DIGITAL RIGHTS DEVELOPMENTS IN BELARUS:

DIGITAL AUTHORITARIANISM AND DIGITAL RESISTANCE

Human
constanta

Contents

Introduction 1
Tools of digital authoritarianism 3
Tools of digital resistance 10
Conclusion and recommendations 13

Introduction

When human rights are violated offline, digital rights are rarely spared. Authoritative governments are increasingly interested in developing oppressive techniques in the digital domain by increasing censorship, overregulating cyberspace, weaponizing tech to spread propaganda and surveillance.

Belarus is no exception. Notorious for being "Europe's last dictatorship" — with its vast history of dissidents' *enforced disappearances*, *torture*, *political persecution*, and appalling *human rights record*, — the role of Belarus as a digital and not merely "analog" dictator is less conspicious. While it is true that the control over Belarusian citizens online may not have reached the scale and professionalism of "textbook" digital dictatorships, like China with its *"Great Firewall"* or Russia with its *"troll factories,"* the tendency towards tightening the grip on Internet freedoms is alarming.

The events *pre, mid, and post presidential election 2020*, widely recognized as *fraudulent*, marked the start of the largest political and human rights crisis in Belarusian modern history. More than a thousand people are officially recognized as *political prisoners* in Belarus. More than *35000* have been subjected to arbitrary detention in degrading conditions. At least *5500* criminal cases have been initiated in connection with "mass riots" since the beginning of the electoral campaign. As of 1 July 2022, *11000* criminal cases were launched on extremism-related grounds. There have been at least *5000* allegations of torture and inhuman treatment, without a single criminal case initiated to investigate the reports. At the same time, the International Committee for the Investigation of Torture in Belarus *documented* about 1,500 cases and *recognized* sufficient evidence of torture in each of the 50 cases randomly selected for examination.

By July 2022, *537* non-profit organizations were liquidated or reported to undergo the procedure of liquidation. Already by 2021, *all independent human rights organisations in Belarus have been liquidated* by the decision of Belarusian authorities. Journalists, human rights defenders, and activists continued to be detained or forced out of the country for fear of persecution. Amendments to the Criminal Code of the Republic of Belarus have effectively *outlawed human rights work*, criminalizing "working on behalf of unregistered or liquidated organisations" and making it punishable by imprisonment.

Belarusian authorities continue to use law as a tool of oppression. *The Code on Administrative Offences* and *the Criminal Code* have been amended to toughen the punishment for protest-related activities, including by introducing *death penalty for "attempted terrorism"* — a term vaguely interpreted by the Belarusian authorities. *The Labor Code* was amended to limit the right to strike. *The Law on Countering Extremism* — to extend the punishment for extremism to any acts of expressing dissent. *The Law on Mass Public Events* — to make the conditions for holding public events stricter. *The Law on Mass Media* and *the Law on Legal Practice* — to subject the practice of journalism and jurisprudence to complete state control. *The Law on Preventing the Rehabilitation of Nazism* has been passed to label protest symbols as Nazi symbols and *the Law on the Denial of Genocide of Belarusian People* — to monopolize historic narratives and label any undesirable speech as false.

In addition to *mass political repressions*, continuing and strengthening since 2020, Belarusian de facto authorities, *not recognized as legitimate* by most international actors, continued *assisting Russian invasion of Ukraine* by allowing Belarusian territory to be used for the attacks. The situation is dire and continues to deteriorate, leading to further silencing of independent Belarusian voices and shrinking of the civic space.

Tools of digital authoritarianism

Civic cyberspace is also shrinking in Belarus. While Belarus is a highly Internet-connected country, scoring 69.5/100 on the GSMA Mobile Connectivity Index 2021, the Internet freedoms leave much to be desired. In fact, Belarus scored 31/100 on the *Freedom of the Net Index 2021* — a score, exemplary of the deteriorating digital rights landscape due to ever strengthening repressions.

Belarusian de facto authorities have been enthusiastic in exploring tech solutions, which can be put to use to control and oppress the population. The willingness to “protect digital sovereignty” by increasing control over Internet platforms is often expressed by state officials and state-controlled propagandists. Pro-government political analyst Vadim Baravik in its interview to a state-owned media outlet Belta *said*:

"During the [2020 presidential] election campaign we understood that we are losing the Internet battle. Now they are blocking our media. We have learned how to work on the Internet, we have competitive channels, yet we do not control the Internet platforms. Do you realize what the problem with that is? Our TV channels can be turned off at any moment. We might have good “missiles,” smart experts, but we must have channels to deliver them. We do not have means of transporting such information war “missiles”and that is why we must effectively protect our information space, like China does.”

Some of the key repressive tactics of Belarusian government in the digital realm include:

- Internet shutdowns;
- Censorship and persecution for online speech;
- State-sponsored online propaganda;
- Surveillance.

Freedom House *defines* digital authoritarianism in the following way:

“Digital authoritarianism is being promoted as a way for governments to control their citizens through technology, inverting the concept of the internet as an engine of human liberation.”

Belarusian practices fall no short of digital authoritarianism, as a way of governing the country through cyber means of oppression, and manipulation.

2.1. Internet shutdowns

Internet shutdowns, *understood as* intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable to exert control over information flows, were especially widely *used by the Belarusian authorities* at the peak of the 2020 peaceful protests.

The total *121 days* of the protest-related shutdowns has affected the work of the most popular online platforms within the country — YouTube, WhatsApp, Telegram, Viber, among others. The shutdown involved a complete outage on 9-12 August 2020, as well as *slowing down* Internet connection (throttling) on days of peaceful gatherings. Shutdowns in Belarus are an example of shutdowns being used as "pre-emptive tools against peaceful assemblies, especially in the context of elections" — a threat, identified by the United Nations Special Rapporteur on Rights to Freedom of Peaceful Assembly and of Association Clement Voule in his *report* "Ending Internet shutdowns: a path forward," as well as in the *2022 report* by the Office of the United Nations High Commissioner for Human Rights. Such a tool aims to make it harder for protestors to coordinate their actions online and for the population generally — to get access to up-to-date information, including that on brutal suppression measures by the regime's security forces.

Despite multiple *claims* by the authorities blaming the shutdown on external cyber-attacks, human rights organizations and IT experts, based on the technical expertise and analysis of the preceding sequence of events, *share the view* of disruptions being orchestrated by the state.

Moreover, while at first *none of the mobile operators acknowledged* the state's deliberate actions aimed at Internet blackout, all of them further explained the deterioration of service's quality by the order of the authorized bodies. Mobile operator MTS *specified* that the state cited national security when ordering the shutdowns.

To implement the shutdown, Belarusian authorities employed deep packet inspection (DPI) equipment, bought from a U.S.-based private company *Sandvine* — as part of a $2.5 million *contract* with the Russian technology supplier Jet Infosystems. When acquiring the new technology in 2018, the Belarusian authorities stated that they needed it to combat cybercrime. According to *Sandvine's commitment to avoid misuse of its products*, the company intends to ensure that its products are not used to interfere with the free flow of information or thwart human rights. However, according to independent researchers from *Citizen Lab*, Sandvine's DPI equipment was used to block websites and shut down the Internet in Turkey, Syria, and Egypt. Following a public outcry, Sandvine *demanded* that the National Traffic Exchange Center (NTEC) in Belarus return the DPI equipment and "refrain from choking the internet to prevent the free flow of information to Belarusians," yet *concerns* on whether the company's practices aided digital dictatorship practices in Belarus and across the world remain relevant.

The limitations on the right to free expression and access to information by means of Internet shutdowns in Belarus are manifestly inconsistent with international obligations of Belarus. The International Covenant on Civil and Political Rights provides for 3 conditions which are simultaneously required to allow for a lawful restriction of the right to information and freedom of expression: legality, necessity, and proportionality.[1] Several international actors maintained that cutting off Internet access unjustifiably restricts the right to freedom of expression.[2]

[1] *International Covenant on Civil and Political Rights*, para. 3, Article 19, *General Comment No. 34, Human Rights Committee*, 12 September 2011, para. 22.

[2] "Cutting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds. The same applies to slow-downs imposed on the Internet or parts of the Internet." *Declaration on Freedom of Expression and the Internet, 1 June 2011*, para. 6 (b).

"Filtering of content on the Internet, using communications 'kill switches' (i.e. shutting down entire parts of communications systems) and the physical takeover of broadcasting stations are measures

2.2. Censorship and persecution for online speech

The toolbox of silencing online speech in Belarus heavily relies on the body of "anti-extremism" laws — including the Law on Countering Extremism, the Law on Countering Terrorism, the Law on Preventing the Rehabilitation of Nazism, as well as the corresponding extremism-related articles of the Criminal and Administrative Codes.

Even before *amending* the Law on Countering Extremism in June 2021, Belarusian "anti-extremism" legislation was notorious for a vague definition of "extremist activities," extending from "engaging in terrorist activities" to "making public calls to organize or conduct illegal meetings, rallies, processions, demonstrations, and picketing." Such wording allows for unfettered discretion in recognizing materials, organizations, and informal groups as extremist and casts doubt over the true intention behind state's actions.

The newly amended Law broadens the notion of "extremism" even further, listing, inter alia, such actions as:

insulting or discrediting public authorities and administration or representatives thereof;

violating the procedure for organizing and holding mass public events;

committing illegal acts against public order and public morals, order of governance, life and health, personal liberty, honor and dignity of the individual, and property, aimed at inciting enmity or discord;

promotion of extremist activities, training or preparation for participation in extremist activities;

dissemination of deliberately false information about the political, economic, social, military or international status of the Republic of Belarus, the legal status of citizens in the Republic of Belarus, discrediting the Republic of Belarus.

Importantly, the Law's new edition introduces the term "extremist formation" as a "group of citizens, engaged in extremist activities, or otherwise aiding extremist activities, or acknowledging the possibility of engaging in extremist activities, or financing extremist activities." The new term differs from "extremist organization" since declaring a group an "extremist organization" requires a court decision, while the decision on recognizing a group as "extremist formation" can be single-handedly taken by the Ministry of Internal Affairs or the State Security

which can never be justified under human rights law." *Joint Declaration on Freedom of Expression and Responses to Conflict Situations*, 4 May 2015, para. 4 (c).

"Condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and calls on all States to refrain from and cease such measures." *Report of the Human Rights Council, A/HRC/32/L.20*, 27 June 2016, para. 10.

"Calls upon all States to refrain from and cease measures, when in violation of international human rights law, that are aimed at shutting down the Internet and telecommunications, or at otherwise blocking Internet users from gaining access to or disseminating information online, or from gathering in online spaces." *Report of the Human Rights Council, A/HRC/44/L.11*, 13 July 2020, para. 13.

Committee (KGB). Such a simplified procedure of declaring informal groups "extremist formations" stifles self-organization and solidarization of people, making it easier than ever to criminalize activism.

Due to the vague legal wording, "creation of and participation in extremist formation" is one of the main legal grounds for imposing criminal liability on founders, admins, and followers of unfavourable online resources. Another commonly employed ground, triggering administrative, rather than criminal, liability is "dissemination of extremist materials," which allows punishing people for reposting "extremist" content, reacting, commenting, or even sharing materials in private chats.

On 11 August 2022, the Investigative Committee of the Republic of Belarus stated that from 9 August 2020 until 1 July 2022, more than *11 000 criminal cases*, investigating crimes "of extremist nature" were initiated. Several cases of "anti-extremist" persecution in the digital realm are particularly notable:

- *Anastasiya Krupenich-Kondratyeva and Sergey Krupenich* were charged with dissemination of extremist materials for sharing posts from "extremist" Telegram channels in private messages to each other and repetitively punished with 15 days of administrative arrest for the same action 8 times in a row — an overall term behind bars amounting to 112 days for each of them.

- *Dzimitriy Padrez*, IT-specialist from Minsk, was found guilty of violating 3 articles of the Criminal Code and sentenced to 7 years of imprisonment for communicating personal data of police officials, involved in suppression of protests, to the "Black Book of Belarus" Telegram channel, *recognized as "extremist."*

- *Sofya Sapega*, detained by Belarusian authorities in an infamous *Ryanair incident* in May 2021, was sentenced to 6 years in prison for allegedly administering Telegram channel "Black Book of Belarus."

- Penalties for extremism-related offences have sometimes been applied retroactively to punish retaining online materials reposted from media outlets even before them being labelled extremist. On 22 June 2022, *Nikolai B., a resident of Ivanovo*, was charged with "dissemination of extremist materials" for making a repost from RadioFreeEurope / RadioLiberty Facebook account on 27 March 2017.

- On 9 December 2021, *Artyom Boyarsky*, ex-student of the Belarusian State University, was sentenced to 5 years of imprisonment for administering "My country Belarus" ("Maya Krayina Belarus" in Belarusian) Telegram channel.

- Anti-war speech continues to trigger criminal persecution in Belarus. On 28 July 2022, 17-year old author of "Pressobol" newspaper *Raman Kachyna* was detained for leaving a comment on social media, stating that "Belarusians have always been at war with Russians." Following his detention, a confession tape, featuring him admitting the guilt was published on pro-government Telegram channels. On another occasion, student *Danuta Peradnia* was sentenced to 6.5 years in prison for reposting a text, which harshly criticized the actions of Vladimir Putin and Alexander Lukashenka in unleashing war in Ukraine, in one of the local chats. It also called for street protests and stated that the Belarusian army has no prospects in case it enters the war directly.

Apart from oppressive application of "anti-extremism" laws, state censorship practices include blocking media resources, deemed as undesirable. Access to dozens of resources *was limited*, even without them being previously recognized as "extremist," based on the decision of the Ministry of Information of the Republic of Belarus, authorized to adopt relevant decisions by the *Law on Mass Media* and the *Regulation on the Procedure for Restricting (Resuming) Access to Internet Resources*.

The list of restricted online resources is managed by the State Telecommunications Inspection of the Republic of Belarus of the Ministry of Communications and Informatization. It *is not publicly available* and disclosed only to designated state authorities. *According to TUT.BY*, already on 22 August 2020, more than 70 websites, including those of belsat.eu, virtuabrest.by, babariko.vision, euroradio.fm, spring96.by, svaboda.org, honestby.org, hramada.org, by.tribuna.com, belarus2020.org, protonmai1.com, psiphon.ca, were blocked. Generally, the blockages affected websites of independent media, civil initiatives and human rights organizations, as well as websites of VPN and e-mail encryption services.

Overall, the described legal amendments and practices of broadening the definitions and the scope for liability, thus tightening already restricted space for expressing dissenting views, were introduced in violation of international human rights law[3] and have the potential to undermine the rights to freedom of assembly, freedom of association, and freedom of expression.[4]

2.3. State-sponsored online propaganda

Simultaneously with a self-declared civil society *"purge"* online and offline, the Belarusian authorities are clearly trying to fill the information space with pro-government narratives by spreading propaganda and disinformation. While conventional state TV propaganda *lacks effectiveness* in Belarusian context, state authorities explore online avenues of getting the propaganda messages across to the public.

The practice of publishing *confession tapes* online is particularly worrisome. Since the 2020 elections, the authorities have heavily relied on forcing dissidents to confess their guilt on camera or coercing them into saying things that benefit the regime. One of the first examples of Belarusian online propaganda coming into the spotlight was *the recording* of a Belarusian opposition politician Sviatlana Tsikhanouskaya, discouraging the public from joining mass protests and putting their lives at risk, which she later admitted she was forced to record and publish under pressure from state authorities.

Belarusian authorities have paid for *Youtube ads*, featuring confession videos of Sofya Sapega and Roman Protasevich, detained following a *forced landing of Ryanair Athens-Vilnius flight* in Minsk airport in May 2021. *Evidence*, directing the ads to Belarusian authorities includes a number of screenshots posted online that link the ads to a pro-government Telegram channel titled "Belarus — the country for life."

[3] *Report of the Special Rapporteur on the Situation of Human Rights in Belarus, Anaïs Marin, A/HRC/50/58, Fiftieth Regular Session of the Human Rights Council, 13 June - 8 July 2022.*, para. 23.

[4] *Report of the Special Rapporteur on the situation of human rights in Belarus, Anaïs Marin, A/HRC/50/58, Fiftieth Regular Session of the Human Rights Council, 13 June - 8 July 2022.*, para. 28.

Confession tapes sometimes contained forced outing of LGBTQ+ community representatives. Such videos, published on pro-government Telegram channels are yet another tool used by the state to marginalize the objectors. Two of the victims of forced outing include *Nikolai Bredelev* — a spokesman from a mobile telecommunications provider A1, and *Artyom Boyarsky* — an administrator of an opposition Telegram channel.

2.4. Surveillance

The Belarusian authorities rely on surveillance to identify and keep an eye on local activists. Whether through routine monitoring of public social media accounts, hacking into private devices, video monitoring, or excessive data collection, — surveillance is essential for a digital autocracy.

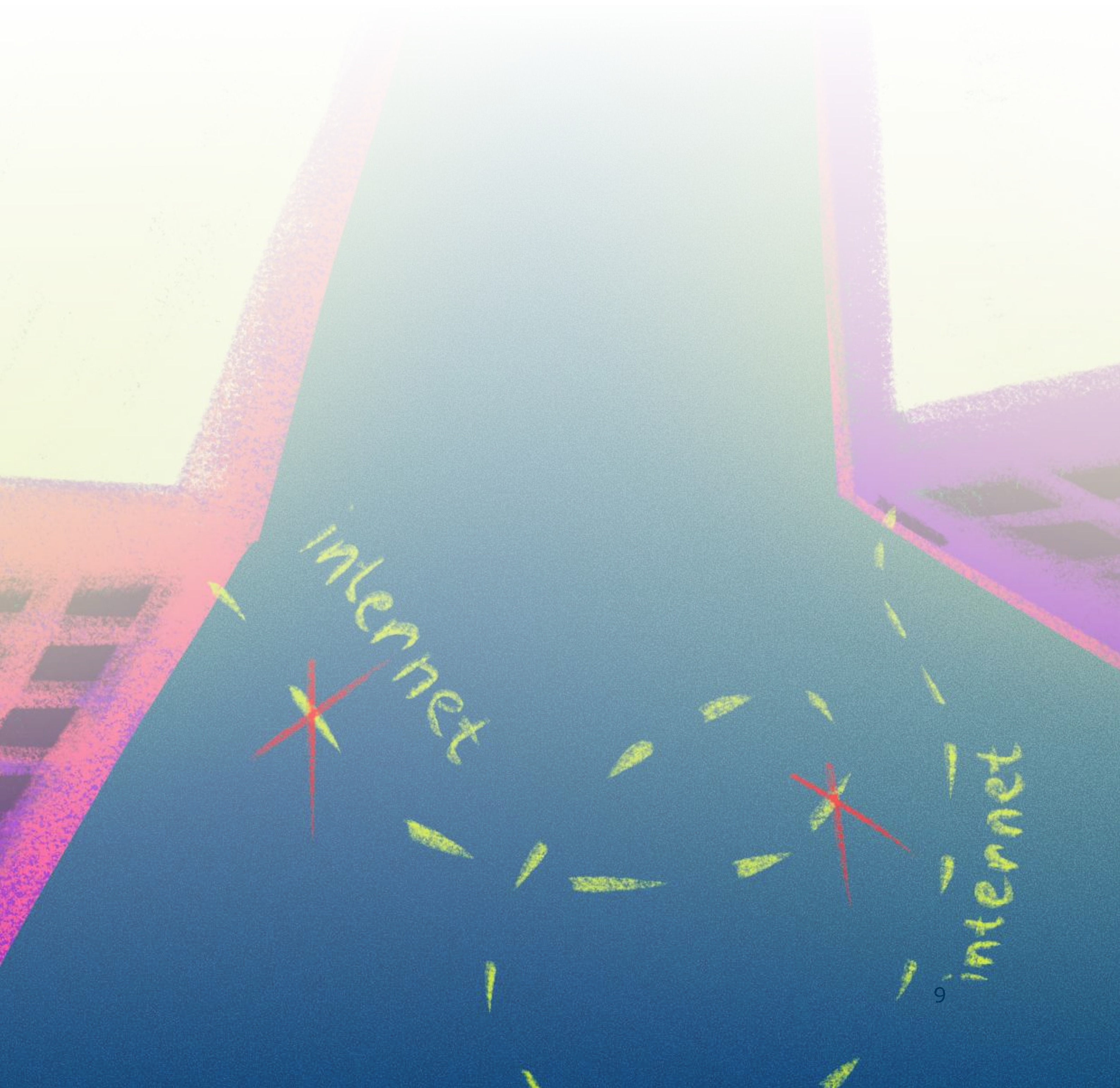
Although the exact methods of surveillance of citizens by Belarusian authorities and the algorithms underpinning them are not public, some comments from state officials confirm the use of surveillance and shed some light onto the tools used. For instance, vice chair of the Belarusian Investigative Committee Anatoliy Vasiliev *stated* that "it is hard to imagine a criminal case, in which the investigators would not look into the information on the phone connections of the suspect." He also mentioned a special automated information system "Footprint," used since summer 2021 as a tool monitoring the digital footprint of suspects.

A recent example of the tool adapted by the Belarrusian authorities to track dissidents is the *"Kipod"* facial recognition software *developed by "24x7 Panoptes" company*. The latter is a subsidiary of Synesis — a notorious Belarusian software developer, included in the European Union sanctions list *for providing authorities with the video surveillance platform and aiding therewith the state in repressing the civil society and democratic opposition.* Synesis also became the target of restrictive measures introduced by *the United Kingdom* and *the United States*. The algorithm became integrated into the *Republican Public Safety Monitoring System* after winning the tender for the selection of the technical operator for this national system. One of the *events*, reportedly proving the platform's application for political persecution, is the arrest of Nikolai Dedok — a prominent political activist and blogger. The security forces set up surveillance on Dedok's acquaintance and managed to track down his regular routes by seizing video recordings from the Minsk metro surveillance cameras, embedded into Kipod platform.

Belarus' de facto authorities were also *known* to hack opposition Telegram channels, primarily through the use of coercive tactics. This includes forcing access to resources when arresting their administrators, followed by changing accounts' names, profile images and identifying subscribers. Such measures affected "Data of Punishers in Belarus," "Drivers 97%."

Other algorithms for detecting activists include the publication of phishing links in chats linked to Telegram channels, and parsing the database of mobile phone numbers of Belarusian holders. By resorting to such tools, security forces were able to identify administrators of "White Coats," "My Country Belarus," "Belarus 24," "Basta," "Belarus of the Brain" Telegram channels.

One more concerning example of the state's alleged intrusion into media activities relates to hacking the Telegram channel of independent media outlet "Nasha Niva," as well as accounts of 3 of its journalists. Some of the evidence, suggesting that the attack was orchestrated by state apparatus, lies in preceding attempts of the Investigative Committee to acquire the personal data of both the full-time journalists and freelancers of the media outlet, who were soon targeted by hacking attempts.



Tools of digital resistance

The power dynamic between authoritarian states and civil society in the extent of control either exercises over technology is sometimes characterized as a *"game of cat-and-mouse."* While Belarusian authorities exhibit a clear interest in using cyberspace as another battleground for state repression, Belarusian activists are using it to advance human rights. Digital authoritarianism tendencies in Belarus are met with digital resistance, producing a phenomenon of *"digital dissidents."* The ways to protect digital rights from state's arbitrary interference vary and include, inter alia:

- Civic tech tools;
- Cybersecurity and self-help measures;
- Hacktivism/digital vigilantism.

3.1. Rise of civic tech

The peaceful protests of 2020 took horizontal connections and solidarity action to a new level. Civil society has developed multiple tech-based solutions to resist state oppression and reclaim human rights. *Civic tech projects* — that is, initiatives using digital technologies to advance social good, — made it possible for citizens to cooperate safely and effectively in order to realize human rights, which are denied to them by the state.

Online initiatives allowed Belarusians to *verify and count votes in the presidential election*, document crimes committed by *election commissions* and *law enforcement authorities*, *provide assistance to political prisoners*, *share ways of monitoring and circumventing shutdowns*, and *discuss new forms of protest*.

Since Belarusian authorities proved ineffective in performing their functions of implementing human rights, civic tech initiatives often assume such functions. In authoritarian regimes, where trust in public institutions is broken and offline civil society platforms are few and persecuted, the role of tech-based initiatives is particularly relevant.

Some of the most notable examples of civic tech initiatives, launched by Belarusian activists during 2020 peaceful protests and in its aftermath, include:

- *ZUBR* platform, which collected and published information on the composition of vote-counting commissions at each of the polling stations, allowing voters and observers to share information about the violations they witnessed. In the post-election period, the functions of a platform changed from election monitoring to exercising civil control of judicial systems, collecting and systematizing information about judges and punishments imposed on peaceful protestors.
- *Golos* ("Vote" or "Voice" in Russian) platform, which, in the context of prohibition of conducting exit polls in Belarus, collected and verified information on the actually collected votes, comparing it to the official data. In the post-election period, Golos transformed into a platform for conducting public opinion

polls, including a *poll* on the need to conduct negotiations launched by the Office of Sviatlana Tsikhanouskaya with the de facto authorities controlling the Belarusian state.

- *Skarga.help* platform, which, in the context of incessant *persecution and disbarment of independent lawyers*, helped citizens to file complaints to state bodies through an automated template system.
- *Politzek.me* and *Letters behind Bars* initiatives, which help communicate with political prisoners online by creating platforms to write and send letters to prisons and jails.
- *Avocado.help* platform, which connects lawyers and people in need of legal assistance, and helps victims cover any associated expenses.
- *Legal.Hub* platform, which provides a secure online platform for pro bono legal advice, which does not retain users' data and allows those seeking advice and providing it to do so anonymously.
- *Digital Solidarity* platform, which systematizes, structures, and distributes resources and directs requests for financial assistance of people suffering persecution to verified and transparent initiatives.
- Cyber Beaver platform, which exists in the form of a *Telegram channel* and a *Telegram chatbot*, provides online consultations on cyber security measures, designed to help civil society and grassroots activists to maintain cyber hygiene and minimize threats and vulnerabilities.
- *ICanHelpHost* platform, which connects people fleeing war in Ukraine and hosts, willing to provide free accommodation within Europe and beyond.

In Belarus, civic tech solutions have proved to be a powerful tool, which helped civil society stay resilient in the face of oppression. Over time, the challenge for many platforms is to remain sustainable, creating ecosystems and digital infrastructures, which active citizens can rely on in Belarus and in exile. Such sustainable ecosystems are a crucial element of digital resistance since they help to preserve solidarity and horizontal ties, thus withstanding the ever mounting state pressure.

3.2. Cyber security and cyber hygiene

Another lesson learned for many Belarusians living through a period of mass repressions has to do with the importance of protecting oneself online. *Mass searches and confiscation of equipment*, *the authorities' attempts to hack into activists' accounts* and *take down websites*, and *inspection of devices to find "extremist" materials* are the practices which made Belarusians particularly aware of how essential cyber security and cyber hygiene are.

The use of virtual private networks (VPNs) became a necessity rather than an extra security step for many in the midst of country-wide Internet shutdowns. Routine removals of data at border checkpoints became common practice for many to avoid persecution for being subscribed to wrong channels. The need for two-factor authentication on apps became more apparent and came with a local twist — since a Belarusian phone number cannot be a reliable second factor, because of the ease with which Belarusian law enforcement can gain access to SMS codes sent to Belarusian numbers.

While civil society's self-help measures are crucial in guarding oneself from intrusive digital policies of the Belarusian state, some challenges still remain. For instance, *the key role* Telegram continues to play for Belarusian society strengthens the reliance on the platform, which is itself notorious for lack of data encryption and poor privacy standards generally. Such Telegram-centrism is understandable — at the very least, because few messengers double down as full-on news aggregators. In the context of multiple independent media being blocked, or otherwise made unavailable, preserving online presence and access to the audience through a functionale of a Telegram channel is a viable and appealing option. Belarusians often use Telegram as not just a messenger, but an equivalent of a news feed. As practical as it might be, the platform is not free from risks which must be monitored.

3.3. Digital vigilantism and hacktivism

Digital vigilantism is often understood as a set of practices of digital self-justice. Such practices can manifest in a variety of forms — such as exposing government officials, suspected of grave human rights violations, by publishing their personal data, or hacking into government websites.

Belarus is one of the countries where de-anonymization was widely used by the activists to exert pressure on the political regime. Since the fraudulent 2020 presidential elections, peaceful protests that followed, and their violent dispersal, resulting in protestors' deaths and lengthy prison terms, people started to seek alternative avenues for justice and use digital civic resistance tools to deanonymize, name, and shame those involved in wrongdoings.

Initiatives, like *Cyber Partisans,* break into government portals and publicize sensitive data, while Telegram channels, like one entitled "The Black Book of Belarus," regularly reveal names, contacts, and pictures of law enforcement officers, suspected of committing human rights abuses. Belarusian de facto government has retaliated against such hacktivists or vigilantes. Under newly amended "anti-extremism" laws, Cyber Partisans initiative was recognized as an *"extremist"* and the administrator of "The Black Book of Belarus" *Sofya Sapega* was sentenced to 6 years in prison, following the infamous Ryanair plane hijacking in Belarus. Citizens transferring information to such channels are often subjected to *persecution for aiding extremism*, while state officials are treated as *victims* under data protection and defamation laws.

At the same time, the Belarusian government has done its "best" to anonymize and protect law enforcement officers involved in state-sponsored violence by allowing them to *hide their identities* when testifying in political cases (having their faces blurred, voices altered, and using pseudonyms).

The growing practice of de-anonymization seems to be a double-edged sword. On the one hand, it helps to balance the power of repressive states, who have the monopoly on much of the countries' Internet landscapes, and activists, who get new leverage to advance their goals. On the other, concerns about possible backsliding in the privacy realm remain relevant.

Conclusion and recommendations

The dynamic of digital rights developments in Belarus is one where the Belarusian authorities are cracking down on digital freedoms, while activists are defending and reclaiming them. It is only natural that an aspiring digital dictatorship, like Belarus, will continue to see open and free Internet as a threat and a platform of spreading "destructive" or "extremist" ideas. It is, therefore, crucial that relevant stakeholders take steps necessary to resist repressive tendencies. The following recommendations are formulated to serve this purpose:

Businesses and platforms:

- Respect obligations in the field of business and human rights, including *the United Nations Guiding Principles on Business and Human Rights* and the Organization for Economic Co-operation and Development Guidelines for Multinational Enterprises;
- Formulate and implement appropriate strategies of operating in digital authoritarianism environment, balancing the need of citizens to access essential digital tools with the need to restrict cooperation with repressive regime by providing double-purposes technologies, or allowing the platforms to be used for propaganda purposes;
- Exercise human rights due diligence in cooperation with local and regional human rights defenders, journalists, tech specialists, and digital rights initiatives;
- Support civil society by providing tools and solutions to activists on equal basis and supporting local activists in developing local civic tech tools.

States:

- Respect human rights obligations online and offline in accordance with both treaty and customary international law;
- Call upon digital autocracts to respect their human rights obligations online and offline in accordance with both treaty and customary international law;
- Mainstream digital rights and digital literacy as part of education for democratic citizenship and human rights.

Civil society representatives:

- Engage in educational, analytical, and advocacy activities aimed at raising civil society's awareness of digital authoritarianism and its consequences;
- Put pressure on digital autocrats by demanding accountability for human rights abuses online and offline;
- Support and spread awareness of digital resistance tools, which help citizens preserve their digital freedoms and mitigate risks.

Human Constanta — a human rights organization.

We work with human rights in three main areas:

- protection of the rights of foreign nationals and stateless persons;
- promoting anti-discrimination and human rights education;
- digital freedoms and rights.

Our mission

Promotion of public interest and joint action in response to contemporary human rights challenges.

What do we do?

- Helping others defend their rights.
- Comparing Belarusian laws and practices with the best international examples and human rights standards.
- Passing on this knowledge through awareness-raising and educational activities.

Author of the document: Tatsiana Ziniakova.

Email: info@humanconstanta.org
Website: https://humanconstanta.org/en/