers and others without a journalistic accreditation, therefore working remotely turned out to be rather limiting for them.

In Albania, from the beginning of the year there were several protests which were broken up, such as the commemorative rally on Europe Day, held by civil society on 9 May, as well as the protest against the demolition of the National Theater, a massive anti-government protest that was violently disrupted, as 37 people were arrested including a journalist. However, probably the most worrisome was the protest in mid-December against the police killing of a young man, which resulted in street violence, and as a result, more than 300 citizens were criminally prosecuted and three journalists were violently arrested.[38] These cases of violence clearly suppressed the right to free association in Albania and caused a chilling effect during the crisis.

Furthermore, an editor from Kosovo was arrested for violating the curfew although she was in fact doing her job.[39] Tatjana Lazarevic, the editor-in-chief of the Kossev news portal, was on duty when she was arrested, and although she was released soon, such an incident could have had a serious chilling effect not only on other journalists, but on everyone whose work included observing the situation on the ground. In the end, the Ministry of Internal Affairs of Kosovo clarified that the curfew did not apply to journalists and media workers, but it remained unclear as to whether human rights activists were also exempted from the curfew.

In Bosnia and Herzegovina, the Institution of the Human Rights Ombudsman of Bosnia and Herzegovina had to react when the work of human rights defenders was obstructed during the crisis.[40] Namely, in the Federation of Bosnia and Herzegovina, press conferences of the Crisis Headquarters were either held with a limited number of journalists or fully excluding the physical presence of journalists, or they would only address questions previously sent by email. Therefore, the Institution of the Human Rights Ombudsman of Bosnia and Herzegovina issued an official recommendation calling on the authorities to ensure to the best extent possible that journalists are present at press conferences.

A similar situation occurred in Serbia.[41] At one point, most of the media were allowed only to email questions in advance of the daily press briefings held by members of the Crisis Headquarters. Journalists were not openly banned from attending press conferences, although only the public broadcaster RTS and state-run Tanjug News Agency had cameras there and questions coming from particular journalists were omitted altogether. This impeded journalists from fulfilling their role as watchdogs and their remote work seemed to have been imposed not only by the pandemic itself, but by the authorities too.[42]

37 NDNV: Enable journalists to work during curfew as well, Danas, 18 March 2020
38 Albanian authorities must prevent further police violence and uphold the right to freedom of peaceful assembly, Council of Europe, 15 December 2020
39 Digital Rights in the Time of COVID-19, BIRD
40 M. Brändle, T. Brankovic, A. Dyrmishi, Democracy and the State of Emergency, Friedrich Ebert Stiftung, 18 May 2020
41 No journalists at daily pandemic briefings, Serbian government says, N1, 10 April 2020
42 Press freedom must not be undermined by measures to counter disinformation about COVID-19, Council of Europe, 3 April 2020

CAPACITY ISSUES

Like other sectors, the pandemic caught human rights defenders, activists and other public interest watchdogs in a situation they have not encountered before; this is particularly true for those working in smaller communities. Taking into account their capacities, both short and long term, the “new normal” seems like an enduring challenge for the civic sector in terms of sustainability. Organisation building and inspiring people to do social activism also becomes harder in times of crisis, particularly due to economic pressures.

Financial, technical and organisational capacities of the civil society are very dependent on grants and projects. The crowdfunding culture is yet to be developed in the Western Balkans, and there are probably no civil society organisations in the region which can rely on micro-donations and membership fees as a larger portion of their income. However, due to the adverse effects of the pandemic on the global economy, donations from foreign state entities, such as embassies and development agencies, might be expected to be reduced. In these circumstances, it will be difficult to ensure growth of the civic and activist sector with limited funds and resources.

For example, CIVICUS, an international network of civil society organisations, published an open letter to donors and supporters in March 2020, asking for as much flexibility, certainty, and stability towards grantees and partners as possible during the Covid-19 crisis.[43] The letter listed several ways in which that could be done:

- Listen to grantee partners and together explore how you can best help them face the crisis, trusting they know best what is needed in their own contexts;
- Encourage the re-design and re-scheduling of planned activities and deliverables and provide clear guidance on how to seek approval for these changes;
- Support new and creative ways of creating a culture of solidarity and interaction while adhering to the physical distancing and other precautionary measures;
- Offer greater flexibility by reconsidering payment installments based on actual needs, converting existing project grants into unrestricted funds, or adding extra funds to help build-up reserves or cover unexpected costs;
- Simplify reporting and application procedures and timeframes so that civil society groups can better focus their time, energy and resources on providing support to the most vulnerable rather than on meeting heavy reporting and due diligence requirements.

One of the main concerns for human rights organisations, and the civic sector in general, is technical infrastructure, such as websites, servers, emails, work devices, etc. Namely, SHARE Foundation’s experience in providing *pro bono* technical support and training has shown that many organisations have scarce IT- related resources, meaning that they often lack in-house IT staff and rely on external associates to manage their infrastructure. In circumstances such as the pandemic, which cause radical shifts in society and in the way organisations operate, a large-scale cyber attack could have devastating consequences for human rights defenders due to the lack of adequate technical and staff capacities to mitigate the attack, and subsequently, repair the damage suffered. This could mean loss of valuable data gathered through years of work, or for example, loss of access to social media accounts or organisational emails. Working from home can also pose a risk to digital security, as security measures employees take on their home/private devices may not be up to the standards of the organisation.

43 Open letter: Donors and supporters must act to ensure civil society resilience against COVID-19 pandemic, CIVICUS, 19 March 2020

Digital Tips

Faced with a global pandemic, activists and organisations around the world are forced to move most of their communication and collaboration into the digital space. Although the last 20 years have been marked by a rather rapid digitalisation of many processes in everyday life, it seems as if everything was a preparation for the steep transition that took place in just a few weeks with the beginning of mandatory quarantines all over the world.

Such a sudden change brought in some seemingly logical, but rash decisions on the choice of technologies, services and software that should compensate for the new limitations and physical distance. It is sensible to accept solutions that are popular and easy to use, but the question is how well they meet the criteria necessary for the safe work of activists and civil society organisations. In addition, the choices we make now will greatly influence the technologies which will be accepted by organisations and society as a whole in the long run. So, the second question is more ethical: do we want to adopt proprietary (commercial) profit-driven services or open source community-driven solutions and how will our choice affect the diversification and decentralisation of the digital ecosystem.

The choice and understanding of the technologies that activists use in their work have a key impact on their integrity and security, the resilience of their organisations, and the sustainability of the society we are building.

Due to the nature of their work, human rights activists are more often exposed to information security breaches, increased surveillance and interception of communications, attempts at censorship through technical attacks, unauthorised access and compromising of personal data, threats, pressures and other methods aimed at stifling freedom of speech and obstructing their work. Resilience to all those threats in the digital space depends on the technologies we use.

Unfortunately, most of the tools we rely on today were created by companies whose business models are based on extracting and monetising the personal data and habits of their users. So far we know very well that we are a part of the “surveillance economy”, but we continue to use these tools because everyone else is using them and it is very easy to rely on them.

However, from a technical point of view, the main disadvantage of most commercial and popular services and applications is that they have a closed code. Closed (proprietary) code can be compared to a black box in which we do not know what is happening and where our data goes, making the use of these tools a matter of trust that, when it comes to corporations, we have little or none. This compromise

that we are willing to accept in order to use technology with no effort can be very dangerous. In addition to trading user data for commercial purposes, it has been proven that security services can intercept communications too easily and have direct insight into our metadata. Using modern tools for cyber espionage, governments around the world carry out targeted attacks on political dissidents and often hire malicious hackers who, with sophisticated technical methods and social engineering, manage to penetrate well-protected systems without being noticed. Finally, the well-known discomfort we feel when some of the popular services we rely on only briefly become unavailable calls into question what will happen when they stop working for a long time, because it is not a question of whether this will happen, but only when will it happen.

On the other hand, the implementation and use of fully responsible and secure open source solutions often require much more effort and more resources. For certain services, it is necessary to hire system engineers to install them, to own or lease servers, maintain the entire system, perform additional training, and many organisations do not have such capacities. However, this kind of investment enables a greater control over data flows, their security, and the long-term sustainability of information systems. Today is a time when technology within an organisation should be thought of as much as management, finances or human resources.

When these matters are taken into account, considering the available resources, individuals and organisations can decide at what level they will advance their approach to technology and the choice of the tools to work with. It can be mitigation - decreasing of risks, achieved by small steps towards the improvement of the technological environment: by replacing certain tools for which there are already proven alternatives, which require minimal effort to make the transition. This approach does not solve problems, but reduces them, facilitates understanding of technology and builds confidence for future bigger choices and decisions. More ambitiously, it can be a complete change of approach and paradigm in relation to technology. It requires more serious investments of resources, time and energy, but in the long run it brings much greater independence in data control, as well as a major systemic and techno-political shift.

Below is an overview and description of some of the more comprehensive tools and solutions that the community can currently offer, which could ensure secure communication and teamwork, not only during the crisis, but also in the times to come.

SECURE COMMUNICATION

Instant communication (alternatives for WhatsApp, Facebook Messenger, Viber etc.)

Signal - A communication app that runs on most platforms and operating systems and a pioneering project in encrypted instant communication. It enables text messaging, including group communication, voice messaging, as well as sharing photos and videos. It recently added support for voice and video calls. It also serves as a replacement for SMS/MMS applications, but requires all parties to use it in order to replace the protocol with its own. It is an open source project, run by a non-profit organisation and is entirely funded from donations, which allows it to work without monetising user data. In the course of its development, it has been most commonly used by activists around the world for secure communication in repressive regimes or situations of increased police oversight, such as protests in democratic societies.

Wire - One of the more popular counterparts developed in parallel to Signal, Wire had certain advantages that other services did not have at the time, such as encrypted group chat, or an option to register for the service and use it without providing a phone number. It offers specific opportunities that are oriented towards additional privacy, which compared to the competition, has proven to be very important for the advancement of technology and diversity of the entire ecosystem. Since Wire is also based on an open source and does not sell user data, its method of financing relies on offering advanced services for business users.

Telegram - Although not completely an open source platform (the application is open code, what happens on the company's servers is not), so far there have been no known incidents of compromising activists' data on Telegram. It is definitely among the most popular services for secure communication, at least when it comes to information exchange between large groups of people through groups and channels. Precisely because of this ease of communication on a larger scale, intuitive interface and great popularity with the general public, Telegram is frequently an option for human rights activists. Even though the platform has built a relationship of trust with its users, caution is advised because the system is not fully open source, the business model is not completely clear and it does not guarantee long-term sustainability.

Web / video conferencing (Alternatives for Zoom, Skype, Google Meet, Microsoft Teams, etc.)

Jitsi Meet

Many organisations and activists have adopted Jitsi Meet as the primary platform for video calls in recent years due to several key features. The platform was among the first to introduce encryption for a open source service of this type. At the same time, the installation of a special application is not required and the platform can be approached directly from all popular internet browsers just by clicking on a designated link. For organizations with greater resources, the platform can be downloaded and installed on their own Linux servers, which offers an additional level of security.

BigBlueButton

The competitive advantage of Zoom in the world of proprietary and commercial video conferencing tools is well matched by BigBlueButton in the world of open and responsible technologies. The platform has many features that meet the needs of major public online events, such as user administration, multimedia content sharing, presentations, collaborative whiteboard/flip chart tools, private and public chats, breakout rooms, etc. The only requirement is the installation of your own instance on Linux servers, or the use of an instance of other organisations that can make it available for use, which is increasingly the case in the civil sector.

SECURE GROUPWARE

Team communication (alternatives for Slack, Microsoft Teams, Discord etc.)

Mattermost

Organisations with plenty of internal communication and materials are often suffocated and lost in email correspondence. Platforms like Mattermost are definitely tools capable of lessening the burden on inboxes and improving communication by themed chat channels, intuitive search, indexing and secure document and file sharing. After the initial setup on the organisation's own or rented server, it does not require much maintenance and administration, so it is convenient for organisations with smaller technological capacities. All data is encrypted and the project is funded by providing support and additional services to business users.

Element

Until recently known as "Riot.im", Element is a chat client that uses the modern Matrix protocol - a federated communication protocol that has been developed as an open standard and aims to enable interoperability between different chat and video conferencing services. This practically means that messages can be exchanged with users of most popular platforms, including proprietary services such as Apple iMessage, Facebook Messenger, WhatsApp, Discord, Slack, and certainly of open source applications such as Signal, Mattermost, IRC, Telegram...

Other tools

Depending on the needs of an organisation, it is worth mentioning a few more good tools that can be used as alternatives to the services of large data-hoarding companies.

Etherpad is an online/web text editor for real-time collaboration (an alternative to Google Docs) that can be installed on your own server, but there are free instances on the internet like **"Riseup Pad"** that offer the service free of charge while not collecting IP addresses and respecting user privacy. The application can also be accessed via a VPN or **Tor Browser**, the use of which is imperative for masking internet activity.

The same technology that Tor uses for onion routing is also used by **OnionShare,** a secure file sharing service. In short, and perhaps quite banal, it works by generating an encrypted file address on a computer that the user on the other side can only access by means of the Tor protocol.

Finally, when it comes to secure data storage and alternative "cloud" services (replacements for Dropbox or Google Drive), **Nextcloud** is in the forefront. It requires installation and maintenance on its own servers, which definitely requires additional resources in the organisation, but also offers the highest level of data control.

Ultimately, these tools and their adoption in everyday work do not provide a total immunity against security risks, but they do give us a greater independence and encourage further understanding of technology. The resilience of individuals and their organisations further depends on understanding the ecosystem of the digital space and the relationship of technology with society. That is why it is important that, in addition to accepting responsible tools, we also understand data flows, surveillance architectures and business models of techno-corporations that are increasingly centralising the internet with modern digital colonialism. Understanding and accepting responsible technologies encourages the development of alternatives, while increased literacy of communities and the society as a whole encourages freedom, openness and decentralisation of the internet, which has become a precondition for a resilient democracy.

Conclusion

As it currently stands, government efforts to introduce restrictive legislation and intrusive technologies, under the pretext of fighting the pandemic, should be under higher scrutiny from human rights defenders, who also need to be more vigilant. Future measures may contain provisions which can adversely affect freedom of expression, the right to privacy and other related rights and freedoms, such as the right to protest or freedom of assembly, but they may be presented in such a "package" that their effect might not be visible at first sight. Therefore, the civic sector, in particular, needs to be on the lookout and question any measures which might be seemingly introduced to curb the spread of the coronavirus, but can in fact be an introduction into permanent surveillance or other disproportionate restrictions of human rights.

The current circumstances, while being very challenging for human rights defenders, activists and the civic sector in general, can also be an opportunity to try out alternative and more secure technical tools, such as free and open source software. Although the transition to working from home and implementation of new tools in the organisations' technical infrastructure may present some difficulties, it can ensure long term flexibility and resilience to times of crisis, especially for smaller teams and organisations with modest investment possibilities. For example, the Galileo Project provides human rights defenders and other public interest actors with resources needed to mitigate technical attacks, prevent vulnerability exploitation and protect data integrity.[44]

However, when it comes to working remotely, organisations need to ensure that their employees apply the same digital security standards at home as in the workplace. In addition, a more open approach to the adoption of free and open source software renders the community more inclined to keeping the internet open, free and decentralised.

for more information on protecting your work online

cloudflare.com/galileo

44 More information about Project Galileo is available at: https://www.cloudflare.com/en-gb/galileo/

CIVIL RIGHTS DEFENDERS

HUMAN RIGHTS IN A PANDEMIC

Sweden
Sverige