Submission by Association Human Constanta International
to the Human Rights Committee
Call for inputs on Draft General Comment No. 38

Ms. Hélène Tigroudja,
Rapporteur for the drafting of the General Comment No. 38 on Article 22
of the International Covenant on Civil and Political Rights,

19 December 2025

In response to the Human Rights Committee's call for inputs on the draft General Comment No. 38 on Article 22 of the International Covenant on Civil and Political Rights (freedom of association), Association Human Constanta International submits the following observations on digitally enabled interference with freedom of association and the conditions for civic participation, drawing on our monitoring and documentation of these patterns in Belarus and in relation to communities living in exile.

As collective action, civic mobilisation, and democratic participation increasingly rely on digital infrastructures, interference with freedom of association is no longer limited to the formal banning of organisations or physical dispersal of assemblies. Instead, association can be undermined through the monitoring and infiltration of online communities, the criminalisation of diverse forms of digital participation on vague national security or counter-terrorism grounds, and the deployment of hostile online discourse that portrays civic actors as threats to public order or "extremists."[1] These dynamics, recognised in the Committee's concept note, are central to the global trends of civic space closure and the rise of authoritarianism.[2]

Belarus provides a clear example of how these patterns unfold in practice under sustained and growing repression. Since the contested 2020 presidential elections, and further intensified following the involvement of Belarusian authorities in Russia's full-scale invasion of Ukraine, the human rights situation in the country has been severely deteriorating. Over this period, the toolkit of state repression has expanded beyond visible, street-level measures to encompass a growing use of digital tools to monitor, control, and police online forms of association and collective action. As a result, civic space in Belarus has been further shrinking, with fear and self-censorship becoming defining features of participation and online platforms becoming primary sites of surveillance and broader human rights abuses.

The work of Association Human Constanta Int. shows how ordinary acts of digital participation in this context, such as following a channel, administering a chat, sharing information, or donating online, are routinely reframed as forms of "participation" or "assistance" in

[1] Human Rights Committee, Concept Note on the Draft General Comment No 38 on Article 22 (Freedom of Association) (OHCHR, 2025) para 8
[2] UN General Assembly, Protecting the rights to freedom of peaceful assembly and of association from stigmatization: Note by the Secretary-General A/79/263 (July 2024) https://docs.un.org/en/A/79/263 para 1

"extremist" activity.[3] Through such measures, communities of even small scale are criminalised, and collective action ends up being disrupted at a very early stage, often before physical assembly can take place. This has a profoundly chilling effect on freedom of assembly and association, leading to community fragmentation and a withdrawal from political and civic participation. Importantly, the effects of such digital repression are not confined to the state's territory. As documented by Association Human Constanta Int. in relation to exiled communities, practices of online surveillance, intimidation, and legal stigmatisation continue to shape people's willingness and ability to organise and participate in associational life even when living abroad.[4] This pipeline from domestic to transnational forms of repression further underscores the need for the Committee's interpretation of Article 22 to reflect the modern realities of digital civic spaces and their cross-border nature.

With this in mind, this submission is structured as follows. First, it examines how digitally enabled practices of surveillance, infiltration, and entrapment interfere with the exercise of freedom of assembly and association in practice by making online spaces unsafe for organising, even before legal action is taken. Second, it examines how these forms of activity are subsequently transformed into criminal liability through the application of anti-extremism frameworks. Finally, the submission covers how these mechanisms subsequently extend beyond territorial borders through digital means, affecting the ability of those living in exile abroad to associate and organise too, analysing the implications of these developments for the Committee's guidance on the interpretation of Article 22 in light of the digital age.

1. Digital surveillance, infiltration and entrapment as interference with freedom of assembly and association

Digital infrastructures have become central to the ability of individuals and groups to communicate, organise, and coordinate, particularly in contexts where opportunities for more traditional forms of civic mobilisation are restricted. Corresponding methods of digital control have increasingly been integrated into such infrastructures, becoming a part of standard state practices of investigation and subsequent repression.[5]

One form of such control, for example, is the use of telecommunications data to establish the fact of participation in assemblies. Association Human Constanta Int. documented instances in which mobile billing data was used as proof of presence at political protests, without the need for additional evidence.[6] In practice, this meant that digital traces alone were sufficient to identify and pursue individuals who had taken part. Alongside this form of surveillance, online spaces themselves have been subject to interference from within. Another documented case

[3] Human Constanta, From Streets to Screens: Digital Repression in Belarus (2025) https://humanconstanta.org/en/strees-screens-en/; ARTICLE 19 and Human Constanta, Quashing Online Dissent: Anti-Extremism Laws Put Digital Rights as Risk in Belarus https://www.article19.org/resources/belarus-anti-extremism-laws-put-digital-rights-at-risk/ (2025)
[4] Human Constanta, Repression Without Borders: Transnational Authoritarianism in the Digital Age (2025) https://humanconstanta.org/en/repression-without-borders-transnational-authoritarianism-in-the-digital-age/
[5] Human Constanta, From Streets to Screens: Digital Repression in Belarus (2025) https://humanconstanta.org/en/strees-screens-en/ page 6
[6] Ibid.

saw a person linked to the Belarusian security services gain access to a group chat and begin interacting with its members. Several participants who followed those messages were later charged, with the infiltrator's testimony used in court.[7] Following incidents of this kind, participation in online activity can no longer be perceived as neutral or low-risk, as engagement itself may later be used as a basis for identification and prosecution.

In some cases, these forms of interference go beyond data gathering or infiltration and involve other types of manipulation. In some documented cases, authorities accessed detainees' phones or laptops and activated chatbots themselves, later relying on this activity in criminal cases.[8] In addition, there have been cases in which fake chatbots, or the so-called "honeypots," were created to fully replicate the design and functionality of genuine civic initiative tools and lure people into disclosing their data. Such "honeypots" are increasingly used to manipulate users to collect their information and carry out subsequent detentions.[9] One notable reported case involved a fake Telegram channel posing as BYPOL, an association of former Belarusian law enforcement officers in exile. It promoted the so-called "Peramoga 2.0" assembly plan and urged visitors to click on a link containing more details on how to take part; one man clicked and was tracked down shortly after the malicious site harvested his data and exposed him to the authorities.[10] In such situations, online spaces that people rely on to organise and associate no longer feel safe, as participating can directly expose individuals to questioning, detention, or prosecution.

Seen in practice, digital tools are increasingly used to interfere with the association itself, rather than simply to observe it. Surveillance and infiltration change how people interact online, as routine acts of participation begin to carry the risk of exposure. In such an environment, the freedom of assembly and association becomes dependent on whether individuals can maintain their trust and digital security in the online spaces through which they attempt to organise. These dynamics amount to a form of interference in which individuals are deliberately discouraged from association in the first place, undermining the conditions necessary for the exercise of Article 22 rights even before the questions of criminal liability or prohibitions arise, and illustrating the need for the Committee's guidance to address such forms of interference.

2. Criminalisation of online association through anti-extremism legal frameworks

The practices described above do not operate in isolation. Once an online association becomes visible or carries exposure due to surveillance, infiltration, or digital manipulation, authorities

[7] 'Родные политзаключенных по делу чата: "По нарушениям в суде можно написать целую книгу"' ['Relatives of political prisoners in the chat case: "One could write an entire book about the violations in court"'] Spring96.org (6 August 2021) https://spring96.org/ru/news/104576

[8] Human Constanta, From Streets to Screens: Digital Repression in Belarus (2025) https://humanconstanta.org/en/strees-screens-en/ page 19

[9] Ibid.

[10] «Увидел ссылку, нажал. А вскоре ко мне приехали». Что силовики могут узнать о вас по одному клику ['"Saw a link, clicked it. They soon came for me." What the security services can learn about you with one click'] Zerkalo.io (26 September 2024) https://news.zerkalo.io/life/79249.htm

in Belarus rely on an expansive anti-extremism framework to legally transform diverse forms of digital participation into criminal conduct.

Association Human Constanta Int. and Article 19 document that Belarusian anti-extremism laws are regularly applied to a wide range of online activities which would otherwise fall within the scope of protected association. As their reporting notes, criminal prosecutions have been recorded for activities including "registering in activists' chatbots, joining activists' chats, participating in online educational programs, sharing information on military and police movements online, engaging in chat roulette conversations,"[11] and so on. Such a sweeping approach not only undermines the legal certainty and wider rule of law but also collapses the distinction between active participation and passive association, as even the most minimal forms of online engagement are treated as sufficient grounds for prosecution.

The very designation of digital communities as "extremist" is central to this process. Under Belarusian law, such designations can be made extrajudicially: "extremist formation" designation can be made upon administrative decision of either the Ministry of Internal Affairs or the State Security Committee (KGB). The list of formations is expansive, with more than 300 entities, primarily independent media and activist networks.[12] Such labelling has been extensively applied to both local digital communities and large online initiatives which combine hundreds of chats, allowing virtually any digital space to be treated as a structural subdivision of an "extremist formation."[13] The report "From Streets to Screens" further demonstrates how this logic is applied in courts. One court ruling described the role of an online chat administrator as follows: "Performing the functions of an administrator of the Telegram channel, the defendant formed the composition of the channel's participants, controlled the content of the channel, 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."[14] Such criminalisation may even be applied retroactively, with cases reported in which individuals were detained for participating in online communities before those communities were formally designated as "extremist."[15]

---

[11] ARTICLE 19 and Human Constanta, Quashing Online Dissent: Anti-Extremism Laws Put Digital Rights as Risk in Belarus https://www.article19.org/resources/belarus-anti-extremism-laws-put-digital-rights-at-risk/ (2025) page 6

[12] 'Разбираемся с «экстремистскими» списками: перечень организаций, формирований, ИП, причастных к «экстремистской» деятельности' ['Explaining the "extremist" lists: the catalogue of organisations, formations and individuals involved in "extremist" activity'] Association Human Constanta Int. (6 March 2023) https://humanconstanta.org/razbiraemsya-s-ekstremistskimi-spiskami-perechen-organizacij-formirovanij-ip-prichastnyx-k-ekstremistskoj-deyatelnosti/

[13] ARTICLE 19 and Human Constanta, Quashing Online Dissent: Anti-Extremism Laws Put Digital Rights as Risk in Belarus https://www.article19.org/resources/belarus-anti-extremism-laws-put-digital-rights-at-risk/ (2025) page 8

[14] Human Constanta, From Streets to Screens: Digital Repression in Belarus (2025) https://humanconstanta.org/en/strees-screens-en/ page 18

[15] ARTICLE 19 and Human Constanta, Quashing Online Dissent: Anti-Extremism Laws Put Digital Rights as Risk in Belarus https://www.article19.org/resources/belarus-anti-extremism-laws-put-digital-rights-at-risk/ (2025) page 9

The practices described above demonstrate how freedom of assembly and association can be effectively hindered without the adoption of explicit prohibitions on assembly or association as such. The designation of online communities and spaces as "extremist" turns digital participation into criminal conduct, with the underlying legal framework put together to disrupt the formation, sustainment, and coordination of collective initiatives at early stages. For the purposes of Article 22, this illustrates how criminalising digital and informal forms of participation erases the substance of the right itself, and underscores the need for the Committee's guidance to address such covert legal frameworks.

3. Transnational digital repression as interference with freedom of assembly and association

Interference with freedom of assembly and association does not stop at a state's territorial borders. As increasingly documented by global civil society actors, repression now follows those fleeing their home countries and settling elsewhere, as governments extend their reach to target critics beyond their physical reach. Those dynamics of modern transnational repression directly affect the conditions for association and organising in digital spaces, which communities living in exile rely on even more heavily, as their collective action largely depends on online platforms and cross-border connections. This has direct implications for the enjoyment of Article 22 rights.

Association Human Constanta Int. documents that the toolbox of digital transnational repression includes practices such as surveillance, phishing and other lures, online harassment, DDoS attacks, and other forms of hybrid digital intrusion. Such measures do not operate in isolation but are often used at once to reinforce each other, leaving people abroad under constant, sustained pressure.[16] As such, personal data extracted through a phishing attack may later be used to launch smear campaigns, and information obtained through surveillance or digital traps can expose not just the victims but their entire networks.[17] These patterns demonstrate that digital cross-border targeting of one individual can disrupt whole communities, producing chilling effects that hinder the exercise of freedom of association abroad.

This is particularly evident in how domestic legal labels are increasingly projected across borders, producing tangible effects even outside a state's territorial jurisdiction. Belarusian anti-extremism frameworks, described above, do not remain confined to domestic proceedings: they also follow dissidents abroad, resurfacing at border crossings, consular offices, or in absentia court proceedings.[18] Digital tools are central in enabling such cross-border projection of repression. They allow authorities to turn mobilisation, be it physical or digital in nature, into a point of vulnerability. Association Human Constanta Int. documents that state-linked Telegram channels in Belarus regularly spread hostile discourse about dissidents involved in

[16] Human Constanta, Repression Without Borders: Transnational Authoritarianism in the Digital Age (2025) https://humanconstanta.org/en/repression-without-borders-transnational-authoritarianism-in-the-digital-age/ page 7
[17] Ibid.
[18] Ibid., page 24

political activity abroad, often coupled with threats of criminal charges, home searches, intimidation of family members, or property seizures. Those who participated in Belarusian rallies in Warsaw, for example, were publicly targeted in this manner,[19] with one campaign publishing a list of 365 demonstrators by name and explicitly promising reprisals.[20] These practices are further reinforced through what Association Human Constanta Int. describes as "legal-tech hybrid" measures, including the use of consular services, identity documents, and administrative procedures as further leverage against exiled individuals. Taken together, these dynamics enable states to put pressure on associational life even beyond their borders, exporting repression, and effectively placing exiled communities in a position of ongoing insecurity even within democratic host states.[21]

These findings show that freedom of association in the digital age cannot be assessed solely within territorial boundaries. Where states use digital tools to monitor, intimidate, and penalise association across borders, Article 22 must be interpreted as encompassing obligations to prevent and address transnational targeting, reflecting the realities of cross-border digital civic space and the vulnerability of communities in exile.

[19] 'Силовики угрожают «уголовными делами, обысками и арестами имущества» также участникам акций в Варшаве 9-10 августа' ['Security forces threaten "criminal cases, searches and property arrests" also to participants of rallies in Warsaw, 9-10 August'] Zerkalo.io (5 August 2025) https://news.zerkalo.io/life/105544.html

[20] 'СК угрожает 365 участникам зарубежных акций, прошедших 26 января. Завели уголовное дело и будут искать имущество в Беларуси' ['The Investigative Committee threatens 365 participants of foreign rallies held on 26 January. A criminal case has been opened and they will search for property in Belarus'] Zerkalo.io (27 January 2025) https://news.zerkalo.io/life/89645.html?c

[21] Human Constanta, Repression Without Borders: Transnational Authoritarianism in the Digital Age (2025) https://humanconstanta.org/en/repression-without-borders-transnational-authoritarianism-in-the-digital-age/