EU SEE SUPPORTING AN ENABLING ENVIRONMENT FOR CIVIL SOCIETY

Principle 6 Monitoring Guide: Sources and Practical Considerations

1. Introduction

Principle 6 assesses the extent to which the digital environment in a country enables civil society to participate securely and with integrity. This includes the ability to access and share information freely, without internet or social media shutdowns, and without fear of censorship, surveillance, cyberattacks, disinformation, or online harassment targeting civil society and its work. Access to digital technologies and basic ICT skills is also an important part of this enabling environment.

This guidebook is designed as a practical resource to support monitoring under this principle. In addition to presenting each dimension and clarifying its main concepts, it brings together a selection of relevant sources organised by dimension. For each source, it outlines what it covers, its geographic scope, update frequency, and key limitations for monitoring purposes. Its main purpose is to help researchers identify which sources may be most useful depending on the issue being examined and the country's context.

The guidebook is a living document that can be updated and expanded based on the experiences of Network Members. It is not intended to be exhaustive, and no single source should be considered sufficient on its own. Sources may differ in scope, methodology, and update frequency, so they should be used with an understanding of their limitations and, whenever possible, in combination with other sources. At the same time, the dimensions and concepts presented in this guidebook should not be understood as fully discrete categories. In practice, they may overlap, and the same source may be relevant to more than one area of monitoring. The structure used here is therefore intended as a practical and analytical guide, rather than a fixed classification.

2. Sources by dimensions

Dimension 6.1: Digital Rights and Freedoms

Civil society actors should be able to operate freely online, accessing and sharing information without **internet shutdowns, censorship, or surveillance**.

Internet shutdowns

Internet shutdowns are **intentional disruptions of internet or electronic communications**, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information. The concept covers actions such as **deliberate throttling (intentional slowing of internet**

services) or shutting down internet access, as well as the blocking of social media or instant messaging platforms. For more information, consult this document created by Access Now.

The following sources can help monitor shutdown incidents, assess patterns over time, and provide contextual or comparative information across countries:

Source	Type of source	What it captures	Geographic coverage	Update frequency	Last update	Limitations
Access Now	Interactive dashboard	Documents internet shutdown instances worldwide since 2016.	Global	Annual	2025	Better for retrospective analysis than for real-time monitoring.
Access Now	Election watchlist	Detects internet shutdowns around key elections in 2025.	12 countries from Asia Pacific, Africa, Eastern Europe and Central Asia, Latin America and the Caribbean	One time	2025	Not a comprehensive global dataset of all shutdowns; coverage is limited to selected elections/countries on the watchlist.
Internet Society Pulse	Interactive dashboard	Tracks internet shutdowns including national and regional shutdowns, service blocking, start and end times, duration, and ongoing disruptions.	Global	Continuously, near real time	Ongoing	Methodology is not fully clear.
Internet Outage Detection and Analysis (IODA)	Interactive dashboard	Monitors internet infrastructure connectivity to identify macroscopic internet outages in near real-time.	Global	Continuously, near real time	Ongoing	Focuses on connectivity outages and likely needs contextual information to determine whether an outage should be classified as an intentional shutdown.
V-Dem Digital Society Survey – Government social media shut down in practice	Cross-national survey	Measures how often the government shuts down access to social media platforms in practice.	Global (179 countries)	Annual	2025	Better for retrospective analysis than for real-time monitoring.

In addition to these secondary sources, it may also be useful to consider other forms of early verification. For instance, using a VPN to check whether connectivity is available from another country may help assess whether a disruption is localised. In some cases, governments may also publicly announce restrictions, which can serve as an additional initial signal.

Online censorship

Online censorship refers to actions that **restrict, control, or suppress access to digital content, platforms, or online expression**, particularly for political reasons. It can include the **blocking of websites, the removal or filtering of online content, the suspension or blocking of social media accounts, and restrictions on access** to social media platforms or political speech in digital spaces. While internet shutdowns may be considered a form of digital censorship, they are treated separately in this framework to better capture their specific features and monitoring needs. In the context of civil society, online censorship affects the ability to access information, communicate freely, and participate in public debate online. For more information, see Freedom House's Freedom on the Net reports.

The following sources can help monitor patterns of online censorship, assess developments over time, and provide contextual or comparative information across countries:

Source	Type of source	What it captures	Geographic coverage	Update frequency	Last update	Limitations
V-Dem Digital Society Survey – Government Internet filtering in practice (v2smgovfilprc)	Cross-national survey	Measures how frequently the government censors political information online by filtering or blocking access to certain websites.	Global (179 countries)	Annual	2025	Better for retrospective analysis than for real-time monitoring.
V-Dem Digital Society Survey – Government social media censorship in practice (v2smgovsmcenprc)	Cross-national survey	Measures the degree to which the government censors political content on social media in practice, for example by deleting or filtering specific posts for political reasons.	Global (179 countries)	Annual	2025	Better for retrospective analysis than for real-time monitoring.
Freedom House – Freedom of the Net	Cross-national survey	Assesses internet freedom, including restrictions on online content such as website blocking, content filtering, content removal, and pressures that may encourage self-censorship.	Global (72 countries)	Annual	2025	Better for retrospective analysis than for real-time monitoring.

In addition to these secondary sources, which are often better suited to monitoring longer-term trends, it may also be helpful to complement them with direct checks. This could include monitoring whether Network Members' accounts, whether personal or organisational, or their websites, as well as those of partner organisations, are being

blocked, whether they are experiencing a significant drop in social media reach that may indicate content demotion, or whether content related to protests, mobilisation, or other sensitive civic or political issues is being moderated by platforms. Such more granular signals can provide a useful additional layer of analysis.

Digital surveillance

Digital surveillance refers to the **monitoring, collection, interception, or analysis of people's online activities, communications, or digital content**, often by state authorities and **without adequate safeguards**. This can include practices such as the **collection of personal data, the interception of digital communications, and the use of intrusive hacking tools, AI-enabled surveillance systems, and biometric surveillance tools such as facial or voice recognition** to collect information about people's digital activities[1]. Surveillance can discourage people and organisations from speaking openly, connecting with others, or taking part in public debate online. In the context of civil society, it can weaken the ability to communicate securely, organise freely, and participate in civic life without fear of being monitored or facing reprisals. For more information, see OHCHR's reports on the right to privacy in the digital age.

The following sources can help monitor patterns of digital surveillance, assess developments over time, and provide contextual or comparative information across countries:

Source	Type of source	What it captures	Geographic coverage	Update frequency	Last update	Limitations
V-Dem Digital Society Survey – Government social media monitoring (v2smgovsmmon)	Cross-national survey	Measures how comprehensive government surveillance of political content on social media is in practice.	Global (179 countries)	Annual	2025	Better for retrospective analysis than for real-time monitoring.
Surveillance Watch | DAIR	Interactive map	Maps connections between surveillance companies, their funding sources and affiliations.	Global (179 countries)	Continuously, near real time	Ongoing	Better suited to mapping the surveillance industry and its actors than to monitoring specific surveillance incidents in real time.
Data Library | Atlas of Surveillance	Dataset repository	Compiles projects on surveillance technologies,	Mixed (U.S. - focused datasets as well as some	Varies by dataset	Varies by dataset	Better suited to background research and ecosystem

[1] While digital surveillance may overlap with online censorship, particularly when monitoring practices are used to intimidate users, or enable content restrictions, the two are treated separately in this guidebook. Digital surveillance focuses on the monitoring and collection of digital activities and communications, whereas online censorship focuses on the restriction, removal, blocking, or suppression of online content, platforms, or expression.

		practices, and actors, including law enforcement surveillance tools, facial recognition, and AI-enabled surveillance.	regional and global resources)			mapping than to monitoring specific surveillance incidents. Scope, methodology, and timeliness vary across datasets.

In addition to these secondary sources, it may be useful to complement monitoring efforts with other evidence-gathering strategies. For example, Freedom of Information requests may help obtain information on the use of AI in public administration, while reviewing public procurement processes may help identify whether authorities are contracting surveillance or monitoring companies. These approaches can provide a useful additional layer of evidence.

Dimension 6.2: Digital Security and Privacy

Civil society actors must be protected from **cyber threats, and harmful online practices such as harassment**, and **information manipulation techniques**, with strong data protection laws and redress mechanisms in place.

Cyber threats

Cyber threats refer to **malicious digital activities or risks** that may compromise systems, networks, devices, or data. In the context of civil society, they can include **phishing, malware, ransomware, account compromise, and other forms of digital attacks** that disrupt operations or expose sensitive information. For more information, consult the cyberspace analytical report consolidated by the Cyber Peace Institute.

The following sources can support the monitoring of cyber threats across platforms and over time:

Source	Type of source	What it captures	Geographic coverage	Update frequency	Last update	Limitations
CyberPeace Tracer	Interactive dashboard	High-level view of cyber threats and vulnerabilities affecting CSOs.	Global	-not available-	2026	Not a comprehensive picture of the full global cyber threat landscape; focused specifically on civil society-related threats.

In addition to these secondary sources, it may be useful to complement monitoring efforts with reports from organisations focused on civic freedoms and human rights violations. These sources may help identify individual cases of cyber threats affecting civil society actors, although they should be treated as complementary rather than specialised cybersecurity sources.

Other harmful online practices

Other harmful online practices affecting civil society may include online harassment and information manipulation techniques such as disinformation. Online harassment refers to **abusive, intimidating, or threatening behaviour** carried out through online platforms or digital communication tools. It can include **insults, threats, stalking, doxxing, coordinated abuse, or other forms of targeted harmful behaviour**. Disinformation refers to **verifiably false or misleading information created, presented, and disseminated to intentionally** deceive and may cause public harm. These practices can undermine the credibility, safety, and effective participation of civil society actors in digital spaces. For more information, visit UNESCO site and OHCHR's work on human rights in the digital age.

Social media monitoring can help identify harmful narratives, targeted abuse, and manipulative content that may affect civil society actors and their work online. Within the EU SEE learning community, Network Members can access social media monitoring trainings free of charge and receive support in applying this methodology in practice. For more information, consult Social Media Monitoring Training – Eu SEE.

Source	Type of source	What it captures	Geographic coverage	Update frequency	Last update	Limitations
Social Media Monitoring	Access to public platform content	Public posts, comments, captions, engagement metrics, and account activity.	Global	-not applicable-	-not applicable-	Does not directly identify harassment or disinformation, which must be inferred through additional analytical methods. Coverage is limited to public content and platform-accessible data, and may be affected by access restrictions, deleted content, and changing platform policies.

Dimension 6.3: Digital Accessibility

Civil society actors and the public **have access to digital technologies and the necessary skills** for effective online engagement.

Internet Penetration Rate

Internet penetration rate refers to the **share of a country's population that has used the internet within a given period**, usually measured as the percentage of individuals who used the internet in the last three months. It is a useful indicator of how widely digital access is distributed across the population and, in the context of civil society, helps assess whether people have the basic connectivity needed for effective online engagement. For more information, consult the World Bank Glossary.

The following sources can support the monitoring of internet penetration across countries and overtime:

Source	Type of source	What it captures	Geographic coverage	Update frequency	Last update	Limitations
Statista	Data visualisation platform	Provides a comparative ranking of countries by internet penetration rate.	Global	Annual	2025	Not an original data producer; better complemented by another source.
DataReportal	Reports	Provides country, regional, and global digital statistics.	Global	Annual	2025/2026	Not an original official statistical producer; relies on multiple external data providers.
World Bank	Dataset	Measures the proportion of individuals who used the Internet from any location in the last three months, expressed as a percentage of the population.	Global	Annual	2025	Country-level data may be published with a time lag, so the most recent available year can vary across countries.
Broadband statistics | OECD	Dataset	Tracks fixed and mobile broadband subscriptions, penetration rates, technologies, speeds, and selected internet usage indicators.	OECD countries	Annual	2024/2025	Better suited to tracking broadband connectivity and infrastructure indicators than overall internet penetration in the broadest sense; coverage is mainly limited to OECD countries and relies largely on subscription-based measures rather than direct measures of meaningful access.

Information and Communication Technologies (ICT) Skills

ICT skills refer to the **abilities needed to use digital technologies effectively**. They are often measured through whether individuals have recently performed specific digital tasks, such as **handling information, communicating online, creating content, staying safe, and solving problems using ICTs**. In the context of civil society, ICT skills are an important indicator of whether the public can engage meaningfully in digital spaces. For further information, visit the ITU Glossary.

The following sources can help assess levels of ICT skills, track developments over time, and provide contextual or comparative information across countries:

Source	Type of source	What it captures	Geographic coverage	Update frequency	Last update	Limitations
ITU DataHub	Dataset	Provides internationally standardized indicators on ICT skills, based on whether individuals have recently performed specific digital tasks.	Global	Annual	2025	Data availability is limited and uneven across countries and skill areas.