Organization for Security and Co-operation in Europe
Office of the Representative on Freedom of the Media

SPECIAL REPORT ON THE SEVENTH ROUNDTABLE OF THE SAFETY OF JOURNALISTS PROJECT

DIGITAL SAFETY

2 NOVEMBER 2023

Foreword

In December 2018, the Ministerial Council of the Organization for Security and Co-operation in Europe (OSCE) adopted Decision 3/18 on the Safety of Journalists. In this landmark document, the participating States committed themselves to improve the safety of journalists on different inter-related aspects, including physical, legal, economic and online threats and attacks, with a special focus on the distinct risks faced by women journalists. In 2022, the year in which we marked the 25th anniversary of the Mandate of the OSCE Representative on Freedom of the Media (RFoM), the current RFoM Teresa Ribeiro decided to devote special attention to the topic of safety of journalists and launched a new project.

The project consists of seven roundtables, each covering another aspect of the topic of safety of journalists: (1) data collection, analysis and reporting on attacks and violence against journalists and promotion of journalistic work; (2) secure working conditions; (3) safety of journalists in conflict situations; (4) intersectional perspectives; (5) legal harassment; (6) police prevention and fight against impunity, and (7) digital safety.

The seventh and last roundtable took place on 13 September 2023, with the participation of six distinguished experts: Ms. Saba Ashraf, Senior Legal Officer, Media Defence; Ms. Felicia Anthonio, #KeepItOn Campaign Manager; Ms. Elisa Lindinger, Superr Lab; Ms. Brandi Geurkink, Senior Policy Fellow, Mozilla; Ms. Dana Buralkiyeva, Erkindik Qanaty Foundation; Mr. Rustam Muhamedov, Digital Rights Expert.

This report is a reflection of the contributions and discussions from the seventh roundtable, with additional information from supporting material and literature. It does not suggest to be complete in its coverage, but rather aims to provide guidance to the participating States in their endeavour to further journalists' safety.

I. Introduction

"When it is safe to practice journalism, society benefits."

Media can only fulfil their essential role in democratic society when journalists can work without fear of attacks or violence. This has always been an issue of concern. However, with the rise of digital platforms, ensuring that journalists can work in a safe environment has become even more complex. There are new vulnerabilities in all parts of the digital realm – albeit clear that these new digital dimensions are not separate from existing threats to journalists in the physical world. More than ever, journalists use digital technologies and rely on online platforms to distribute their content to the public and to interact with their sources and audiences. At the same time, social media platforms that allow for such user interaction, next to wikis for collaborative storing, creating and editing of content, or content hosting services also present significant security concerns. As new technologies become readily available, the need to strike a balance between safety and privacy in the digital world and freedom of expression is key.

Journalists are routinely subjected to online harassment and attacks, especially when their coverage concerns particularly sensitive or controversial topics, or in the context of elections. Such types of attack are sometimes organized, co-ordinated and orchestrated, most commonly in the form of smear and disinformation campaigns. Already in 2019, a report published by the RFoM and the International Press Institute showed that coverage of refugees and migration issues was a trigger for unrelenting online violence against journalists in many OSCE participating States. This research also showed the detrimental impact of such online attacks on journalists' mental health, and their ability to work without fear of retaliation within society.

This issue is of particular concern for female journalists, where cyber violence is oftentimes accompanied by hateful and sexist messages of a chauvinist, misogynistic nature, disdain and humiliation. A study by UNESCO and the International Center for Journalists confirmed that almost three-quarters of women journalists experience online abuse, whereas 30% of women journalists said they self-censor on social media after being targeted.

It is clear that a lack of digital safety poses a significant risk to the free flow of information, media freedom and pluralism – which are at the core of our democratic societies. Concerted action is needed to minimize the potential harm to journalists and other media professionals, with an emphasis on women journalists and those from minority backgrounds.

II. Digital safety risks and access to information

Digital safety includes the risk of becoming targets of hacking, unlawful or arbitrary surveillance, interception of communication or online harassment, intimidation or other forms of violence, which can deter journalists and other media actors from continuing their work or lead to self-censorship. Several participating States have undertaken initiatives to counter these risks and adhere to relevant OSCE commitments related to digital safety, including those in the 2018 OSCE Milan Decision on Safety of Journalists.

However, continuous technological developments, including generative AI (a type of AI technology that can generate content such as images, texts, videos and other media in response to prompts), new digital surveillance techniques, and an increase in online threats require States to find new effective measures to ensure journalists' digital safety.

To effectively mitigate the risks of online violence against journalists, the experts at the roundtable stressed the need to direct efforts towards the implementation of legislation that, on the one hand, aims to protect the digital space against the spread of illegal content, while at the same time ensuring the protection of users' fundamental rights.

In this light, they referred to the recently adopted Digital Services Act (DSA) as a good example in this direction, stressing the need for platforms to be more transparent regarding the way they moderate and curate content, and to ensure access to data for independent research. The experts emphasized that next to transparency it is equally important to establish accountability mechanisms for platforms' role in disseminating illegal content. As online platforms deploy artificial intelligence (AI) to support the curation and dissemination of content as well as to filter and take down illegal content, AI-led processes provide the basis for how society today interacts with information online. Noting that content governance should prevent the algorithmic amplification of content that is violent or harmful, the experts stated that platforms need to act more effectively and in a human rights-based manner in this regard. *In order to provide guidance to States on free speech safeguards in the context of online platforms and content governance, the RFoM last year published policy recommendations putting a spotlight on AI and freedom of expression (SAIFE Policy Manual).*

Moreover, the experts explained that AI tools used to produce content affect journalists in their work, with technologies like generative AI raising questions concerning the truthfulness and accuracy of content production. For instance, generative AI can be used to create and spread disinformation that convincingly mimics real media news content. This has the potential to undermine trust in the media by making it increasingly difficult to discern between authentic

and fabricated content. Distrust and anti-media sentiments are also interlinked with online attacks against journalists.

As stated above, women journalists face additional threats of online violence because of their work and because of their gender. Gender-based online attacks aim to deny women journalists a public voice, leading to their self-censorship or their retreating from the public sphere, hence depriving society of diverse, pluralistic information and inclusive public debates in a democratic society. As a counter measure, experts underscored the urgent need for guiding principles and an intersectional approach to digital policy and regulations, including to avoid that the online violence moves to the offline sphere. In an effort to address the escalation of this dangerous trend, the RFoM has recently launched the "OSCE Guidelines for monitoring online violence against female journalists" based on 15-research informed indicators.

Another major threat to journalists' digital safety, experts pointed out, is the growing misuse of digital surveillance technology and spyware. Journalists rely on safe and secure digital communications, not only for their own privacy and personal safety, but also to secure the confidentiality and protection of their sources. Digital surveillance technologies are diverse and can be very intrusive, ranging from location tracking to deep packet inspection, facial recognition and mass monitoring.

Although in very specific circumstances digital surveillance can have legitimate uses, it can have a negative impact on media's ability to conduct its work safely without undue interference. In a recent Communiqué on the Use of Digital Surveillance Technology on Journalists, the RFoM elaborates how surveillance negatively affects journalism and communication between individuals, limiting their ability to access opposing, critical, or dissenting information, to investigate critical issues and disseminate information freely and securely.

III. The way forward: a safe information space

One of the recommendations mentioned during the roundtable entailed the need to co-operate with tech companies – to ensure that their platforms are safe for users to access diverse, accurate, and public interest information, and that illegal content is being taken down effectively, with due consideration to the fundamental right to freedom of expression.

Another point raised was the need to avoid internet shutdowns: In 2022, 197 such incidents were documented globally. Without an open and accessible internet, the general public as well as journalists cannot fully exercise their right to freedom of expression, which includes the

right to access information. While certain restrictions can be justified, they need to be based on a clear legal basis for certain specified purposes, such as the protection of national security, public order (ordre public), or public health, and must be proportional and necessary in a democratic society. Experts underlined that, in reality, internet shutdowns are frequently imposed for other purposes, without justification, including during elections or protests. In such cases, and when failing to meet the criteria for restricting rights outlined in the International Covenant on Civil and Political Rights (ICCPR), including Articles 19 (freedom of expression), 21 (peaceful assembly), and 22 (association), shutdowns contravene human rights law.

Moreover, the experts agreed that the gender-aspect should be acknowledged, including in digital safety trainings. As social media companies, news organisations and States are struggling to respond effectively to online violence against journalists, there is an urgent need for more effective legislative responses, in full compliance with international standards on freedom of expression and privacy. This includes regulatory frameworks aimed at delivering more transparency and accountability, providing effective mechanisms for independent oversight and due process – all of which should be developed with a human-rights centric approach, and applicable to the digital realm.

All experts to the roundtable agreed that media and digital literacy play a crucial role in improving digital safety. In order to make informed decisions, people need the ability to access, analyse and engage in critical thinking about the range of information they obtain in the online sphere. The inclusion of media and digital literacy in formal education can be a bridge across digital divides and can provide the necessary instruments to identify higher quality content in media.