Enhancing Digital Civic Space through OGP

Addressing Harmful Information Online

Disinformation, online gender-based violence (GBV), and hate speech greatly impact online civic space and democratic processes. Disinformation increases polarization, influences elections, and fuels violence. Meanwhile, online GBV and hate speech discourage and prevent women, girls, LGBTQIA+ individuals, ethnic and religious minorities, and other communities from actively participating online. And yet, it is extremely difficult to accurately identify disinformation, hate speech, or misleading content. Some government responses to these harms have disproportionately curtailed freedom of expression. Governments should take steps to promote healthy and safe information ecosystems online while also protecting the exercise of online civic freedoms.

Caption: Educational programs is one way to address harmful information online, especially as children interact with technology both in and out of school. Sarah Pacayra, a civic monitor for public schools in Manila (Philippines) is pictured with her two children, working with a laptop. Photo by OGP.

ICNL
INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW

Open Government Partnership

Open government thrives when people can freely access government information and services, share opinions and information among themselves and with their leaders, and act individually and collectively to influence decision-making and hold governments accountable—both online and offline. While the internet and digital tools can play an important role in empowering the public, more action is needed to ensure that these spaces enable robust civic action and participation. This series highlights the recommendations from the International Centre for Not-for-Profit Law's *Enhancing Digital Civic Space through the OGP Process*.

Recommended Open Government Commitments

- **Revise relevant laws to address online GBV.** These include revising relevant criminal statutes to authorize the investigation and prosecution of cyberstalking, online sexual harassment, online posts of non-consensual sexual images, and other forms of tech-facilitated gender-based violence. These revisions should avoid the use of vague or broad language that could include legitimate forms of expression, and criminal investigations and prosecutions pursuant to these provisions should follow appropriate due process standards. Law enforcement should be equipped to investigate these incidents using trauma-informed practices.
- **Repeal or amend vague laws targeting harmful information online** if the laws do not precisely identify a specific harm or are not narrowly tailored to address the harm. Vague and disproportionate laws that target online speech violate a State's human rights obligations and lead to censorship of otherwise protected speech. Engage in a multi-stakeholder, consultative process to ensure any legal measures that restrict online speech are based on the State's human rights and constitutional obligations and high-quality research about the harm, its impacts, and its pervasiveness.
- **Enact targeted measures to increase transparency on online platforms** to counter disinformation, such as "anti-bot" laws requiring automated online accounts to reveal their identities to users under certain circumstances, or laws mandating transparency about the origins of online advertising or sponsored content.
- **Invest in non-legal measures to counter harmful online content.** This includes media literacy programs, curriculum development for schools on how to critically assess information and news, and support to women and vulnerable communities that are at greater risk of being targets for harmful content online.
- **Publish regular reports on content takedown orders and requests** issued or lodged by public authorities, including the number and type of requests and their rationale.

- **Convene diverse stakeholders on creating healthy online ecosystems.** These stakeholders should include digital platforms and other technology companies, civil society, academic experts, and representatives of communities frequently targeted by abusive online communications—to share information, identify research questions, and explore practices that can contribute to the development of healthy and safe online information ecosystems. Governments should also encourage platforms and other technology companies to invest in capacity building, reporting, and dialogue mechanisms that can foster the free exchange of information with civil society and the public, with the aim of promoting safe navigation of platforms and reducing the incidence of harmful information online.
- **Engage with the public on legal protections for children online** to review existing laws or bills related to protecting children online. Such engagement should help ensure that such laws are precise and narrowly tailored to protect children from online harms while avoiding infringement upon children's right to freedom of expression. Governments should further invest in non-legal measures that engage and educate children and parents about risks online and mitigation measures they can take.

Positive Examples from OGP Action Plans and Beyond

- The state of **São Paulo** in Brazil has offered media literacy as an elective class for middle schoolers. The class includes lessons on how to responsibly use the internet and recognize trustworthy information.
- The Code of Practice on Disinformation is a voluntary initiative, undertaken based on guidance from the **European Commission**, under which 34 private sector signatories committed to demonetizing disinformation, ensuring the transparency of political advertising, empowering users, enhancing the cooperation with fact-checkers, and providing researchers with better access to data.
- **Finland** developed a media literacy module that helps school-age individuals identify and distinguish amongst misinformation, disinformation, and mal-information.
- **France** committed to hosting multi-stakeholder dialogues with civil society and research institutions, to identify research priorities and existing tools, resources, and techniques to monitor and counter misinformation and disinformation. The government also committed to discussing proposed solutions to counter the dissemination of misinformation and disinformation.
- The **Netherlands** committed to introducing greater transparency into how political parties are funded while making online election campaigns and political advertisements more transparent, as a means of combatting disinformation.

- The state of **California** in the United States has enacted an "anti-bot law" that requires that bots (or the person controlling them) reveal their "artificial identity" when they are used to sell a product or influence a voter. The law defines a "bot" as "an automated online account where all or substantially all of the actions or posts of that account are not the result of a person."
- In April 2019, six of **Uruguay**'s political parties signed an Ethical Pact Against Disinformation that pledged "not to generate or promote false news or disinformation campaigns to the detriment of political adversaries." The Uruguayan Press Association proposed the pact as one of three prongs to combat disinformation, alongside fact-checking training sessions and training for media professionals.

Successfully addressing the threats posed by disinformation, online GBV and hate speech to democratic discourse requires carefully calibrated, rights-based, and multi-stakeholder approaches to regulation of online expression. Governments, working together with key actors like civil society and tech companies, can leverage open government principles to advance these approaches and protect democratic freedoms both online and off.