The Enabling Digital Environment for Civil Society: Global Trends in Repression and Resistance — an EU SEE Perspective

EU SEE
SUPPORTING
AN ENABLING ENVIRONMENT
FOR CIVIL SOCIETY

Introduction

The online world mirrors the offline wherever there is democratic backsliding or growing authoritarianism. In other words, governments are using digital technologies and co-opting regulatory frameworks that govern digital technologies as an extension of other tactics to undermine the enabling environment for civil society and democratic freedoms.

This is also reflected in government inaction where non-governmental actors use digital technologies to attack civil society actors, in particular vulnerable groups such as women human rights defenders. Furthermore, tech companies, including social media companies and telecoms operators are not only failing to sufficiently implement their roles and responsibilities in relation to protecting user rights, but they are also actively engaging in anti-competitive practices that consolidate and strengthen their political and economic power.[1] This deterioration is amplified by a global funding squeeze, with shrinking aid budgets and compliance burdens that are weakening civil society organisations' (CSOs) capacities to respond.

At the same time, the internet has become an indispensable means of exercising the fundamental freedoms of expression, association, and assembly. Globally, civil society is resisting government tactics through the use of the judicial systems and strategic litigation, advocacy at regional and international mechanisms, and coordinated engagement in national policy opportunities, such as those relating to access to information legislation, constitutional reform, or expanding access to the internet. They are also themselves using digital technologies to promote accountability, disseminate counter-narratives online, coordinate broader advocacy campaigns, protect vulnerable groups from surveillance, provide accurate information in the face of disinformation, and address digital divides.

This policy brief first outlines three main global trends related to the enabling digital environment for civil society. It then describes the tactics that civil society is using to address this decline. Finally, it ends with recommendations for different stakeholder groups.

1 Oxfam America, "The Rise of the Tech Oligarchy: Part I Degradation of the Digital Civic Space", *Politics of Poverty*, October 9, 2025; Amnesty International, *Breaking up with Big Tech: A human rights-based argument for tackling Big Tech's market power*, 28 August 2025.

Definitions and methodology

The EU System for an Enabling Environment for Civil Society (EU SEE) is a consortium of international civil society organisations and network members in 86 countries. The partnership implements an Early Warning and Monitoring Mechanism to document changes and shed light on critical trends in the enabling environment for civil society. The analysis in this brief is drawn from an in-depth review of the data most recently available from the EU SEE Early Warning and Monitoring Mechanism. This is complemented by a review of other up-to-date research and literature related to the enabling digital environment, including recent reports from Freedom on the Net,[2] CIVICUS,[3] and the Global Network for Social Justice and Digital Resilience.[4]

Across the world, data collected from network members of the EU SEE project shows that there are mounting challenges to the enabling digital environment for civil society.

An enabling environment is defined as "the combination of laws, rules and social attitudes that support and promote the work of civil society. Within such an environment, civil society can engage in political and public life without fear of reprisals, openly express its views, and actively participate in shaping its context", while a country's digital enabling environment should enable civil society actors "to participate securely and freely online, including by accessing information without censorship, internet shutdowns, or surveillance, and through protection from cyberattacks and disinformation campaigns".[5]

1) The effects of global digital trends on the enabling environment for civil society

The three trends outlined below are linked: The government tactics described under trend 1 are tactics of repression, and are reflected in the legal infrastructure that is underpinned by securitised framings of digital technologies (trend 2), while efforts to implement stronger policies, frameworks, and standards (trend 3) that would promote enabling digital environments and would counteract trends 1 and 2 continue to lag behind.

---

2 Allie Funk, Kian Vesteinsson & Grant Baker, "Freedom on the Net 2024: The Struggle for Trust Online", Freedom House, 16 October 2024.

3 CIVICUS, "Analysis of the Digital Democracy Ecosystem: Synthesis Report", 2025.

4 Digital Resilience Network, "Pulse 2025: A Response to the Funding Crisis from a Global Majority Perspective", 21 August 2025.

5 EU SEE, "EU System for an Enabling Environment for Civil Society".

Trend 1: Governments deploy a similar range of digital tactics to undermine the enabling environment for civil society

Across the five regions (the Americas, Africa, the Asia-Pacific, the Middle East, and Central Asia) covered by the EU SEE network, governments are using similar tactics to control online speech that is dissenting or critical, and are using digital surveillance to crack down on civil society actors. These tactics broadly fall into three categories, which also overlap:

Online surveillance

Governments are using a range of tools to surveil civil society actors, including human rights defenders and journalists. These include the use of sophisticated spyware, the surveillance of messaging apps and social media, the use of biometric technologies (such as facial recognition), and the hacking of activists' social media accounts. Examples of these tactics include:

- **Mexico,** where the military is one of the world's largest users of spyware, used against those investigating corruption and human rights abuses;[6]
- **India,** where spyware has also been used against human rights defenders and journalists;[7]
- **Peru,** where journalists have been intimidated and harassed via direct messages on messaging apps or social media accounts;[8] and
- **Argentina,** where "cyber patrol reforms" to federal police statutes have expanded surveillance of social networks.[9]

Content driven threats and intimidation campaigns

The use of bots and of disinformation campaigns on social media (including those that employ generative AI) by political actors to peddle narratives that undermine the legitimacy of civil society actors, e.g., by portraying them as "foreign agents". Examples of this include:

- **Paraguay,** where digital media and social media are used to create or reinforce negative narratives about civil society actors, e.g., that they're not accountable, that they are corrupt,

---

6 Freedom House, "Mexico: Freedom on the Net 2024," 31 May 2024.

7 EUSEE, "India Enabling Environment Baseline Snapshot", 17 July 2025; Freedom House, "India: Freedom on the Net 2024 Country Report," 1 June 2023.

8 EUSEE, "Deterioration of Press Freedom in Peru Amid Recent Acts of Intimidation against Journalists," *EUSoutheast Europe Alert (EUSEE),* 6 August 2025.

9 EUSEE, "CyberPatrol: Reforms to Federal Police Statutes Threaten Privacy and Freedom of Expression," 29 July 2025.

and/or that they receive foreign money to promote a "global" agenda that undermines the country's sovereignty;[10]

- **Tajikistan,** where civil society activists are targeted by online harassment and pro-government troll factories that flood social media and online media comment sections;[11]
- **Nigeria,** where the government has orchestrated disinformation campaigns via trolls who have discounted witness testimonies of police brutality during protests;[12]
- **Chile,** where there has been an increase in online harassment and smear campaigns targeting journalists, human rights defenders, and activists;[13] and
- **Cambodia,** where the portrayal of civil society actors as foreign agents is disseminated through social media .[14]

Censorship via blocking, distributed denial-of-service (DDoS) attacks, social media bans, shutdowns, and online content takedown orders

Governments are using "technical measures", such as DNS and IP blocking and DDOS attacks, as well as serving online content takedown orders to social media platforms (see trend 2, below) to undermine free expression by controlling and censoring content. Examples of this include:

- **Jordan,** where at least 12 independent news websites were blocked in 2025 for "spreading media poison", in a move that raised widespread condemnation by media freedom groups for disregarding due process;[15]
- **Indonesia,** where news websites have been the subject of DDoS attacks;[16]
- **Nepal,** where major messaging and social media apps have been banned;[17]

---

10 Juliana Quintana & Romina Cáceres. "De la transparencia a la cruzada 'antiwoke': las narrativas que las milicias del cartismo instalaron contra las ONG." *El Surtidor,* 29 November 2024.

11 EUSEE, "Tajikistan EE Baseline Snapshot", 17 July 2025.

12 EUSEE, "Nigeria EE Baseline Snapshot", 31 January 2025; Lawal, Shola. "Nigerian Trolls Defend the Government and Gaslight Victims." 15 July 2022.

13 EUSEE, "Chile Country Focus Report", 4 August 2025.

14 EUSEE, "Cambodia EE Baseline Snapshot", 18 February 2025.

15 EUSEE, "News websites blocked in Jordan", 7 July 2025.

16 EUSEE, "Increasing threats against journalists following the revision of Indonesia's National Armed Forces Law", 16 April 2025)

17 Bhadra Sharma, "Nepal Bans 26 Social Media Platforms, Including Facebook and YouTube", *The New York Times,* 7 September 2025.

- **India,** the global leader in internet shutdowns, where these are usually justified to maintain "law and order, restrict protests, prevent cheating during school exams, and prevent the spread of disinformation";[18] and
- **Pakistan,** where the government has installed a national firewall that can track social media content and block it.[19]

Within this trend, there are other cross-cutting similarities across the countries and regions studied:

- **The use of the above tactics impacts vulnerable groups disproportionately:** The impact of these tactics on vulnerable groups illustrates how the online world mirrors the offline. Groups who are already marginalised in physical spaces such as women, LGBTQI communities, and land rights or environmental defenders are also vulnerable and targeted online. For example, the use of bots, deepfakes, and doxxing impact women and LGBTQI communities in particular.[20] In South Africa, online civic space has become increasingly hostile, with rising digital harassment targeting human rights defenders and the LGBTQI community,[21] and in Zambia, "women politicians, in particular, have faced cyberbullying and online sexual harassment during election campaigns". Environmental and land rights defenders have also been found to be the targets of digital violence where they use digital platforms to challenge corporate interests.[22]
- **Elections or politically sensitive periods result in the increased use of the above tactics**: According to the EU SEE project data, in Uganda, there has been an increase in the online targeting of activists and in censorship during elections,[23] a trend that has been documented by Freedom on the Net in other countries, such as Bangladesh, Cambodia, Pakistan, Venezuela, and Zimbabwe,[24] as well as in a recent report by the UN Special Rapporteur on Freedom of Expression concerning elections in the digital age.[25]

---

18 EUSEE, "India EE Baseline Snapshot" 17 July (2025).

19 EUSEE, "Pakistan EE Baseline Snapshot" 11 March 2025. https://eusee.hivos.org/document/pakistan-ee-baseline-snapshot/

20 UN Women, "FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women", 10 February 2025.

21 EUSEE, "South Africa EE Baseline Snapshot", 21 August 2025.

22 Global Witness, "Toxic Platforms, Broken Planet", 16 July 2025.

23 EU SEE, "Government Plans to Introduce a Social Media Monitoring Tool That Could Threaten Freedom of Expression." *EU SEE,* 19 July 2025; EUSEE, "Burundi EE Baseline Snapshot", 31 January 2025.

24 Freedom House, "Freedom on the Net 2024".

25 "A/HRC/59/50 Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. Freedom of Expression and Elections in the Digital Age: Report of the Special Rapporteur on the Promotion and Protection of the Right to Free", 11 June 2025.

- **The use of digital tools exacerbates other means used to repress the enabling environment:** These include increasingly restrictive laws on accessing foreign funding and the use of overly complex means of accessing registration online under the guise of "addressing foreign agent influence."[26]

Trend 2: The digital environment is increasingly regulated in way that undermines the enabling environment for civil society.

The governance and regulation of digital technology is necessary. For example, cybersecurity and data protection legislation can strengthen cybersecurity systems and protect civil society from data breaches and cyberattacks, while regulation to promote community networks can enable civil society to access information freely online.[27] Across the regions surveyed, however, regulation is instead being used to undermine the enabling environment.

This trend reflects the broader securitisation of digital governance, where a widening range of online activity is treated as a potential national security threat. In some cases, this includes the mislabelling of legitimate expression – particularly criticism of government or powerful actors – as disinformation, defamation, or "fake news". Depending on how these terms are defined in law and policy, such framing can be used to justify disproportionate measures that restrict human rights, including the freedoms of expression, association, assembly, and privacy. The EU SEE project has previously drawn attention to this issue,[28] and worked with other stakeholders to raise awareness of this at the 2025 edition of the Internet Governance Forum, in Norway.[29]

---

26 CIVICUS, "Analysis of the Digital Democracy Ecosystem, Digital Democracy Initiative", *op. cit.,* note 3.

27 Carlos Rey-Moreno, "Community network regulation around the world", APC, 15 December 2023.

28 Clarisse Sih, Bibbi Abruzzini & Vitoria Dacal, "Cyberlaws and Collective Rights: What Are the New Models of Digital Governance?" *EU SEE,* 25 June 2025.

29 IGF2025, "Cyber laws and civic space: GN-GS advocacy strategies – WS 4, Day 2", (2025),

This weaponisation and securitisation of regulation comes in two forms:

- **New legislation relating to cybersecurity and cybercrime.** Recent examples sourced through the EU SEE project include:

  - **Sierra Leone**: Since it was adopted in 2021, the country's Cybersecurity and Cybercrime Act has been used to harass and intimidate human rights defenders and journalists,[30] abusing its vague provisions and through selective enforcement. There are also concerns that the country's recently adopted Counter Terrorism Act (2025) will be abused to silence journalists work online, as a result of unclear definitions and disproportionate penalties;[31]
  - **Eswatini:** The Computer Crime and Cybercrime Act lacks adequate safeguards for the right to freedom of expression, raising concerns that it could be used to criminalise legitimate speech and silence critics;[32]
  - **Kenya:** The recently introduced Computer Misuse and Cybercrimes (Amendment Bill) 2024 contravenes human rights standards in several ways, including by imposing disproportionate penalties and through the expansion of government powers without judicial oversight;[33]
  - **Nigeria:** Civil society organisations in Nigeria have filed a lawsuit against the Nigerian government over "the repressive use of the Cybercrimes (Amendment) Act 2024 to criminalise legitimate expression and violate the human rights of Nigerians, including activists, journalists, bloggers, and social media users."[34]
  - **Jordan:** Within a year of its passing, civil society had documented how the Jordanian Cybercrimes Law (2023) has been used to prosecute 15 individuals for criticising authorities online; in all cases the defendants' rights had been violated;[35]
  - **Zambia:** The recently adopted Cybersecurity Act and Cyber Crimes Act have sparked widespread concern, due to overbroad provisions that facilitate government surveillance and that may cause self-censorship amongst civil society actors;[36] and

---

30 EU SEE, "Sierra Leone Country Focus Report", 4 August 2025"; EU SEE, "Cyber Law Weaponized Against Journalist in Sierra Leone, Raising Alarms Over Press Freedom", *Alert,* 4 September 2025.

31 Reporters Without Borders, "Sierra Leone: New AntiTerrorism Bill Exposes Journalists to Heavy, Unjust Prison Sentences", 7 May 2025.

32 EU SEE, "Eswatini EE Baseline Snapshot", 17 July 2025.

33 EU SEE, "Kenya EE Baseline Snapshot", 2 September 2025.

34 "SERAP Takes Tinubu Govt, Governors to ECOWAS Court Over 'Misuse of Cybercrimes Act'" *Vanguard* (Nigeria), 12 January 2025.

35 Amnesty International, "Jordan: New Cybercrimes Law Stifling Freedom of Expression One Year On", 13 August 2024.

36 EU SEE, "Zambia Country Focus Report", 25 August 2025.

- **Pakistan:** Cybercrime legislation – especially through the Prevention of Electronic Crimes Act (PECA, 2016) and its 2025 amendments – has increasingly been wielded to erode civic space. PECA's provisions (such as Section 26A) are vague, with wide powers provided to authorities to impose disproportionate penalties for online speech.[37]

- **The reform or overreaching application of existing laws, such as penal codes:**

  - **Nepal:** The Electronic Transactions Act is used to criminalise social media posts, resulting in legal actions against journalists and social media users.[38]
  - **Indonesia:** The newly revised ITE law maintains overbroad criminal provisions for online speech.[39]
  - **Mongolia:** The Criminal Code has been used to prosecute journalists for spreading "false information".[40]
  - **Ecuador:** Despite some reforms to legislation, concerning penal code provisions that affect online speech remain.[41]

There is a need to address national security threats, cybercrime, and harmful online content and disinformation, as well as online harassment and violence. However, a rights-respecting approach to these issues is largely lacking. Instead, as described above, regulation relating to digital technology platforms and cybersecurity and cybercrime are undermining the enabling environment for civil society through broad and vague definitions of cybercrime, overly harsh and disproportionate criminal penalties, and the expansion of surveillance without adequate safeguards.[42] As a result, these regulatory practices undermine the enabling environment for civil society by limiting access to uncensored information, exposing them to unwarranted surveillance and creating a chilling effect that stifles dissent.

---

37 International Press Institute, "Pakistan Amended Cybercrime Law Poses New Threats to Press Freedom", IFEX, 26 March 2025.

38 Media Defence, "Freedom of Expression & Digital Rights in Nepal", 3 October 2023.

39 International Commission of Jurists, "Indonesia: Newly Revised ITE Law Threatens Freedom of Expression and Must Be Amended", 6 December 2023.

40 Reporters Without Borders, "Mongolia: Journalist Faces Eight Years in Prison for Exposing Suspected Embezzlement by Deputy Prime Minister", 6 June 6, 2024.

41 Freedom House, "Ecuador: Freedom on the Net 2024", 2025.

42 Maya Recanati & Beth Kerley, (eds.), "Big Question: How Are Cybercrime Laws Weaponized to Legalize Repression?", *National Endowment for Democracy,* 16 December 2024; LEXOTA (Interactive Tool), available at www.lexota.org (accessed 24 September 2025).

This misuse of regulation exists despite the significant and urgent need for strong privacy, data protection, and cybersecurity protections, especially in light of the documented threat and rise of ransomware and cybersecurity attacks on users and on government agencies.

Trend 3: There are limited privacy, data, and cybersecurity protections in the global majority countries or implementation of relevant legislation

Across the world, there is a need for stronger data protection and cybersecurity measures, along with increased cybersecurity capacity within governments and general populations, including the ability to identify perpetrators of cybercrime and hold them to account. Ransomware and cybersecurity attacks on government agencies have been documented in:

- **Trinidad and Tobago**: In 2023–2024, several ransomware attacks targeted public institutions, including one that shut down the postal service;[43]
- **Costa Rica:** In 2022, the Government of Costa Rica was hit by a widescale ransomware attack that led to the declaration of a "national emergency" and affected 27 government departments for many weeks,[44] disrupting the delivery of public services and directly impacting the population's access to essential services;
- **Timor Leste:** External evaluations have found that the country's infrastructure is vulnerable to cyberthreats and that e-government services have basic cybersecurity issues, particularly in defending against social engineering attacks, managing passwords, and securing infrastructure;[45]
- **Nepal:** The country has experienced cybersecurity incidents affecting both the public and private sectors. In January 2024, the government's main server faced cyberattacks, leading to the disruption of hundreds of official websites. Additionally, in 2024, hackers siphoned off NPR 34.2 million (approximately EUR 200,000) from a leading digital payment provider, highlighting vulnerabilities in the financial technology sector;[46] and
- **Paraguay:** Recent years have seen a surge in cybersecurity incidents in Paraguay, including a large data breach of sensitive citizen data in 2025.[47]

---

43 EU SEE, "Trinidad and Tobago EE Baseline Snapshot", 28 May 2025.

44 Cyber Law Toolkit. "Costa Rica Ransomware Attack, 2022.

45 EU SEE, "TimorLeste EE Baseline Snapshot", 31 May 2025.

46 EU SEE, "Nepal EE Baseline Snapshot", 31 May 2025.

47 Julieta H. Heduvan, "Paraguay in Cyberspace: Strategic Vulnerabilities at the Digital Frontier", Asunción: TEDIC, 2 September 2025; Resecurity. "Paraguay Is Being Targeted by Cybercriminals: 7.4 Million Citizen Records for Sale", *Resecurity Blog*, 13 June 2025.

In countries where data protection and cybersecurity legislation doesn't yet exist, this legislative gap presents an opportunity and could be leveraged to promote strong regulatory standards. Where legislation exists but is not adequately implemented, civil society could support implementation, through awareness raising to engage citizens and advocacy to support the resourcing of relevant implementation mechanisms. Some examples include:

- **The Gambia:** The Data Protection Act passed in 2021 has yet to be enacted, and discussions about the implementation of data protection legislation are ongoing;[48]
- **Somalia:** Despite the enactment of the Data Protection Act in 2023, implementation is lagging;[49]
- **Trinidad and Tobago:** Efforts to fully implement the Data Protection Act (passed in 2011) are ongoing;[50] and
- **Ecuador:** the existence of data protection legislation modelled on the GDPR (2021) is not being adequately implemented.[51]2) Building resilience: Civil society's strategies to counter digital threats

2) Building resilience: Civil society's strategies to counter digital threats

Across the world, civil society is adopting legal and advocacy strategies to counter trends that undermine the digital enabling environment. These fall broadly under four categories:

1. Strategic litigation and the use of the judicial system

Civil society has successfully challenged legislation and government actions that undermine the digital enabling environment through national and regional courts. This includes collaboration by local CSOs with regional networks and, in some cases, global CSOs:

48 Council of Europe, "Support for the Legislative Process on Data Protection in the Gambia," Council of Europe: Data Protection, 2025.

49 EU SEE, "Somalia EE Baseline Snapshot", 17 July 2025.

50 EU SEE, "Trinidad and Tobago Baseline Snapshot", April 2025. https://eusee.hivos.org/assets/2025/05/Ttrinidad-and-tobago-baseline.pdf

51 EU SEE, "Ecuador EE Baseline Snapshot", 7 July 2025.

- **Nigeria:** In 2022, the ECOWAS Court ruled Nigeria's 2021 ban on Twitter (now X) was unlawful, violating freedom of expression and access to the media. This followed challenges by civil society and affirmed the illegality of government-imposed internet shutdowns and social media bans in the West African region.[52]
- **Togo:** In 2019, the Paradigm Initiative, along with other Nigerian and regional CSOs joined global CSOs, including Access Now and the Committee to Protect Journalists (CPJ), to submit a "friends of the court brief" in a lawsuit to ECOWAS filed by local CSOs in Togo. In 2020, the court ruled that the restriction on Internet access (2017) was illegal and an affront to the applicants' right to freedom of expression, and ordered the government of Togo to pay two million XAF (approx. EUR 3,000) as compensation, and to take all the necessary measures to guarantee the implementation of safeguards with respect to the right to freedom of expression of the Togolese people.[53]
- **Senegal:** In May 2025, the ECOWAS Court found that the Republic of Senegal violated the fundamental rights of its citizens by shutting down internet and social media platforms during political unrest in 2023, in a case brought by the Association of Information and Communication Technology Users (ASUTIC) and Ndiaga Gueye.[54]
- **Pakistan:** A court suspended a ban on YouTube channels in 2025, following significant backlash from journalists, civil society, and digital rights advocates, as well as the Human Rights Commission of Pakistan.[55]
- **Malaysia:** The civil society organisation SIS Forum contested the application of a fatwa and a ruling that instructed the Malaysian Communications and Multimedia Commission (MCMC) to ban and seize online content relating to them. In 2025, they were successful in overturning the fatwa. The SIS ruling mirrors recent constitutional rulings that reassert federal supremacy over religious overreach in the country.[56]
- **Zambia:** In 2025, the Law Association of Zambia petitioned the Constitutional Court to challenge various provisions within the recently enacted Cyber Crimes and Cyber Laws.[57]

---

52 Media Defence, "Judgment: ECOWAS Court Finds Nigeria Violated Freedom of Expression with Twitter Blocking", 14 July 2022.

53 Paradigm Initiative, "Paradigm Initiative Praises Historic ECOWAS Court Decision on Internet Shutdown in Togo", *Paradigm Initiative,* 25 June 2020.

54 Internet Society Pulse "ECOWAS Court Finds Senegal in Violation of Freedom of Expression and Right to Work Over Internet Shutdowns", 14 May 2025.

55 EU SEE, "Courtroom Clash Over Free Speech: Pakistan Suspends Ban on 27 YouTube Channels Amid Censorship Controversy", 22 August 2025.

56 EU SEE, "Women Rights NGO Wins Lawsuit Against Fatwa Limiting Its Freedom to Act and Speak", 18 August 2025. https://eusee.hivos.org/alert/women-rights-ngo-wins-lawsuit-against-fatwa-limiting-its-freedom-to-act-and-speak/

57 EU SEE, "Law Association of Zambia Petitions Against Zambian Cyber Laws", 30 July 2025.

2. Engagement in national policy processes to expand civic space

These efforts include advocating for the adoption of new laws, such as access to information and human rights defenders' legislation, or to reform existing legislation. Recent examples include:

- **Nigeria:** The Human Rights Defenders Bill introduced in 2024;[58]
- **Bolivia:** Efforts to establish an access to information law have been led by the opposition, who introduced a bill in February 2022;[59]
- **Botswana:** The Access to Information Act (2024) and efforts to ensure that constitutional review is transparent and inclusive;[60]
- **Madagascar:** Efforts to pass an access to information law have recently been the subject of advocacy and capacity building initiatives by local civil society, with the support of UNESCO;[61]
- **The Gambia:** A constitutional review process has been underway since 2018,[62] with civil society advocating for a people-centric constitution;[63] and
- **Sri Lanka:** A public review of the Online Safety Act was initiated in 2025, seen as a significant opportunity to address provisions in the law that have been criticised for their impact on freedom of expression.[64]

3. Engagement with regional and global mechanisms

The use of regional human rights mechanisms (e.g., the ACHPR in the Africa region and the IACHR in the Americas region), bilateral diplomatic platforms (such as the AU-EU partnership), as well as global human rights mechanisms, such as the Universal Periodic Review, treaty body reviews, and engagement with internet governance processes, such as the Global Digital Compact, offer opportunities to advance and enforce human rights norms and standards in the digital sphere.

In countries where national mechanisms are very limited, the use of regional and global networks

---

58 EU SEE, "Morocco Launches Subsidy Program to Promote Amazigh Language Integration", 28 July 2025.

59 EU SEE, "Bolivia EE Baseline Snapshot", 17 February 2025.

60 EU SEE, "Botswana EE Baseline Snapshot", 16 April 2025: EU SEE, "Lack of Civil Society Inclusion and Participation in Botswana's Constitution Review Process," *EU SEE,* 20 August 2025.

61 EU SEE, "Madagascar EE Baseline Snapshot", 29 January 2025; UNESCO, "Building Journalists Capacity to Champion Access to Information in Madagascar", *UNESCO,* 24 January 2025.

62 EU SEE, "The Gambia EE Baseline Snapshot", March 2025.

63 Satang Nabaneh, "Constitution Bill Rejected at Second Reading: Halting the Reform Process in The Gambia?", *ConstitutionNet,* 8 July 2025.

64 EU SEE, "Call for Public Input for Amending the Online Safety Act", 27 August 2025.

and mechanisms to promote awareness and accountability can be particularly important for civil society. For example, following sustained pressure and advocacy by civil society actors in response to Sri Lanka's shrinking civic space and restrictive legislation, UN High Commissioner for Human Rights Volker Türk visited the country, and called for the repeal of the Online Safety Act (OSA), citing its vague and overly broad provisions as a threat to the freedom of expression and digital rights.[65] This intervention has since contributed to the government's decision to open consultations on amendments to the OSA.

4. Civil society use of digital technologies to promote a safer and more secure digital space

Digital rights groups provide a wide range of services that advance a secure, safe and inclusive society:

- **Lebanon:** The digital rights group SMEX has provided tips to support citizens in keeping their online accounts safe, and in being able to assess information on the internet and social media over the course of the Israel-Gaza war.[66]
- **Colombia:** The civil society group Fundación Karisma has identified digital vulnerabilities in government and private-sector solutions, particularly during the COVID-19 pandemic, leading to security improvements and the development of a government strategy for vulnerability disclosure.[67]
- **Nigeria:** The digital rights group Paradigm Initiative has partnered with local media outlets to promote media literacy and critical thinking to address disinformation in the country.[68]
- **Morocco:** In July 2025, the Moroccan government launched a subsidy programme for associations, institutions, and companies to support the integration of the Amazigh language in public administration and digital transformation. This follows sustained advocacy by civil society, notably the NGO Azetta Amazigh, and builds on a government fund established in 2023 to implement the official status of Amazigh.[69]

---

65 EU SEE, "UN High Commissioner for Human Rights Calls for the Repeal of the Online Safety Act and Moratorium on Enforcement of the Prevention of Terrorism Act in Sri Lanka", 7 July 2025.

66 SMEX, "Staying Safe Online in the Context of Conflict in Gaza", 25 October 2023.

67 Fundación Karisma, "New OECD Report Recognizes Karisma's Contribution in the Development of a Strategy for the Disclosure of Vulnerabilities in Colombia," 11 February 2020.

68 Kwame Asante, "The Role of NGOs in Countering Disinformation in Africa: A Vital Tool for Community Empowerment", *Hive Mind,* 4 February 2023.

69 EU SEE, "Morocco Launches Subsidy Program to Promote Amazigh Language Integration," *op . cit.*, note 59.

- **Taiwan:** The civic tech platform vTaiwan has been used to gather citizen input into policy reforms relating to ride-hailing platforms and, more recently, AI governance.[70]
- **The Africa region:** The BudgIT Foundation platform is used to monitor government spending.[71]
- **Globally:** The Ushaidi platform is used to crowdsource data from citizens to strengthen evidence-based policy.[72]

3) Recommendations to promote a digital enabling environment for civil society

For Civil Society Organisations:

Strengthen Advocacy and Collective Action

- **Monitor and document changes** in the digital enabling environment and share verified evidence with the media, legislators, and oversight institutions to inform better laws and policy responses.
- **Advocate for clear, consistent, and transparent digital frameworks** that safeguard civil society's ability to operate, communicate, and mobilise online without undue interference or restrictions.
- **Promote accountability in technology governance**, encouraging governments and platforms to explain how online content is managed, how surveillance tools are deployed, and how citizens' data is used.
- **Build coalitions across sectors.** Partner with media, academia, and private sector allies to promote an enabling digital ecosystem that values pluralism, transparency, and responsible innovation.
- **Use the courts and oversight mechanisms** strategically to challenge laws or practices that restrict online civic participation or hinder organisations' ability to register, access resources, or communicate.
- **Engage in multistakeholder dialogues**, such as national and regional Internet Governance Forums, to ensure that civil society perspectives shape future policy frameworks and technical standards.

---

70 Peter Jia Wei Cui, "AI Governance: How Public Participation Can Improve AI Governance: vTaiwan's Initiatives", *Friedrich Naumann Foundation for Freedom,* 22 October 2024.

71 The BudgIT Foundation, "About Us".

72 Ushahidi, "Deployments".

- **Strengthen digital resilience and literacy.** Organise training for staff and communities on data security, responsible technology use, and preparedness for online disruptions such as internet shutdowns.

Diversify and Sustain Organisational Resources

- **Develop and diversify funding strategies**, including community-based fundraising, solidarity networks, and pooled regional funds that can sustain advocacy during crises.
- **Invest in digital capacity.** Dedicate resources to digital tools, secure communications, and data management systems that allow organisations to work safely and efficiently.

For Governments:

Legal and Regulatory Frameworks

- **Review and update laws affecting digital engagement**, including cybersecurity, data protection, and media regulation, through open consultations with civil society and experts.
- **Ensure clarity and proportionality in all digital regulations**, avoiding vague or overly broad definitions of "cybercrime," "disinformation," or "national security" that can restrict civil society's work.
- **Publish regular transparency reports** on content removal requests, online monitoring, and government data use to promote accountability.
- **Establish independent oversight bodies** that can review complaints about surveillance, censorship, or internet disruptions.
- **Adopt comprehensive data protection standards** and ensure that institutions responsible for oversight are independent, well-resourced, and transparent in their procedures.

Inclusive and Accountable Governance

- **Guarantee open and participatory policymaking processes** on digital and technological issues, ensuring early consultation and inclusion of civil society, media, and the private sector.
- **Encourage dialogue, instead of restriction.** Promote communication and partnership with civil society to jointly address misinformation, online safety, and responsible use of technology.
- **Facilitate access to information.** Ensure that open data and government information systems are transparent, secure, and accessible to CSOs.

Infrastructure and Capacity

- **Close the digital divide.** Invest in affordable and reliable internet connectivity, local infrastructure, and inclusive digital literacy programmes.
- **Support local innovation.** Encourage partnerships that develop civic technology solutions, such as inclusive e-governance platforms, digital feedback tools, and open-source software.

Regional and International Cooperation

- **Engage in regional cooperation on digital governance.** Share lessons and good practices on protecting the enabling environment and preventing digital repression.
- **Promote accountability across borders.** Raise concerns about cross-border misuse of technology, such as spyware exports or online disinformation, through regional and multilateral forums.

For Donors and Development Partners

Programmatic Support

- **Integrate civic space and digital environment indicators** into democracy and governance programmes to track progress on civil society participation, access, and digital safety.
- **Provide predictable and flexible funding** to support long-term work on policy reform, legal monitoring, and digital resilience.
- **Establish rapid response mechanisms** for emergencies such as internet shutdowns, online attacks, or sudden restrictions on civil society communication channels.
- **Support evidence-based advocacy.** Fund local research initiatives that assess how laws, platforms, and technologies affect the enabling environment for civil society.

Investment and Partnerships

- **Support digital infrastructure for civil society.** Provide grants for secure communication tools, data protection measures, and online collaboration platforms.
- **Invest in digital literacy programmes** to help smaller organisations understand technology risks, manage data safely, and participate effectively in online policymaking.
- **Promote open technology ecosystems.** Encourage the use of open-source tools and standards that reduce dependency on proprietary systems and enhance transparency.

For Technology Companies:

- **Design for inclusion and safety.** Embed features that protect users' privacy, prevent online harassment, and ensure transparency in content moderation.
- **Be accountable.** Publish regular reports detailing government requests for content removal or data access, and make them accessible to the public.
- **Engage with civil society.** Consult with civil society groups to assess the local impact of company policies, especially before launching new services or responding to government demands.
- **Ensure fair access.** Support initiatives that promote affordable connectivity, local language inclusion, and accessibility for underserved communities.
- **Evaluate partnerships carefully.** Avoid commercial relationships that enable surveillance, censorship, or other practices undermining civic participation and democratic accountability.

Collective Action Across All Stakeholders

- **Establish coordination mechanisms** that bring together governments, civil society, donors, and the private sector to monitor and improve the digital enabling environment.
- **Carry out periodic public reporting**, for example, annual digital enabling environment reviews at national level, to evaluate progress and maintain transparency.
- **Review the data from the EU SEE's Early Warning and Monitoring mechanisms** to anticipate challenges and identify opportunities to strengthen the enabling environment for civil society before crises occur.

Date: October 2025

About the EU System for an Enabling Environment for Civil Society (EU SEE)

The EU System for an Enabling Environment for Civil Society (EU SEE) is a consortium of international organisations and network members across 86 countries in Africa, the Middle East, Asia and the Pacific, the Americas and the Caribbean. The partnership implements and maintains an Early Warning Mechanism to document changes and shed light on critical trends in the enabling environment for civil society. EU SEE equips civil society, governments, and stakeholders with actionable insights to address challenges and leverage opportunities effectively. It focuses on addressing deterioration in the enabling environment and supporting opportunities for improving the enabling environment for civil society. The Early Warning and Monitoring Mechanism is strongly complementary to a Flexible Support Mechanism that responds to the need for more flexible and timely financial support for civil society in situations of urgency.

Author

Sheetal Kumar

Contributions

Bibbi Abruzzini
Clarisse Sih
Daniela Alvarado Rincón
Eduardo Marenco
Elisa López Alvarado
Emma Achilli
Jake Wieczorek
Lena Muhs
Marie L'Hostis

This brief is part of the EU SEE Project, funded by the European Union. The sole responsibility for the content lies with the author and contributors, and the content may not necessarily reflect the position of the European Union.

The Enabling Digital Environment for Civil Society: Global Trends in Repression and Resistance – an EU SEE Perspective

EU SEE

SUPPORTING
AN ENABLING ENVIRONMENT
FOR CIVIL SOCIETY