

**Contribution to the discussion on  
Security of Journalists on Social Platforms**

**Shushan Doydoyan, FOICA**

11/03/2025

The current information and communication space are facing an unprecedented decline in public trust, marked by power asymmetries between tech companies and the rest of society, alongside a growing reliance on social media as a primary source of information. Media and civil society have never faced such challenging times of the undermined public trust, growing threats to journalists, cutting of the financial means and the loss of sustainability. Journalists today face unprecedented challenges. The rise of deepfakes, manipulated content, and AI-driven falsehoods help disinformation spreads rapidly, weaken accountability mechanisms, and journalists are increasingly subjected to online harassment and coordinated attacks.

**Addressing these issues requires a coordinated effort—one that bridges the media, open government and information integrity communities.**

The recent research of the Forum on Information and Democracy shows how data is being monopolized by big tech companies. There is a wide variety of corporate data practices that contribute to unfairness. Most involve two main types of monopolistic activity: **monopolization of user data** (i.e., all the data produced about us), which makes money for companies by converting information seekers into 'information products' offered for sale to advertisers; and **monopolization of knowledge** (i.e., data organized as usable insight) and information that makes money by converting data resources (including public data resources) into private assets. These pervasive forms of datafication give rise to numerous forms of digital dependency and injustice. The monopolization of data (i.e., data organized as usable insight or knowledge) occurs by converting data resources (including public data resources) into private assets. People are surveilled for data and the big tech companies do not limit their data collection to the data they extract. They buy or license data from other companies (and acquire data analytics companies) that gather or process data.

**Privacy issues** of individual journalists are also among the most challenging ones. Journalists as members of our modern societies are creating a digital record of every step of their lives. Corporations track, record and analyze our online activities to predict and shape consumers' behavior. This is the data that companies such as Google, X (formerly Twitter), Meta and Microsoft collect when individuals use their apps and

services to create, find, consume and share information. They collect everything about our lives – when we take public transport, where and what we eat, what we ordered, when we rent an apartment, when we go to the doctor, etc. The more companies achieve control of data, the more difficult it is to enact structural and systemic changes. Big tech companies are creating de facto data governance frameworks that are inconsistent with data justice.

**Here are some solutions I find important for addressing the current challenges.**

**Solution 1. – We cannot do everything all at once, so we need to prioritize.** I think a useful starting point is this comparative legal and regulatory discussion, and that it would be useful to put together a shared vision on the legal enabling environment for information integrity and resilience that accounts for media freedom, digital rights, and AI.

## **Solution 2. The role of education**

**2.1 Media and AI Literacy** – this has a central role for equipping journalists with the skills to combat harmful information. Moreover, I think that media and AI literacy should become an integral part of the education system. Like studying math, every child in the school has a right to gain media literacy and AI competences. As deepfake technology, and new forms of digital manipulation evolve because of AI tools, Governments and civil society should collaborate to integrate fact-checking and AI skills into general education system to empower citizens and future journalists against manipulative narratives.

**2.2 The need of a reform of the journalism education system** - As the challenge we face is comprehensive, the addressing strategies should also be as holistic as possible. Reforming journalistic education is becoming a must. The curricula at university journalism departments remained in the late 20th century, while technological developments have rapidly transformed the media landscape. Digital journalism, artificial intelligence, and data-driven reporting, data security, data protection principles should become integral to the profession, yet many academic programs fail to equip journalism students with the necessary skills to navigate these changes. Journalism education must integrate modern tools, ethical considerations for digital reporting, and hands-on training in new media technologies, ensuring that future journalists are prepared for the evolving demands of the industry.

**Solution 3. European Media Freedom Act and the Digital Services Act can be used as templates for regulation in countries outside the European Union to tackle this problems.** While these frameworks can serve as valuable references, particularly for nations with limited human and economic resources, their adoption requires careful consideration of

local challenges. Regulations must be adapted to align with national legal frameworks, economic conditions, and institutional capacities while ensuring compliance with human rights standards, which may differ from those in the EU.

**Solution 4. – Fact checking groups** should be strengthened and equipped with necessary toolkit allowing them to conduct **detecting, analyzing of mis-disinformation**. Governments and international organizations, including the OSCE, should provide funding and institutional backing to fact-checking initiatives, ensuring their independence and sustainability. Without effective fact-checking, social platforms become instruments of manipulation, and journalists become victims of orchestrated misinformation campaigns. **In addition, data security experts should be supported also to ensure strong protection and prevention of violations of journalists’ digital rights.**

**Solution 5. - Initiate numerous and consistent legal appeal precedents** -Civil society may launch lawsuits in the national and international courts to file against big tech companies and those actors spreading disinformation to recognize the violation of human rights and demand appropriate remedies. Moreover, data protection authorities with their strong powers as well as the European Data Protection Board, the European Data Protection Supervisor should be widely engaged in the appeal processes as online surveillance and spying of journalists greatly affects the data protection rights of journalists.

**Solution 6 - The next key area which needs our collaborative efforts is financial instability of the media, in light of the sudden freeze of USAID funding.** This has sent shockwaves through independent newsrooms across the world. Many smaller outlets face closure, while larger ones stay for financial strain. In the meantime, the decline in independent news outlets will lead to an increase in disinformation, as the reliable sources for information will be decreased. Moreover, autocratic leaders in some countries may seize the moment to tighten the media control. We should join and mobilize our efforts to find quick and viable solutions (including engaging European institutions and private donors) to fill the sudden gap and prevent long-term damage to media pluralism.

**Solution 7 - It is more than obvious that no single actor can address the current challenges.** Governments, civil society, media, private sector and technology platforms must work together to co-create solutions that ensure free, independent, and transparent media ecosystem. The OSCE may partner with Open Government Partnership, Forum on Information and Democracy to closely work with the governments for **creating a more favorable environment for the media and civil society by launching diversified incentives to ensure financial sustainability and providing technical assistance in this new reality.** And only through

collaboration we can ensure that governments uphold their commitments to transparency, independent media, and access to information.

**Solution 8 – The role of states** Watching how the big tech companies spin and distort around Trump, shows that the state is strong and capable of restraining their work and appetite. Despite their influence, the state's ability to control or counteract the big tech's actions. This could include regulatory measures, legal actions, or political interventions that limit Big Tech's dominance, monopolization and data injustice. The OSCE should encourage member states to implement balanced regulatory measures that promote transparency, prevent undue influence, and uphold freedom of expression. Stronger laws criminalizing cyber threats against journalists are also needed. The states also have great role to end of impunity and place sanction on the perpetrators.

### **Solution 10 - Strengthening Responsibility Mechanisms**

We need clear, enforceable policies that make platforms legally and morally responsible for mitigating harm. Transparency in content moderation decisions must be improved, and there must be independent oversight mechanisms to ensure platforms are fulfilling their obligations. Furthermore, collaboration between law enforcement and digital rights organizations should be enhanced to track and address serious threats against journalists. **Real threats require real consequences, and only through a strengthened responsibility framework can we deter bad actors from using social platforms as weapons against journalists.**

**Final solution** - I propose establishing an OSCE Security Fund for media professionals under attack online. This would provide direct financial and legal assistance to journalists facing targeted harassment and cyberattacks. This Fund should be accessible to freelance journalists, investigative reporters, and media workers who face disproportionate risks online. The OSCE, in collaboration with civil society and tech companies, must take the lead in making this initiative a reality.

I appreciate your time and attention, and I am happy to answer any questions you may have. Thank you!