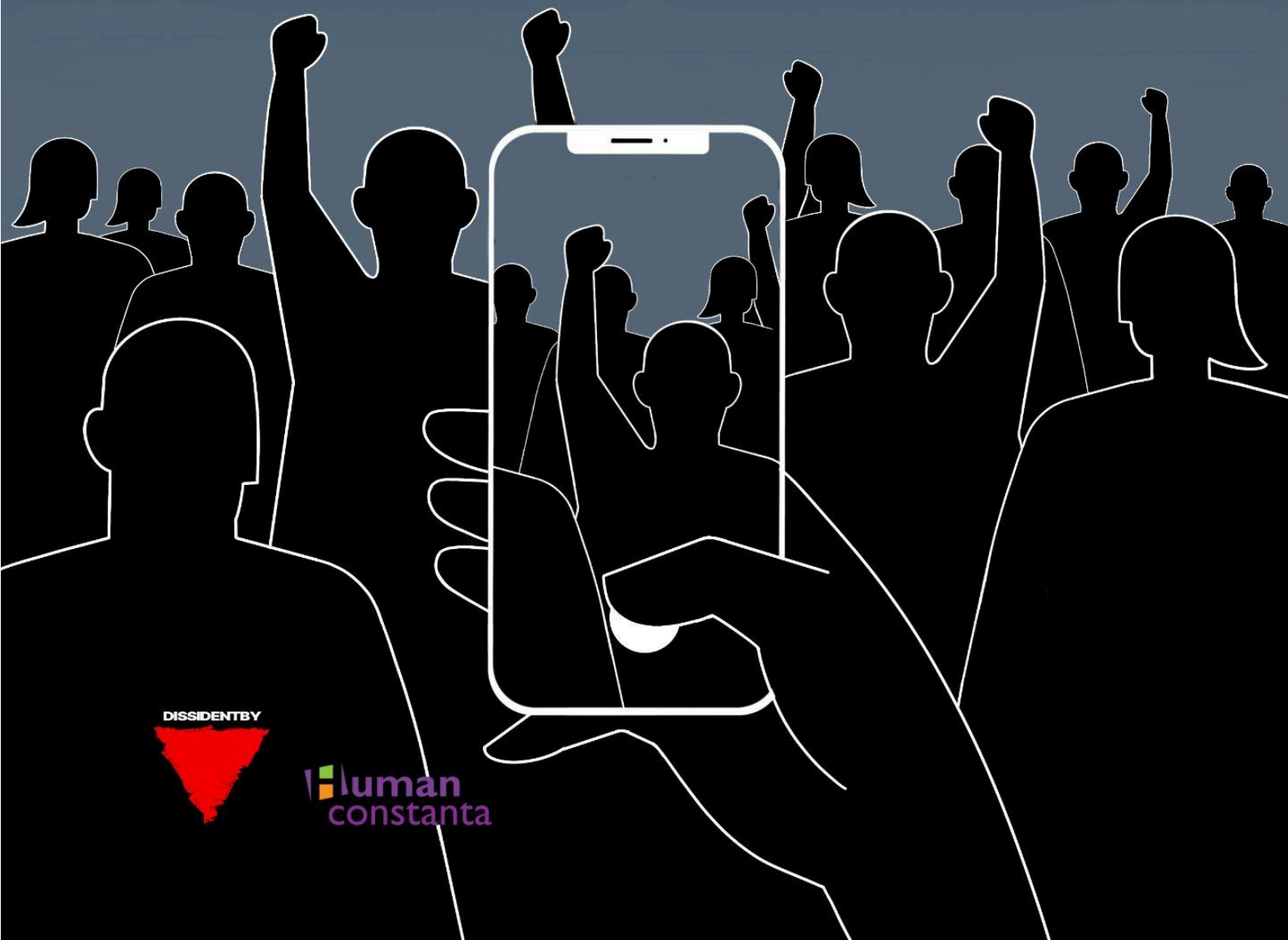
# FROM STREETS TO SCREENS: DIGITAL REPRESSION IN BELARUS



This report is co-authored by Dissidentby and Human Constanta, with cover design by Kseniya Derouga.



December, 2025

*This text is the result of the author's and editor's intellectual and analytical work. The ideas, structure, and content of the article were fully developed, written, and edited by a human. ChatGPT was used during the process to improve clarity of wording, refine individual sentences, and check the logical coherence between ideas. All AI-generated fragments were reviewed, edited, and approved by a human before being incorporated. All data drawn from specific court cases consist of unique information documented by Dissidentby.*

Email: info@humanconstanta.org
Website: https://humanconstanta.org/
Instagram: https://www.instagram.com/humanconstanta/

Email: imdissidentby@gmail.com
Website: https://dissidentby.com

# Table of Contents

# From Streets to Screens: Digital Repression in Belarus

## Introduction

Five years after the mass protests of 2020, Belarus still faces systemic political repression,  some of the most intense in Europe. However, the nature of this repression has changed. In the past, the main targets were people taking part in street demonstrations. Today, the pressure is increasingly moving into the digital space. As many activists have left the country and public protest has subsided, the authorities are adjusting their methods and shifting control to the place where resistance continues – the digital space.

According to data from Dissidentby, more than **3,476 criminal cases** related to online activity have been opened in Belarus since 2020, and **2,861 people** have been convicted. In addition, at least **8,687 administrative cases** have been documented under Article 19.11 of the Code of Administrative Offences of the Republic of Belarus, which is used to punish the "*distribution of extremist materials*" online. For comparison, in Russia there have been around **1,100 anti-war criminal cases** and more than 200 prosecutions for online statements between February 2022 and December 2024.

In a broader regional context, the suppression of digital freedoms has become a common trend. As shown by Freedom House's global *Freedom on the Net* ranking, governments are increasingly using technology to monitor, censor, and criminalize online activity – a pattern that researchers describe as "digital authoritarianism." Similar developments can be seen in Azerbaijan and Kazakhstan, as well as in Georgia, which was previously considered relatively free but has shown clear signs of rapid decline in recent years. However, Belarus stands out in this landscape due to the scale and intensity of its repression: the country outpaces most of its neighbors in the criminalization of online behavior, turning anti-extremism legislation into a key tool of political control.

The digital space, once seen as a relatively safe area for communication and solidarity, is gradually turning into a site of criminal prosecution. In recent years, Belarus has developed a consistent practice of punishing online activity: from administrative fines for "likes" and reposts to multi-year prison sentences for donations or participation in online projects. The authorities increasingly rely on broad and flexible definitions in anti-extremism laws such as "calls for actions that

threaten national security," "participation in an extremist formation," or "financing extremist activity" to expand the boundaries of punishable behavior and give legal form to political violence. As a result, the legal system now functions as a mechanism of digital intimidation, where any click, donation, or comment can be treated as a crime.

The goal of this analysis is to show how the Belarusian authorities interpret and apply the law in order to expand the boundaries of punishment for online expression and civic activity, and to compare this practice with international freedom of expression standards, which require that any restrictions be proportionate, necessary, and transparent. This approach makes it possible to assess how online freedom of expression has changed in recent years and what new risks online activity now carries in an authoritarian context.

## Evolution of Digital Repression in Belarus (2020–2025)

After the 2020 elections and the mass protests that followed, repression in Belarus initially had a clearly street-focused character. Thousands of people were detained for taking part in demonstrations, for carrying white-red-white flags, for taking photos in public squares, or even for wearing clothing of the "wrong" color. However, by late 2020 and early 2021, the center of repression began to shift into the online space.

The vast majority of people in Belarus have access to the internet, which made the online space a natural platform for communication, discussing public events, and finding like-minded people. In 2020, several key civic projects were created and actively used online: *Golos* (an alternative vote count), *Honest People* (election and detention monitoring), *Zubr* (coordination of observers and collection of evidence of violations), as well as the initiatives *Okrestina Detainees* and *August2020*, which collected and organized information about detainees and victims of violence. The internet quickly became one of the main spaces for civic self-organization and, as a result, a new target for state control.

In August 2020, the authorities deliberately restricted access to the internet, introduced filtering, and slowed down traffic, using DPI technologies to block independent media and messaging apps. These technical tools were applied not only during mass protests but also locally before targeted detentions. Human rights groups documented cases where the internet was temporarily shut down in specific districts or even for individual users, so that a person could not call for help, report a raid, or log out of their accounts before being detained.

Over the following years, digital control methods became part of standard investigative practice. For example, mobile billing data was used as “proof of presence” at protests even without photo or video evidence. At the same time, security forces began using digital tools not only for monitoring but also for provocations. One of the most illustrative cases was the so-called “tobacco kiosk arson case” (“дзела падпаленных табакерак” in Belarusian) of 2021. According to relatives of the convicted and human rights materials, the charges were based on the testimony of one chat member who, according to their information, may have acted as a provocateur. He suggested locations for actions, provided information about places without surveillance cameras, and later became the main source of evidence in court. Based on his testimony, more than ten people were sentenced to between five and nine years in prison. These cases show how the digital space is used to control and discredit civic networks of resistance.

After Russia’s full-scale invasion of Ukraine in 2022, repression in Belarus took on a new dimension. Anti-war statements were treated as “discrediting the state” or “inciting hostility.” During this period, new methods of online persecution also emerged. Security forces began actively using chat roulettes and staged conversations, in which officers or trusted intermediaries engaged people in discussions, prompting them to make anti-war comments or criticize the authorities, and then used these exchanges as grounds for criminal charges. Foreign online communities where Belarusians were active were monitored as well, for example, under videos posted by Ukrainian bloggers. There were also documented cases in which security officers used detainees’ phones to join bots, subscribe to Telegram channels, or send messages on their behalf, creating “evidence” of involvement in “extremist activity.” These practices allowed the authorities to fabricate grounds for persecution and expand the scale of criminalizing online behavior.

From 2022–2023 onward, repression became systematic and almost automated. Courts operate according to fixed templates, and the lists of “extremist formations” and “extremist materials” are updated nearly every month. According to the official registry of the Ministry of Internal Affairs, the number of entries in the Republican List of Extremist Materials increased from 128 in 2020 to 1,846 by 2025. These entries include online resources and media including Telegram channels, YouTube pages, civic initiatives, and even local group chats.

In 2023–2025, the system of persecution became even more refined. The authorities began actively applying Articles 361-1, 361-2, and 361-4 of the Criminal Code, which allow prosecution not only for actions but also for “participation” or “assistance” in the activities of an extremist formation. As a result, almost anything can be criminalized from making a donation to administering a chat or subscribing to a Telegram channel. This gradual transformation reflects the evolution of the internet

into a space where any word, photo, or reaction can become grounds for prosecution.

# Practice of Criminalizing Online Behavior in Belarus

## Prosecution for “insulting” officials and the President

*Articles 367, 368, 369, 391 of the Criminal Code*

Since 2020, the criminal articles related to “insult” and “defamation” have become some of the most frequently used tools of repression in Belarus. According to Dissidentby, at least **2,799 people** have faced criminal prosecution for comments, posts, or messages on social media.

Cases where online activity involved criticism of the President of the Republic of Belarus were punished especially harshly. In such cases, prison sentences were imposed almost automatically, while “insults” of other officials (under Articles 369 and 391) more often resulted in restricted freedom with or without placement in an open-type facility. The severity of the punishment also depended on the number of episodes and the nature of the comments, which in practice allowed investigators and courts to determine the level of punishment based on political expediency rather than legal reasoning.

The main articles of the Criminal Code used in such cases are:

- **Article 367** — “Defamation of the President of the Republic of Belarus, including one who has ceased to exercise their powers”;
- **Article 368** — “Insulting the President of the Republic of Belarus, including one who has ceased to exercise their powers”;
- **Article 369** — “Insulting a government official”;
- **Article 391** — “Insulting a judge or a people’s assessor.”

As stated in the wording of one of the court judgments:

> *“The comments posted by X, containing insults against the acting President of the Republic of Belarus, are **public in nature, as they were made available for general viewing on the Internet**. The insults contained in this post contradict established norms of communication between people and the requirements of universal moral standards, diminish the honor and*

*dignity of the head of state, undermine his authority, personal and professional qualities in the eyes of those who have read the post, as well as the authority of state power as a whole."*

Such formulations show that state bodies interpret criticism as an act that undermines the authority of the government, while judicial rhetoric in these cases typically appeals to categories such as "universal moral standards" and "the authority of state power," replacing legal criteria with political or moral judgments. This creates a legal environment in which any negative assessment of the authorities' actions can be classified as an insult.

By 2021, large numbers of criminal cases for comments on social media had already begun to appear. This was the period when a new model of repression took shape, and "speech as a crime" became a separate direction of state policy. Court proceedings were accompanied by linguistic "expert examinations" that classified even non-abusive phrases as insulting. These examinations are carried out not by independent specialists but mostly by loyal employees of state universities and educational institutions, turning them into instruments of political judgment. Across the country, this happens in a conveyor-like mode: almost any content that contradicts the official discourse is declared "extremist" in an expedited manner, without professional analysis or transparent procedures.

Typical formulations in court decisions show how the authorities use "linguistic examinations" to criminalize ordinary online expressions. One of the judgments states:

*"According to the inspection report of the specified publications, conducted by a specialist in phonoscopic and linguistic examinations, it was established that they contain images and text with negative evaluative meaning and an* ***improper form of verbal expression*** *... Expert Report … concludes that the posts published by B. on the social network O. contain an image comparing the state symbols of the Republic of Belarus with the symbols of [Nazi Germany], which is unacceptable from the point of view of modern culture; the publication depicts a comparison of the Republic of Belarus with a country based on Nazi ideology (as indicated by the placement of the coat of arms of the Republic of Belarus on a Nazi swastika, as well as the background of the image stylized as the national flag), which is* ***unacceptable from the point of view of modern culture*** *…"*

In another ruling, the court explains the "crime" in the following way:

*"...having chosen a method of disseminating such information designed for a wide and undefined circle of people, namely through the Internet, from an*

> *account under the pseudonym … in [Telegram] messenger, accessible for viewing by other users of this online resource, and expecting that other persons would perceive the insulting information, fully aware of the public and degrading nature of his statement and* ***intending to cause harm to the authority of state power and governance*** *… [as chat administrator] he posted an image depicting Minister I., who is a representative of state power and is protected by the state, [and] a* ***message contradicting universal moral standards and established norms of communication*** *between people, containing a statement expressed in an indecent form that demeans honor and dignity, and which, according to forensic linguistic examination evaluates [Minister I.] negatively."*

As the examples above show, "expert examinations" in Belarusian courts often become political interpretations of language. The court does not analyze context but relies on broad categories such as "universal moral standards," "indecent form," or "undermining the authority of state power." The conclusions are produced by loyal specialists from state universities, which makes independent analysis impossible. According to a lawyer from the Human Rights Center "Viasna," in most cases these linguistic examinations are purely formal and do not meet evidentiary standards. As a result, the trend toward self-censorship grows, with people refraining from expressing themselves openly online, which reduces participation in public communication and narrows the space for public debate.

## "Zeltser Case"

*Articles 369-1, 130 Part 1 of the Criminal Code*

After 2020, when the "insult" articles became some of the most frequently applied in criminal practice, several high-profile events triggered an especially harsh response from law enforcement and led to mass detentions. One of the first such cases was the "Zeltser case," which showed how a single online comment could become grounds for criminal prosecution.

On the evening of 28 September 2021, the State Security Committee (KGB) reported the death of one of its officers, who was shot during an operation to detain an "especially dangerous criminal." According to the official version, the shot was fired from a hunting rifle. The KGB officer died in the hospital, and the man who fired the shot was killed on the spot. He turned out to be Andrei Zeltser, an employee of the IT company EPAM.

Video of the incident was quickly distributed by state media, claiming it had been recorded by Zeltser's wife, Maryia Uspenskaya, who was soon arrested and taken to a pre-trial detention center. The events triggered widespread public reaction on social media. Within days, mass detentions began targeting people who expressed sympathy for the Zeltser family or criticized the actions of the security forces. According to human rights defenders, at least 135 criminal cases were opened in connection with online comments. Former political prisoners noted that in many cases, less than 24 hours passed between posting a comment and being detained. The detentions continued from the moment of the incident until 2024, including against people who returned to the country after living abroad. Typical prison sentences ranged from one to three years, and by mid-2025, 117 people had already served their terms and were released.

In most cases, the prosecution relied on Article 369-1 of the Criminal Code of Belarus, "Discrediting the Republic of Belarus," which allows punishment for statements that allegedly "undermine the authority of the state." The concluding part of one of the judgments states:

> *"...with the intent to demonstrate to an unlimited number of people knowingly false information about citizens of the Republic of Belarus approving and glorifying the crime committed by [Zeltser], as well as condemning the actions of KGB officers by presenting them as unlawful, thereby **undermining the authority of the KGB as a republican state body**, discrediting the Republic of Belarus, … forming a positive image of [Zeltser] and a negative attitude toward KGB officers..."*

Another part of the judgment explains the actions as being motivated by "political and ideological hostility:"

> *"Thus, the case reliably establishes that the accused, carrying out his criminal intent and the common goal aimed at disseminating knowingly false information about the legal status of citizens in the Republic of Belarus and the activities of state bodies, which discredit the Republic of Belarus, foreseeing and intending the consequences in the form of **causing substantial harm to state and public interests**, acted deliberately and purposefully, motivated by **political and ideological hostility**, fully aware of the public nature of his actions and wishing to commit them, **by posting information on the Internet**, using as a pretext the information about the killing [KGB officer], which on that same day and in the following days was widely covered in the media and on various Internet resources."*

A particularly telling case is that of Maryia Uspenskaya, the widow of Andrei Zeltser. She was arrested and placed in a pre-trial detention center, where, according to

non-public accounts from former detainees, she was subjected to punitive medical treatment. On 16 June 2022, Judge Valyantsina Ziankevich of the Minsk City Court declared the widow subject to compulsory treatment in a psychiatric facility and ordered her to pay 100,000 Belarusian rubles to the widow of the deceased KGB officer. As a result, Uspenskaya was isolated and unable to speak publicly about the circumstances of the tragedy. According to open sources, as of September 2025 she remains in the Novinki psychiatric clinic and is deprived of the ability to raise her minor son.

This case became an example of collective punishment and the state's complete control over the interpretation of public events in the online space. By criminalizing comments, the authorities eliminated any alternative to the official version of what had happened.

## Examples of Criminal Sentences for Online Comments (2021–2023)

| Case (comments) | Article of the Criminal Code of the Republic of Belarus | Year | Sentence |
|---|---|---|---|
| *"Иуда"*<br><br>*"Judas"* | Article 369 | 2022 | 2.5 years of restricted freedom (similar to probation), without placement in an open-type facility; fine of 1,000 BYN |
| The President was called a *"blabbermouth"* (in an obscene form) | Article 368 Part 1 | 2023 | 1 year of imprisonment |
| *"что ни рожа, то парася"*<br><br>*"every face looks like a piglet" (roughly)* | Article 369 | 2023 | 1.5 years of restricted freedom with placement in an open-type facility (similar to probation); fine of 3,700 BYN; 2,000 BYN in moral damages |

| | | | |
|---|---|---|---|
| *“Так этим тварям режимным и надо. Парня жалко.”*<br><br>*“That’s what these regime animals deserve. I feel sorry for the guy.”* | Articles 369-1 and 130 Part 1 | 2022 | 3 years of imprisonment |
| *“в стране страшнее, чем в Сомали”*<br><br>*“this country is scarier than Somalia”*<br>*“если бы было у меня ружье и ко мне ломались бы такие люди, я бы тоже защищал свой дом, только бы баррикады сделал”*<br><br>*“if I had a rifle and people like that were breaking in, I would also defend my home I’d even build barricades”* | Article 369-1 | 2022 | 2 years of imprisonment |
| *“Народ открыл счет.”*<br><br>*“The people have opened the score.”* | Article 130 Part 1 | 2022 | 3.5 years of imprisonment |
| *“Устроил терроризм и геноцид в стране, еще и оккупацией занялись.”*<br><br>*“They carried out terrorism and genocide in the country, and now they’ve moved on to occupation.”* | Article 367 Part 1 | 2022 | 2 years of imprisonment |
| *“Такія Хероі і хай увесь свет пачакае.”*<br><br>*“Such heroes – let the* | Article 369 | 2021 | 2 years of restricted freedom without placement in an open-type |

| | | | |
|---|---|---|---|
| *whole world wait."* | | | facility (similar to probation) |
| *"Андрей Зельцер у себя в квартире защищал свой дом, свою семью от неизвестных людей, которые выломали дверь при помощи топора. Он защищался, как умел..."*<br><br>*"Andrei Zeltser was defending his home and his family in his own apartment from unknown people who broke down the door with an axe. He defended himself the only way he could..."* | Article 130 Part 1 | 2022 | 1 year and 2 months of imprisonment |

These examples illustrate a clear disproportionality between the nature of the statements and the severity of the punishments imposed. Most comments are emotional or evaluative in tone and do not contain calls for violence, yet the authorities interpret them as crimes against state power or public morality. The court rulings show that the criminalization of speech in Belarus has reached a point where even a single comment on social media can lead to imprisonment.

## Anti-war statements

*Articles 368 Part 1 and 130 Part 1 of the Criminal Code*

After the Russian invasion of Ukraine in 2022, one of the most widespread directions of criminal prosecution in Belarus became the punishment of people for expressing an anti-war position. To "find" such individuals, security forces began actively using chat-roulette (an anonymous video chat platform). According to human rights defenders, the conversation partners were often provocateurs who intentionally steered the discussion toward topics of war, the authorities, or politics, prompting the person to speak openly. The conversations were recorded on video, after which

OSINT methods (tracking social media profiles, analyzing background details, devices, and speech) were used to identify the participants. Operational groups were then sent to their homes, and people were detained under Article 368 Part 1 and Article 130 Part 1 of the Criminal Code. According to Dissidentby, at least 12 such cases are known; in 10 of them, the fate of the individuals remains unknown, despite their personal information having been published in pro-government social media channels along with claims of their "detention."

One of the most well-known cases was that of Dzmitry Lahutsenka, a resident of Rahachou. He was detained together with a friend; officers placed white-red-white flags over their heads and forced them to mop the floor with the flags. After the arrest, Lahutsenka was taken to a pre-trial detention center, later sentenced to three years in prison, and added to the "terrorist list." After a year and a half, he was released under a presidential "pardon."

This case is telling because the authorities do not simply respond to already expressed online statements, they deliberately create conditions to provoke these statements. In the case of chat-roulette, the state moves from monitoring to actively participating in communication, pushing people to say things that then become grounds for criminal prosecution.

## Prosecution for Supporting Initiatives Through Donations

*Articles 361-2 Parts 1 and 2, 361-3 Parts 1 and 2, 361-4 Parts 1 and 2, 290-1 Parts 1 and 2 of the Criminal Code*

After criminal prosecution for comments and online expressions became routine, the authorities expanded their control to the sphere of civic solidarity. The next stage was the prosecution of donations, where punishment was applied for any attempt to provide financial support to victims, media outlets, humanitarian projects, or civic initiatives that were later labeled "extremist" or "terrorist." After 2021, Belarus launched a systematic campaign of designating initiatives and organizations as "extremist formations." The list began to include not only civic groups but also human rights, media, and humanitarian projects. As a result, almost any financial support became risky, and even a symbolic contribution could lead to a criminal case.

The cases of prosecution for donations have several specific features. *First*, when security forces detect a transfer of money to an initiative labeled as "extremist," the person is summoned to the KGB, where they are pressured to admit guilt and offered to "compensate the damage," usually in an amount ten times larger than the donation. According to victims, this "compensation" is not regulated by any formal documents and does not guarantee safety or an end to the persecution. It is not uncommon for people who have already paid the "compensation" to be detained again and later convicted under criminal articles for the same donation.

*Second*, an important aspect is the disproportionality of the punishment. One of the judgments documented a case in which a person attempted to make a donation of USD 16.17 (47 rubles 59 kopecks) to Kastus Kalinouski Regiment, a volunteer armed formation within the Armed Forces of Ukraine. , which ultimately did not even reach the recipient and was returned by the bank. Nevertheless, the court classified this as an "attempt to facilitate extremist activity" and sentenced the donor to three years of imprisonment:

> *"...acting intentionally, she attempted to transfer funds in the amount of 16.17 US dollars to bank account … used by representatives of the extremist formation [Kastus Kalinouski Regiment], … thereby attempting to* ***provide funds for the deliberate support of extremist activity****; however, these funds were later returned to her by the issuing bank due to the prohibition on carrying out this banking operation.*
>
> *… claims that she did not intend to provide funds for the deliberate support of extremist activity, because [Kastus Kalinouski Regiment] had not yet been recognized as an extremist formation at the time of the act, are unfounded, since* ***publicly available information on the Internet indicates the destructive nature of this formation****. Her own statements during the pre-trial investigation acknowledged that she understood she was helping citizens of the Republic of Belarus who were members of it and who participated in combat operations on the side of Ukraine"*

This fragment of the judgment shows that Belarusian courts in practice rely not on legal but on political categories. Instead of proving intent or actual harm to the state, they use formulations such as "the destructive nature of the formation" or "information available in open sources."

*Third*, a key element of persecution is the use of retroactive application of the law. People are prosecuted for transfers made before an organization or initiative was designated as "extremist." A telling example is the case of IT specialist Aliaksandr Ziyazedinau, who made a donation in support of BYPOL in May 2021. The organization was declared "extremist" only in November of that year, yet in 2022

Aliaksandr was sentenced to three years in prison. A year later, when BYPOL had already been designated a "terrorist organization," a new case was opened against him, and in 2024 the court sentenced him to an additional nine years of imprisonment.

These cases show how the state criminalizes the act of solidarity itself, regardless of its real impact or the moment it was carried out. In Belarus, donations have been transformed from a form of support into "evidence of involvement in extremist activity," reflecting a broader trend of fully criminalizing civil society. As a result, financial support is now treated as an act of political disloyalty, and civic solidarity as a crime.

## Prosecution for Participation in Digital Initiatives and Online Communities

*Articles 361-1, 361-2, 361-4 of the Criminal Code*

While a systemic "cleansing" of civic activity was taking place inside the country, events unfolding in the region demanded new forms of response and engagement from Belarusian society. Russia's full-scale invasion of Ukraine in 2022 became a catalyst for the development of new forms of online resistance from volunteer networks to OSINT monitoring projects. Belarusian society expressed a strong anti-war stance, manifested not only in street protests and social media statements but also in the creation of information initiatives focused on collecting and disseminating facts about the war.

The most well-known example was the "Belaruski Hajun" project, which had around 345,000 subscribers and brought together users from across the country who shared information about the movement of military equipment, aircraft flights, railway transportation, and other military activity. This made it possible to quickly collect and analyze open-source data and make it accessible to the public, journalists, and analysts. In early February 2025, security forces gained access to the project's chats and chatbot, as well as to part of the user data. Within days, mass detentions began targeting people who had sent photos or videos of military equipment. As a result, "Belaruski Hajun" was forced to announce the termination of its operations.

According to the Human Rights Center "Viasna," at least 122 people are known to have been detained and convicted in connection with the "Hajun case." In most instances, people were charged under Article 361-4 of the Criminal Code ("assisting extremist activity"), receiving sentences ranging from three to five years of

imprisonment or up to four years of restricted freedom, with or without placement in an open-type facility. In one of the judgments, the court describes the defendant's actions in the following way:

> *"[defendant] at an unidentified time, but no later than 16⁵⁰ on 10 February 2023, while on the territory of the Republic of Belarus and the city of ** (the precise location not established),* ***having the intent to assist extremist activity,*** *including by expressing* ***disagreement with the special military operation conducted by the Russian Federation on the territory of the Republic of Ukraine for demilitarization and denazification with the aim of protecting the civilian population****, contacted the Telegram bot 'Dapamozha Hajun,' which is part of the structure of the Telegram channel 'Belaruski Hajun,' which, according to the decision of the Central District Court of Minsk of 18 March 2022, is recognized as extremist materials..."*

Such formulations show that Belarusian courts not only adopt the rhetoric of Russian state propaganda but also effectively integrate it into legal texts. Court judgments begin to include language that repeats Kremlin narratives about the "special military operation," "denazification," and "protection of the civilian population," turning these phrases into instruments of informational warfare in the region.

From the very beginning of the 2020 protests, the internet, especially social networks and messengers, became the main space for coordination and information exchange. In cities and districts across the country, hundreds of local and decentralized chats emerged, from neighborhood groups to small private channels for just a few people. They were used to discuss events and organize collective actions. Over time, more structured online initiatives, chatbots, and platforms appeared, offering relatively safe forms of civic participation, including coordination and mutual support.

However, in the practice of the Belarusian authorities, even participation in such chats and communication with bots began to be interpreted as "assisting extremist activity." Administrative functions, routine moderation, or sharing information within a community are treated as "managing an extremist formation."

One court ruling explains the actions of an administrator of a local neighbourhood chat who moderated the chat by refusing to add pro-state provocateurs as chat members in the following way:

> *"Performing the functions of an administrator of the Telegram channel ', in addition to deleting users' messages, [the defendant] formed the composition of the channel's participants in accordance with the*

> *administrator's functions — by adding and removing them (as evidenced by the established fact of changes in the group's number of participants), as well as* ***blocking users who supported the existing constitutional order****; formed and adjusted the channel's news agenda,* ***controlled the content of the channel by filling it with extremist materials aimed at discrediting the Republic of Belarus****, state authorities and administration, disseminated knowingly false information about the economic, political, and international situation of the Republic of Belarus, containing public calls to plan, organize, prepare, and commit acts encroaching on the foundations of the constitutional order and public security of the Republic of Belarus, thereby* ***consolidating and supporting the growth of radical protest sentiment in society****; that is, he directed the* ***extremist activity of the participants of the Telegram channel****."*

Among digital initiatives, one of the main targets of repression became the "Peramoha" ("Victory") project – an anonymous chatbot through which users could submit their contact details, indicate readiness to participate in future protest actions, or support coordination structures. According to Dissidentby, at least **39 people were detained on criminal charges** for registering with this initiative. The authorities treated even the mere fact of interacting with "Peramoha" as "participation in an extremist formation," despite the fact that most users took no action beyond clicking the "start" button. In 2025, the project was shut down due to repression and criticism from civil society.

A separate direction of repression has been the criminalization of contacts with initiatives operating outside Belarus. One such example is the Kastus Kalinouski Regiment, a volunteer armed formation within the Armed Forces of Ukraine. According to Dissidentby, at least **29 people were detained** for registering in the regiment's chatbot or attempting to join its ranks. Participation in its activities, as well as any attempt to join the regiment or communicate with its representatives online, began to be treated as "participation in an extremist formation" or "assisting terrorism." One of the cases involved a man who was convicted simply for attempting to register through the chatbot. The court's wording shows that even online correspondence or the intention to take part in such an initiative is viewed as a crime:

> *"He, being a citizen of the Republic of Belarus, no earlier than 24 February 2022, while on the territory of the Republic of Belarus, including in the city of Minsk, as well as near border …, located within the border strip of the Lielchytsy District of the Homel Region of the Republic of Belarus, acting intentionally, through an agreement and* ***established communication with an unidentified representative of the armed formation*** *— the separate Belarusian regiment named after Kastus Kalinouski, which is part of the*

*International Legion of Territorial Defense of the Armed Forces of Ukraine. By following instructions, collecting personal belongings, and attempting to illegally cross the State Border of the Republic of Belarus in the direction of Ukraine, [he]* ***prepared to participate in said armed formation*** *of the opposing side — Ukraine, in military actions and in the armed conflict taking place on its territory without authorization from the Republic of Belarus.*

…

*Since [he] prepared to participate, as a citizen of the Republic of Belarus, on the territory of a foreign state in an armed formation of one of the opposing sides, as well as to participate in an armed conflict and military actions without state authorization and in the absence of elements of the crime provided for in Article 133 of the Criminal Code ("Mercenarism"), his actions in this part fall under and shall be qualified according to Article 13 Part 1 and Article 361-3 Part 1 of the Criminal Code."*

Human rights defenders have documented cases where, during searches and interrogations, security forces gained access to detainees' phones or laptops and manually launched chatbots themselves, including "Peramoha" or other related initiatives. This allowed them to artificially create grounds for prosecution. In addition, there have been cases in which security agencies created fake chatbots that fully replicated the design and functionality of genuine civic initiative tools. These fake bots were used to collect user data and carry out subsequent detentions.

## Criminalization of De-anonymization Efforts and Attempts to Hold Security Forces Accountable

*Articles 203-1 Parts 1–3, 352 Parts 1–3, 130 Part 3, 179 Part 1, 364 and 365, 426 Parts 2 and 3 of the Criminal Code*

After 2020, as repression intensified and state institutions became increasingly opaque, several initiatives emerged that sought to document and disclose information about individuals involved in violence and persecution. One such initiative was the "Black Book of Belarus" – a project that collected data on security officers, judges, propagandists, and officials. State authorities treated this activity as the "dissemination of personal data," which led to numerous criminal cases against participants and "informants" of the initiative.

Participation in such initiatives was often spontaneous, and information security issues remained overlooked. In May 2021, Sofia Sapega was detained, and through

her computer security forces gained access to user accounts and correspondence of project participants. It was later revealed that from October 2020 to May 2021, a GUBAZIK officer, Artur Haiko, had been working inside the "Black Book of Belarus," effectively controlling part of the communication and transmitting information to the security agencies. According to official statements, large volumes of data came into the authorities' possession, leading to dozens of criminal cases and lengthy prison sentences. According to Dissidentby, at least **37 people were convicted** in connection with this case, many receiving up to ten years of imprisonment.

One such case was the trial of Aliaksei Kuzmin, a father of many children and an employee of a telecommunications company. According to the investigation materials, he had access to information about MTS clients and passed some of this data to Telegram channels, including the "Black Book of Belarus." The case listed 57 "victims," among them security officers, propagandists, officials, prosecutors, and members of their families. He was sentenced to seven years of imprisonment.

Another example is Dzmitry Kakhanouski, an employee of the Mahiliou branch of Beltelecom. For transmitting information about individuals involved in repression, he was convicted under three articles of the Criminal Code (Article 203-1 Part 3, Article 130 Part 3, and Article 352 Part 3) and sentenced to six and a half years in prison.

Although the publication of personal data does indeed contradict European standards of data protection (including GDPR requirements), these actions cannot be viewed unambiguously in the Belarusian context of 2020. In the case of the "Black Book of Belarus," the aim was not to violate privacy but to seek public accountability and demand justice in a situation where legal mechanisms had completely collapsed and access to justice was impossible. These actions can be interpreted as a civic response to impunity at a time when traditional channels of protection inside the country had ceased to exist, as not a single criminal case was opened against security officers in Belarus.

## Repression Against Journalists

*Articles 361-1 Parts 1–3, 361-3 Parts 1–3, 369-1, 361 Parts 1–3 of the Criminal Code*

Journalistic activity in Belarus has also come under total state control. According to the Belarusian Association of Journalists (BAJ), by the end of 2025, 43 media projects and editorial offices had been designated as "extremist formations" – a legal classification that allows the criminalization of any involvement in their work or interaction with them. This means that journalists and technical staff can be held

criminally liable even if, by the time the outlet was declared “extremist,” they were no longer connected to its activities.

According to Dissidentby, at least **76 journalists have been subjected to repression**. In 2024 alone, according to BAJ, 30 people became defendants in criminal cases, 66 experienced home searches, and 19 were subjected to administrative prosecution. In 2025, the number of searches increased to 34, and another 4 journalists were convicted under administrative articles.

One of the first high-profile cases of criminal prosecution of journalists was the case of Belsat TV reporters Katsiaryna Bakhvalava and Darya Chultsova, who were detained while livestreaming a spontaneous memorial gathering for Raman Bandarenka in November 2020. At that time, repression against the media had not yet been institutionalized, so the charges were based not on “extremism” articles but on Article 342 of the Criminal Code. Later, such practices expanded, and journalists began to be prosecuted not only for covering events but also for alleged “tax violations.” Article 243 of the Criminal Code, for instance, was used as a tool to crack down on independent media under the guise of economic crimes.

Starting in 2021, repression against journalists acquired a systemic and legal character. Materials from independent outlets, social media posts, and even comments were labeled as “extremist materials,” while the outlets themselves were designated as “extremist formations.” This meant that journalistic work in Belarus became equated with “extremist crimes,” and Articles 361-1, 361-3, 369-1, and 361 of the Criminal Code became the primary tools for criminal prosecution of media workers, effectively stripping them of the right to practice their profession.

In Belarusian realities, “extremism legislation” has turned into a universal instrument for dismantling professional communities that possess their own channels of communication and influence. By designating independent media as “extremist formations,” the state eliminated the last remaining spaces of independent journalism and free information. Similar mechanisms are applied to other groups as well such as human rights defenders, lawyers, and volunteers. As a result, the concept of “extremism” in the Belarusian context has lost its legal clarity and has come to mean any form of autonomous civic activity that falls outside state control.

## Repression Against Relatives of Political Prisoners

*Article 361-4 of the Criminal Code*

Over the past two years, a new trend of repression has emerged in Belarus – the criminal prosecution of relatives of political prisoners. Whereas previously the state focused on direct participants in protests or civic activists, it now targets the close family members of those who have already suffered under the regime. Most often, the grounds for criminal cases are interviews given to independent media outlets that have been designated as "extremist formations." The timing of publication does not matter: even interviews recorded two years earlier can be used as a basis for prosecution.

One of the first examples was the case of Darya Losik, the wife of former political prisoner and journalist Ihar Losik. Darya publicly advocated for her husband and raised their daughter while he was imprisoned. For giving an interview to Belsat TV designated as an "extremist formation" she was sentenced to two years in prison. This case sent a clear signal to other families of political prisoners that any communication with independent media can now be treated as "assisting extremist activity."

In the summer of 2024, similar detentions targeted Tatsiana Frantskevich and Natallia Labatsevich, both mothers of political prisoners. The sons of both women had already been repressed: Natallia's son, Ilya, served a sentence for participating in protests and left Belarus in 2022, while Tatsiana's son had been sentenced to 18 years in prison. Both women publicly supported their children between 2020 and 2022, and years later were detained for these actions. According to the investigation, the grounds were two interviews given to Belsat TV; Natallia Labatsevich was sentenced to three years in prison, and Tatsiana Frantskevich to three years and three months. In addition, many relatives of current political prisoners have been forced to leave the country due to threats of prosecution and are now listed in the national wanted database.

Thus, political repression is turning into a form of collective punishment, where not only direct participants in events suffer but also their families. The state uses the criminal prosecution of relatives as an additional tool of pressure to isolate political prisoners, deprive them of support, and create an atmosphere of total fear. In a number of cases, the authorities confiscate or forcibly sell the property of those convicted, effectively turning repression into punishment for the entire family. As a result, many people find themselves separated across different countries, unable to meet, support one another, or speak openly about their experiences. This practice shows that the Belarusian system of repression extends far beyond individual

persecution and functions as a mechanism of collective intimidation and the dismantling of social ties.

## Statistics 2020–2025: Legal Commentary

The statistics reflect the number of cases in which investigative authorities classified the actions of residents of the country under specific articles of the Criminal Code of the Republic of Belarus. In many cases, several articles appear simultaneously within a single criminal case, which means that the total number of recorded violations exceeds the number of individuals prosecuted. According to the human rights initiative Dissidentby, at least **3,476 people have been convicted** in criminal cases related to online activity. Of these, charges connected to expressing opinions on social media were brought against 2,799 people, while 997 cases involved online activism and participation in digital initiatives.

| Article of the Criminal Code of the Republic of Belarus | Qualification | Number of cases in which the article was applied (2020–2025)* |
|---|---|---|
| Art. 367 Parts 1, 2 | Defamation of the President of the Republic of Belarus | 328 |
| Art. 368 parts 1, 2 | Insulting the President of the Republic of Belarus | 1186 |
| Art. 369 | Insulting a representative of authority | 1357 |
| Art. 391 | Insulting a judge or lay judge | 115 |
| Art. 369-1 | Discrediting the Republic of Belarus | 72 |
| Art. 130 parts 1–3 | Incitement of racial, national, religious, or other social hatred or discord | 823 |
| Art. 179 part 1 (removed from the Criminal Code of the Republic of Belarus) | Illegal collection and dissemination of information about private life | 23 |

| | | |
|---|---|---|
| Art. 426 parts 1–3 | Abuse of power or official authority | 21 |
| Art. 361-2 parts 1, 2 | Financing extremist activity | 150 |
| Art. 361-3 parts 1, 2 | Participation on the territory of a foreign state in an armed formation or armed conflict, military actions, recruitment or training of persons for such participation | 80 |
| Art. 361-4 parts 1, 2 | Assisting extremist activity | 430 |
| Art. 290-1 parts 1, 2 | Financing terrorist activity | 36 |
| Art. 361-1 parts 1–3 | Creation of an extremist formation or participation in it | 359 |
| Art. 203-1 parts 1–3 | Unlawful actions regarding information about private life and personal data | 91 |
| Art. 352 parts 1–3 (removed from the Criminal Code of the Republic of Belarus) | Unlawful acquisition of computer information | 23 |

**Indicates the number of cases in which the article was used in the qualification of actions (a single person may have several articles listed in the indictment).*

International standards require that any restrictions on freedom of expression and communication must simultaneously be prescribed by clear and foreseeable law, pursue a legitimate and evidence-based aim (such as protecting the rights of others or ensuring security), and remain the least restrictive means available to achieve that aim. This so-called three-part test — legality, necessity, and proportionality — is the universal standard for assessing restrictions on freedom of expression under Article 19 of the ICCPR and Article 10 of the ECHR.

**In practical terms:**

**Legality** means that restrictions must be grounded in a law that is sufficiently clear and foreseeable, allowing a person to understand when and for what their expression may be limited. If legal concepts are too broad or vague, this creates a risk of arbitrary application and effectively makes everyone a potential offender.

**Necessity** requires that a restriction genuinely pursue a legitimate aim, for example, protecting national security, public order, health, or the rights of others, and that a real and demonstrable threat exists in a democratic society to justify such interference.

**Proportionality** means that the measures chosen must be the least restrictive available to achieve the aim; the state must consider alternatives that would cause less harm to freedom of expression.

In Belarus, the requirements of international standards on freedom of expression are systematically disregarded. Restrictions are used primarily as a tool for controlling information and civic activity rather than for protecting legitimate interests:

**Legality.** Key components such as “discrediting the state,” “assisting extremist activity,” or “insult” are formulated in overly broad and evaluative terms; court rulings rely on non-legal categories such as “universal morality” or “undermining the authority of the state,” which do not meet the requirements of clarity and foreseeability.

**Necessity.** Criminal cases for comments, donations, subscriptions, or registration in chatbots do not demonstrate the existence of any real threat to security and pursue not a protective but a political aim, namely, suppressing criticism and solidarity with repressed individuals.

**Proportionality.** Actual prison sentences for expressions, symbolic transfers, and technical online actions are excessive and have an intimidating effect. Less restrictive alternatives were not considered by the state (for example, Article 10.2 of the Administrative Code on “insult”).

The right to privacy under Article 17 ICCPR and within a data protection framework like GDPR is likewise infringed. During detentions, security forces gain access to phones and user accounts without effective judicial oversight; fake chatbots and channels are created and used to identify users; extensive monitoring and de-anonymization checks are carried out (cross-matching nicknames, photos, metadata). Such practices result in disproportionate interference with private life and unjustifiably restrict freedom of communication. In the international context, the relevant standards are set by the EU General Data Protection Regulation (GDPR), which requires legality and minimization in the processing of personal data. Although Belarus is not a party to the GDPR, these principles remain a benchmark for assessing privacy violations.

# Conclusion. Consequences and emerging trends

The legal landscape described above is reflected in the everyday experience of individuals, communities, and organisations. The criminalisation of online expression, support for civic initiatives, or even the simple consumption of information produces concrete social consequences that reshape behaviour and the structure of society. Below are several trends and behavioural patterns that emerge as a result of these “digital repressions” and illustrate how communities adapt to constant risk and control.

## Self-censorship driven by “digital fear”

The criminalisation of comments, subscriptions, and donations has led to widespread self-restraint in expression: people delete old posts and comments (there are even initiatives that help users find and remove past comments), close their accounts, and avoid reacting to or subscribing to channels labelled as “extremist.” Systematic content removal and self-censorship result in society losing its own evidence of repression and key social and political processes. Without public traces, the past becomes less visible, and meaningful re-evaluation of historical events becomes nearly impossible, opening the way for their reinterpretation in an ideologically convenient direction. This erases a significant part of the country’s socio-political history, makes the online space predictably silent, and wipes out the digital footprint of repression.

## Forced displacement and fragmentation of communities

The risk of criminal prosecution pushes activists, journalists, human rights defenders, and their families into forced emigration. This leads to the fragmentation of civil society: some remain inside the country under constant surveillance, while others continue their work from abroad but without the ability to communicate safely with those still in Belarus.

An information gap gradually emerges. People inside the country have restricted access to blocked media and cannot freely read or comment on their materials, while communities in exile operate within a different information reality. This not only undermines cohesion but creates a “double isolation”: independent media and

initiatives lose the ability to receive comments and testimonies from inside the country, and people inside the country lose the ability to be heard. Moreover, because independent media have been designated as “extremist formations” and professional activity is effectively banned, many journalists have been deprived of their profession and are forced to work anonymously or leave the country.

## The shift of activism into “dark zones”

After open communication platforms were dismantled, organising and civic activity moved into encrypted channels and closed infrastructures that rely on VPNs, Tor, secret chats, and end-to-end encryption. Operational security has become an inseparable part of civic engagement, but the cost of participation has increased significantly. To simply read the news or watch a video, people now have to use circumvention tools, browse in anonymous modes, clear their viewing history, disable geolocation, and unsubscribe from channels immediately after reading their content.

## Digital divide

This makes access to information more difficult and increasingly uneven. People with limited technical skills or insufficient digital experience (especially teenagers and students) risk facing repression without fully understanding the consequences of their actions — for example, when they react to or comment on a post labelled as “extremist.” As a result, young people are increasingly turning to “safe” channels where information is presented in a propagandistic format, while banned media are forced to publish content without their branding in order to reach a non-politicised audience.

For the older generation the situation is even more challenging: many pensioners and older adults lack digital security skills and therefore deliberately avoid reading alternative media to reduce risks. This leads to the informational isolation of large groups of the population and widens the gap between generations  in terms of trust, access to information, and understanding of reality.

## Systemic repression of online activity

The conveyor-belt designation of channels and initiatives as “extremist,” along with the continuous expansion of lists of “extremist materials” and “extremist formations,” creates a stable administrative-legal framework in which any communication outside state control can be reclassified as a crime at any moment. The system operates on arbitrary and non-transparent criteria, contradicting the principle of legal certainty.

For example, in donation-related cases, courts found people guilty even when, at the moment of transferring funds, they could not have known the status of the recipient. In one such ruling, the court stated that “the destructive nature of this formation is evidenced by information publicly available on the Internet,” effectively substituting legal norms with a subjective assessment of “destructiveness.” As a result, the boundaries of permissible conduct are constantly shifted retroactively, illustrating the complete arbitrariness with which criminal law is applied to online activity in Belarus.

## Information scarcity

Systematic blocking, the labelling of independent media as “extremist,” and the fear of using open sources create a chronic deficit of reliable information. People deprived of safe access to alternative media are forced to rely either on state-controlled channels or on random anonymous sources. Over time, this produces a habit of consuming fragmented information, where instead of a coherent picture of events people see only snippets, rumours, and second-hand retellings which significantly increases society’s vulnerability to propaganda and disinformation.

## Withdrawal from civic engagement

Constant fear of potential consequences pushes many people not only into silence but into fully abandoning any civic or volunteer activity. Individuals stop subscribing to initiatives, avoid participating in fundraising, do not sign petitions, and even refrain from discussing social or political issues online. This leads to a gradual erosion of the culture of participation and solidarity.

Where participation in online communities once served as a way to express civic position, it is now perceived as a potential risk. As a result, people shift their

engagement into the private sphere, where it becomes invisible to the community and to human rights defenders, making it harder to document violations and provide assistance in cases of detention. Others choose complete non-involvement, weakening civic solidarity and reducing the capacity for collective action.

Even under conditions of deepening control, preserving and documenting the truth about repression remains a foundation of civic resilience. When online resistance is met with online oppression, recording facts and transmitting them through independent channels becomes a form of response to state violence.

Another, fully practical response to digital threats is strengthening technological literacy and holistic security culture. Using encrypted communication tools, handling personal data responsibly, and understanding the risks associated with online activity make life in the digital space (relatively) safer. Building these skills does not eliminate repression, which itself relies on digital technologies, but it expands the space of action available to civil society. Beyond individual efforts, coordination and knowledge-sharing among organisations working in human rights, digital security, and media literacy are essential. This creates a network of solidarity capable of responding more quickly to emerging threats, supporting people under pressure, and working to prevent further repression.