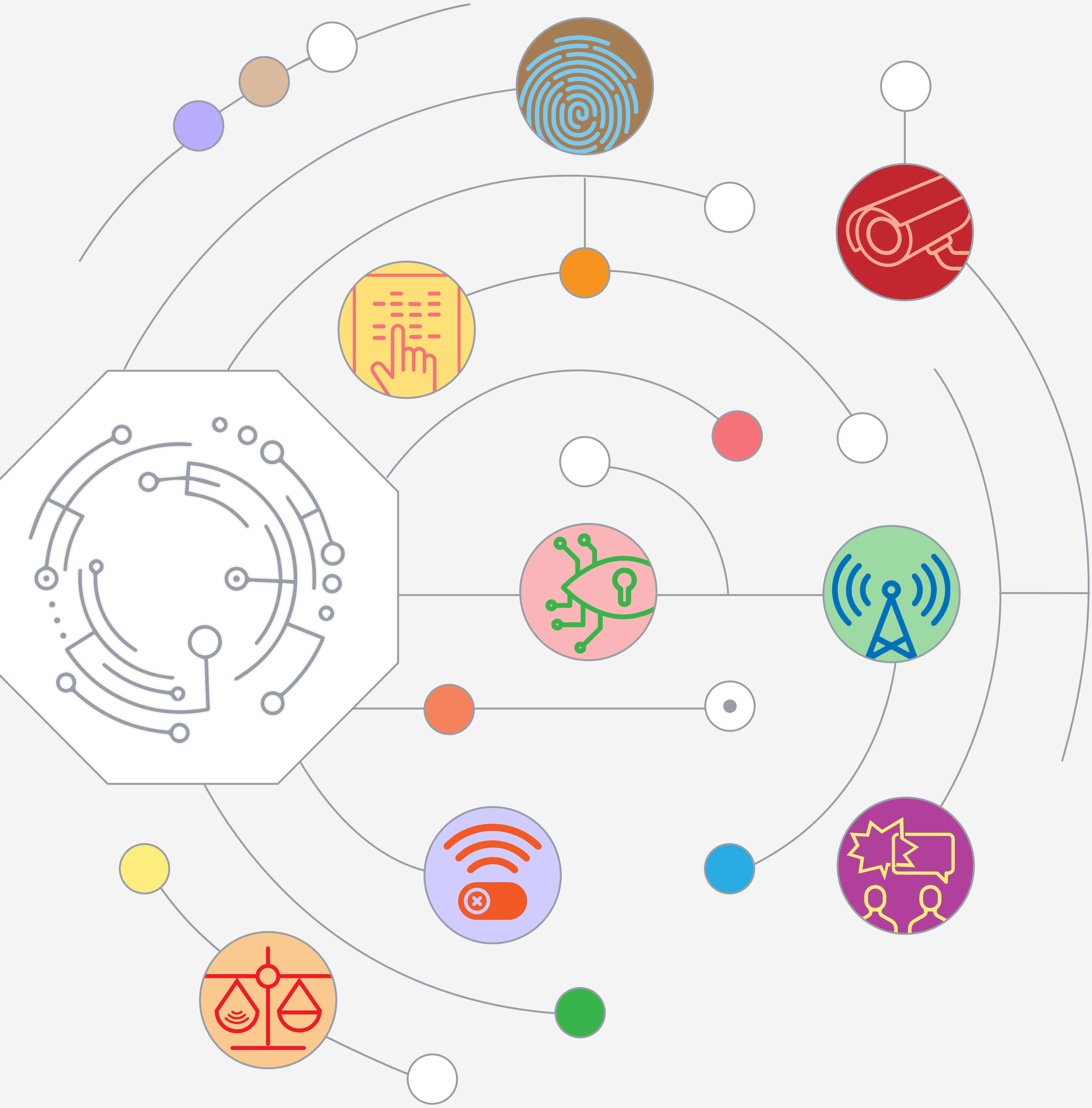
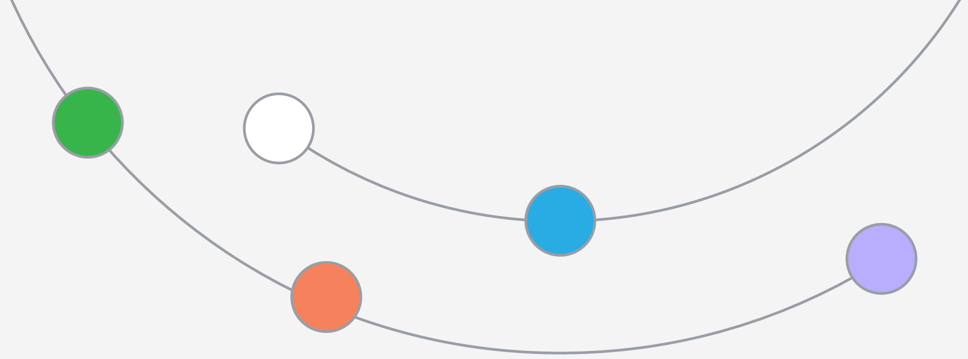
Together for an Equal, Just and Democratic Digital World

Action Programme for Tech for Democracy – Civil society recommendations



Tech for Democracy

GLOBAL **FOCUS**
- Danish CSOs for Development Cooperation



Preamble:

Aim of the Action Programme

With the Action Programme for Tech for Democracy, civil society from across the world gives its recommendations for concrete actions to be taken by a broad range of stakeholders including governments, the private sector, multilateral institutions and civil society. The Tech for Democracy initiative is initiated and funded by the Danish government to ensure that digital technologies enable, rather than oppose democracy and human rights. The Tech for Democracy Pledge has been introduced by the Danish government, which outlines the principles and values important for Tech for Democracy to be signed by governments, the private sector and civil society. The Action Programme dives deeper into the concrete actions that civil society recommend should be taken and is based on a global consultation with inputs from over 100 civil society organisations, experts, human rights defenders and academia from over 40 countries around the world.

The challenge with tech for democracy

While digital technologies hold immense potential for promoting pluralist democracy, popular participation, and giving a voice to marginalised groups, the current reality is in stark contrast to the emancipatory ideals fundamental to the open values of the internet and potential of digital technologies. Mass surveillance, internet shutdowns, polarising algorithms, and a pandemic of misinformation and disinformation have overtaken the internet. Meanwhile, freedom of speech is being restricted and online activities are criminalised. In 2021, global internet freedom declined for the 11th consecutive year, while the first 5 months of the year saw 50 intentional internet shutdowns across 21 countries.

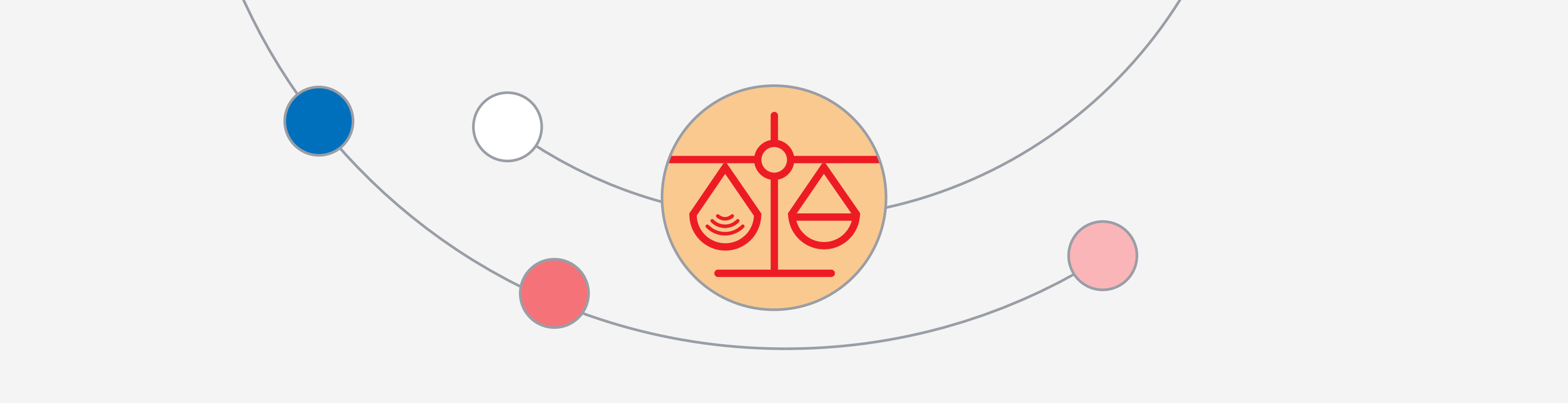
Digital technologies have provided the opponents of freedom and human rights a vast array of sophisticated tools to limit, exploit, and restrict online behaviour while consolidating their own power. Especially groups facing discrimination and exclusion are at the frontline of these attacks whether due to gender, ethnicity, sexuality, religion, race, or others. Yet this does not have to be our future! The Tech for Democracy initiative calls on all relevant stakeholders to come together and advance actionable solutions to the challenge of our time. To ensure that digital technologies positively contribute to democracy, human rights, freedom, justice, equality and dignity, rather than oppose it.

The need for civil society to be placed front and centre

Civil society, human rights defenders, and journalists around the world are often main targets of digital crackdowns, surveillance, and censorship. Civil society plays a crucial role in ensuring that solutions are based on local challenges and needs that they and other citizens around the world face. Building digital resilience and mobilisation, improving digital and media literacy, and fair access of civil society are key to ensuring that technology fosters democratic and inclusive societies, where human rights and civic space ensure meaningful citizen participation and dignity.

Civil society is already working to ensure this but is met with challenges especially related to lack of digital responsibility by duty-bearers and the private sector as well as lack of funding to address the many challenges faced. Civil society voices must be kept at the forefront of the dialogue and supported financially to carry out the needed work. This includes ensuring the ongoing digital skills acquisition and capacity building of the public and civil society given the rapidly changing nature of digital technologies.

It is our belief that only collectively, drawing on a wide range of stakeholders representing different interests and sources of expertise, can we confront the challenges facing digital technologies and democracies today.



1. Protecting Human Rights in the Digital Space and Establishing Digital Accountability

In order for digital technologies to promote and advance, rather than suppress democracy and human rights, there needs to be support for robust and transnational frameworks. The governance of the digital ecosystem should be transparent, accountable and inclusive. There is an urgent need for a fundamental shift away from the status quo where enforcement is weak and accountability non-existent. We need to move towards multi-stakeholder models of governance in which civil society plays an integral role to establish digital accountability.

1.1. **Governments** should s**upport international, institutional and multi-stakeholder frameworks** to **facilitate responsible global governance** of digital technologies, **empower** the frameworks and ensure that they have power through mechanisms such as import and export controls

1.2. International regulatory frameworks should emphasise **protecting citizens' digital rights** and political freedoms. The framework should further include **possibilities to sanction** governments, companies, organisations, and individuals that do not abide by these principles

1.3. **Global treaties, standards, and international institutions** involved in the **governance** of the digital space, should be build and reflect **international human rights principles**. This must, as a minimum, include the right of **freedom of association** and **freedom of expression**, the right to privacy and the **right to non-discrimination**

1.4. Multilateral institutions should establish **oversight committees** that supervise whether governments are **infringing upon** the **online rights** of citizens. These committees should be at both **national and international level**, ensuring a **bottom-up chain of command**, so people at ground level can report abuses

1.4.1. **There is a need for international push back** against national laws which seek to limit **fundamental digital rights and civic space** both online and offline. Including, but not limited to national security laws, criminalisation of online activities, employee registration legislation, data localisation laws, censorship or content moderation laws

1.5. There is an urgent need to commit to and enforce a robust governance framework which **empowers civil society** and finances national and international watchdogs

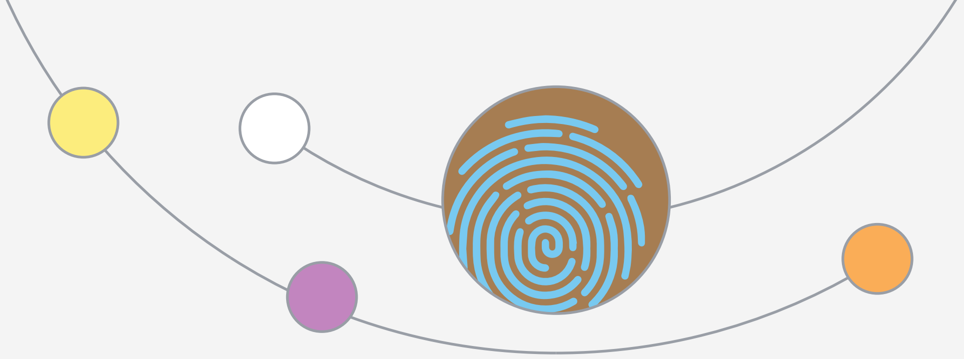
1.5.1. **Ordinary citizens**, and representatives of marginalised and vulnerable groups, should be **represented** in the **governance** of the digital space, as it creates positive spill over effects when governance is **diverse** and **multi-stakeholder**, including among others, academia, civil society representatives, trade unions, employees, and ordinary citizens

1.6. All countries should seek to establish a **national digital-rights ombudsman**

1.7. Digital technology providers and governments should conduct **human rights impact assessments**, including during design and development phases and prior to and throughout deployment, where **civil society** organisations and **diverse communities** are **broadly represented**, at local, national, and global levels

1.8. Global **certification standards** must be developed to be awarded to tech companies and other actors in the digital ecosystem, who are **consistent** with **human rights** and **ethical standards** including adequate user protection and access to remedies

1.9. Large tech companies and platforms should establish **consumer panels**, with real influence on the operations of the platforms, to **monitor** and **reflect** on the public impact of the policies and practices of these large tech companies



2. Building Secure Digital Infrastructure

Currently, the internet is designed and structured as a profit-maximising business model. In line with the fundamental “right to access”, the internet should be viewed as a collective, critical and fundamental infrastructure as well as a global public good, which belongs to us all. Safety, equality, equity, health and human rights should be thoroughly emphasised in the design and structure of the digital space. Taking into consideration the disfunction and damaging effects on democracy of our current digital infrastructure, our long-term vision is infrastructure that explicitly and by design serves the public interest, democracy and human rights.

2.1. **Private** internet providers, and **other actors** involved in the diffusion and maintenance of the internet should be **legally obligated** to govern their internet in accordance with a **human rights-based approach**

2.2. Public institutions in democratic countries should use **open software** and be transparent regarding which systems utilise **automated decision-making processes, like AI and algorithms**, and to what effect. Any use of such technologies should be **thoroughly tested** and be the subject of human rights impact assessments throughout their lifecycle in order to fully understand their impact, drawing on relevant stakeholders including **civil society actors**

2.3. Governments and multilateral institutions should establish **bans or moratoria** on the deployment of **automated decision-making processes, including AI systems**, that present an unacceptable risk of interfering with the enjoyment of human rights, the functioning of democracy, and the observance of the rule of law. This includes AI systems using biometrics to identify, categorise or infer characteristics or emotions of individuals, and AI systems used for social scoring to determine access to essential services

2.4. In some countries, primarily in the Global South, the **large tech companies and platforms** are to a large extent the **entire internet infrastructure.** Tech companies need to take this **responsibility serious, maintaining safe spaces**, making their tools available in **recognized languages** and **upholding individual** and **collective rights**, and **address accessibility** concerns

2.5. Governments and private companies, such as large tech platforms and data centre providers should offer **safe, decentralised data storage and platforms** to organisations, hosted in democratic and legally well-functioning countries, with established **rule of law and judicial processes**. This will mitigate **pressure** from **authoritarian regimes** to **access data**

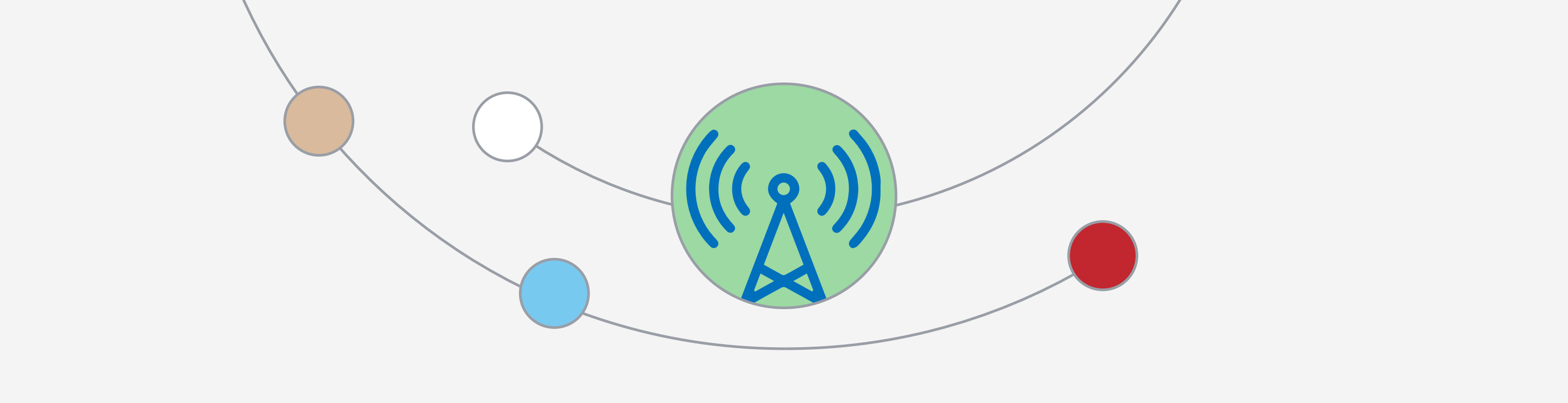
2.6. Under the global regulatory framework, **governments should commit to pushing back** against **data localisation laws** enacted by autocratic leaders for surveillance and censorship purposes

2.7. Governments and relevant tech companies, including software and platform providers, should **commit** to ensuring **safe and anonymous ways to communicate**, such as **encrypted communication tools**. This is especially true for **human rights defenders, activists, and other vulnerable or marginalised groups**

2.7.1. Governments and tech companies should **promote knowledge** of safe and encrypted technologies and **apply** them widely

2.8. Democratic governments and tech companies **should establish local** and **regional points of support** for organisations experiencing **digital attacks**

2.9. Tech companies should develop **healthy design** of both software and hardware that don’t promote **addictive, persuasive** technology principles and techniques but focus on **ethical**, or **conscious** design instead



3. Closing the Digital Divide

Currently, almost half of the world's population do not have access to the internet. In a time of hyper digital connectivity, excluded peoples are put at a significant disadvantage when it comes to expressing their democratic views, engaging in online conversations, accessing information, and much more. The digital divide includes, but is not limited to, a north-south divide, a divide across rural-urban dimensions, gender, generations, accessibility, and more. In order to move towards an equal, equitable, and democratic online digital space, citizens of the world must have the opportunity to access the internet on equal footing.

3.1. The **international community** should **recognise** the "**right to access**" to the digital space as a **fundamental human right**

3.2. In recognition of the universal and fundamental "right to access", governments, international organisations, and private actors should **commit** to **mobilising resources** to eliminate the digital divide, including **faster, safer, cheaper, and more inclusive digital infrastructure**

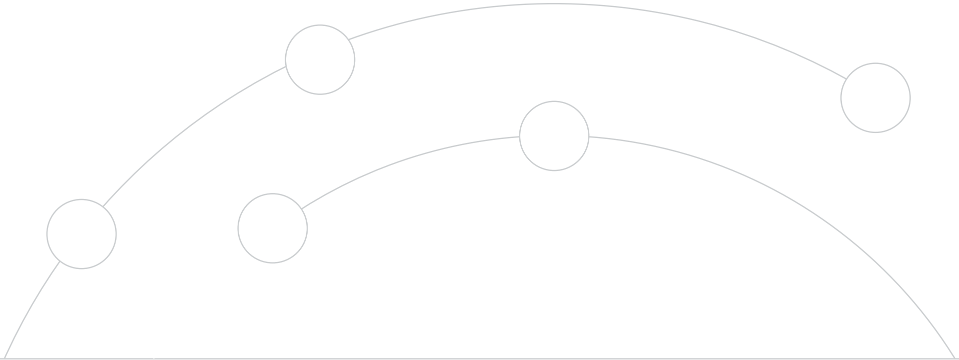
3.3. **Actors** involved in digital expansion and eliminating the digital divide should conduct **human rights impact assessments** involving **relevant stakeholders**, including **local communities and civil society**; to assess the potential negative impact and disruption of their policies

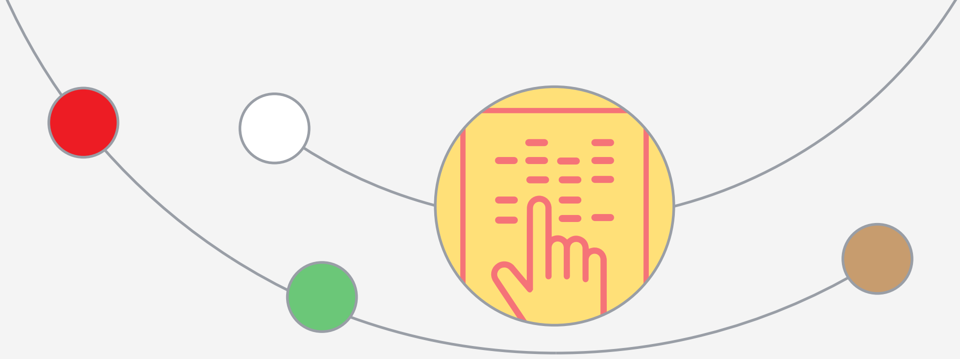
3.3.2. Actors involved in eliminating the digital divide should also be conscious of promoting digital literacy and knowledge of digital rights

3.4. **Governments** should provide **physical locations** where people can **access** the internet, **publicly funded**

3.5. **Multilateral institutions should ensure opportunities for meaningful online civil society participation** in UN meetings and give space to local civil society organisations to access their internet to take part in online and hybrid UN meetings

3.6. The **international community** should **commit resources** to capacity building for local and national **regulators**, training, and education to **technologists** from all over the world





4. Improving Digital Accessibility and Usability

Accessibility concerns are often under-prioritised due to market mechanisms and the fact that digital participation is viewed as a privilege not a fundamental human right. In line with the ‘right to access’ and the principle of *Leave No One Behind*, accessibility and usability concerns should be taken serious and prioritised higher by governments and large tech platforms.

4.1. There is a **need** for greater **diversification** of **languages** that are supported on technical platforms, including encrypted communication tools. Both in terms of **languages**, and which **keyboards** are supported; as well as **support and help functions**

4.2. There is a necessary and urgent need to develop **international standard icons to support international sign language**. Governments, tech platform providers, and civil society organisations should come together and formulate a uniform standard for digital sign language

4.3. Multilateral organisations, government websites, and large tech platforms should provide **disability-friendly** choices including **language, interface, and assistance options**

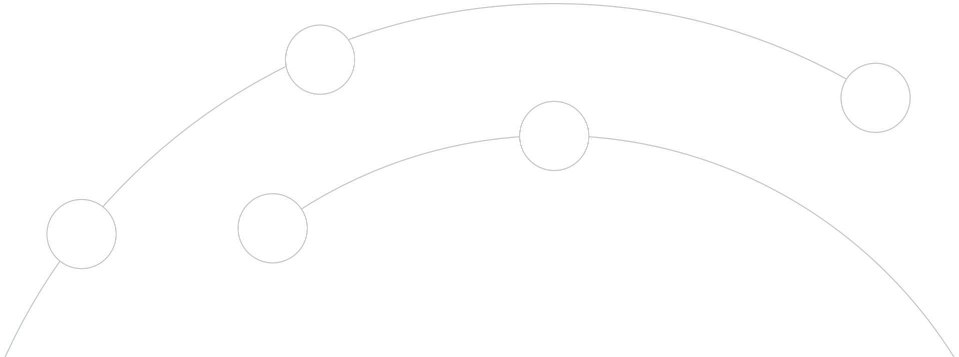
4.4. Multilateral institutions, national governments, and large tech companies should **support** the **development** of **disability friendly** technologies, platforms, and supported languages, third-party programs, and other functions

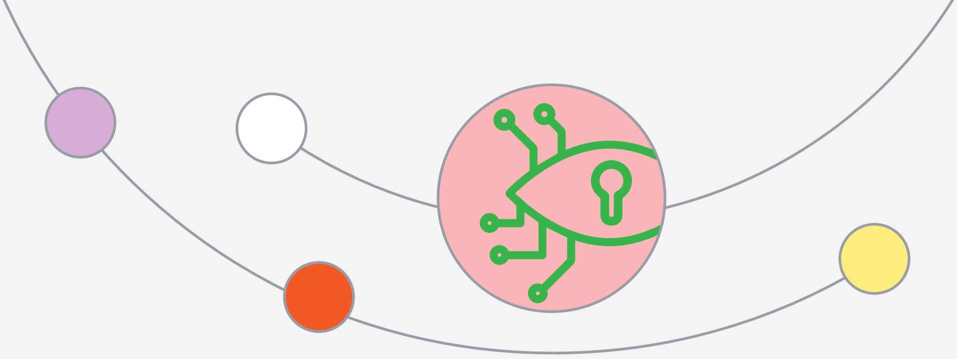
4.4.1. This should not transfer costs onto already vulnerable and marginalised peoples. Governments and tech companies should come together and remedy this injustice; including responsible and compatible data handling

4.5. Multilateral organisations and governments should invest in **capacity building initiatives** for **people with disabilities** to help navigate the internet

4.6. Multilateral organisations, national governments, and digital service providers including large tech platforms, should commit to provide **equal** and **equitable access** to technologies. No **digital inequality** in terms of quality of access

4.6.1. Ensure that **local payment methods** and credit cards are supported by all platforms. Users should not be restricted from using a kind of technology or digital service because the service lacks a **localised payment option**





5. Establishing Digital Privacy

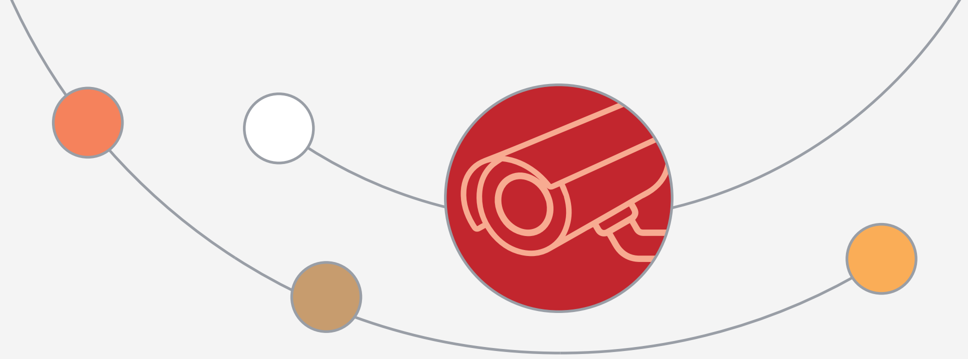
The developments regarding personal privacy and the extraction of data in the digital space, which has been dubbed 'Surveillance Capitalism', should be viewed as an expropriation of critical human rights and a violation of individual sovereignty. Any move towards a rights-based, equal, and just digital ecosystem must take the *Right to Privacy* seriously and take the necessary steps towards a privacy-by-design online economy.

5.1. The **privacy-by-design** online economy must include **global regulation** of what **data** companies are allowed to collect, what it can be used for and what it cannot

5.2. Private companies that collects **data** on its 'customers' should be **obliged** by law to be **transparent** and disclose **what data is collected and what it is used for**. This includes, but is not limited to, large tech platforms, internet providers, soft, and hardware producers, and data analysis firms

5.3. **Personal data** being used in **political campaigns**, like the Cambridge Analytica scandal, represents a brazen **attack** on our **democratic capacity and values**. Political campaign targeting based on personal data should be made **explicitly illegal**. Furthermore, the gravity of this unethical practice should be recognised, and sanctions should reflect this. It should not just be a case of "paying the costs to do business"

5.4. Empower civil society actors to critically **audit** the **national security benefits** of **extra-territorial mass surveillance** programs engaging intelligence agencies, courts, and private actors involved in the ecosystem



6. Proliferation of Spyware Technologies

The spread and adoption of sophisticated spyware technologies, as documented by the 2021 Pegasus Leaks, a leak uncovering global abuse of cyber-surveillance technologies, have highlighted the dangers and capacity for abuse posed by such emerging technologies. Often activists, human rights defenders, and civil society are the main targets of such extra-legal surveillance. In order to democratize the digital space, and make it safe for frontline defenders, the use of emerging spyware technologies must be adequately regulated.

6.1. In line with the 2021 Pegasus leaks, and the breath and scale of those findings, **states** should impose an **immediate embargo** on the **sale and diffusion** of spyware technologies until a **robust human rights regulatory framework** is in place

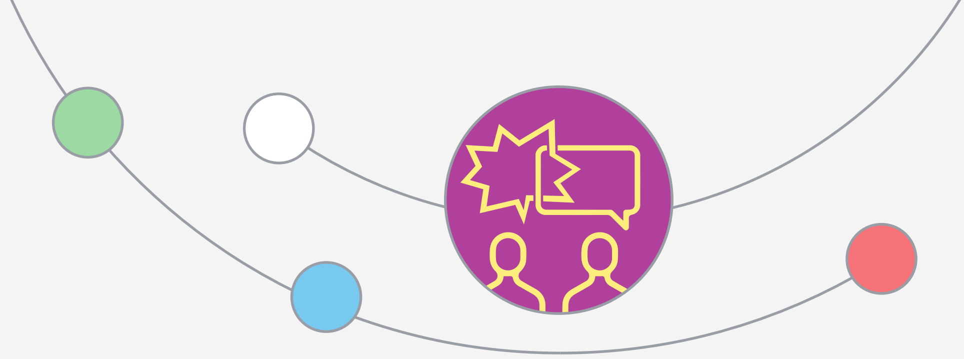
6.2. The regulatory framework on the Proliferation of spyware technologies should as a minimum **regulate the export of spyware technologies**, including the **rejection** of **export sales** to countries where there is **substantial risk** it could lead to **human rights violations** or countries that have **inadequate** legal, procedural, or technical standards to prevent abuses. This should all be in line with the United National Guiding Principles on Business and Human Rights a minimum standard

6.3. This regulatory framework on the proliferation of spyware technologies should further enforce **transparency** by states of the **export and procurement** of surveillance and spyware technologies. This includes transparency regarding the **volume, nature, value, destination, and end user**. Furthermore, states should be **obliged** to disclose information on their procurement of all previous, current, and future contracts with **private surveillance companies**

6.4. **Private surveillance companies** should be **legally obliged** to disclose products and services offered and sales; and transparency of clients, including end users and relevant third parties

6.5. Private surveillance companies should be **legally required** to **conduct human rights due diligence** of their operations, supply chains, and clients in order to **identify and mitigate** the human-rights related risks of their activities

6.6. Private surveillance companies should be **legally required** to act **responsibly**, and **held liable** for their **negative human rights impact**, including liability for harms caused and a roadmap for restitution and compensation to victims



7. Infodemics – Countering Disinformation and Hate Speech

The pandemic of disinformation and hate speech poses some of the starkest challenges to democracy and human rights. In many countries, it is an organized and strategically run program by state and semi-state actors. This problem is compounded by the fact that many platforms lack adequate and inclusive language options making it challenging to report abuses or have the platforms take down content in a timely manner. In order to make the digital space open, safe, and democratic for everyone; multilateral organizations, national governments, and tech companies need to take several concrete steps.

7.1. Governments should balance countering the spread of misinformation, disinformation, and hate speech by **safeguarding freedom of expression**. Governments should not use the threat of disinformation as an **excuse** to **crackdown** on legitimate speech

7.2. Multilateral organisations, governments, large tech companies, and research institutes should **financially** support **research** on the systematic **spread of disinformation**, including how **algorithms** facilitate the spread of fake news and minority discrimination. This should include research with particular attention to disinformation in regard to **elections**, also in smaller countries

7.3. Deepfakes and shallow fakes are **threatening** the **trustworthiness** and **legitimacy** of **grassroots organizations** Governments and large tech companies should come together, and draw on the experiences and expertise of civil society actors in designing ‘authenticity infrastructure’

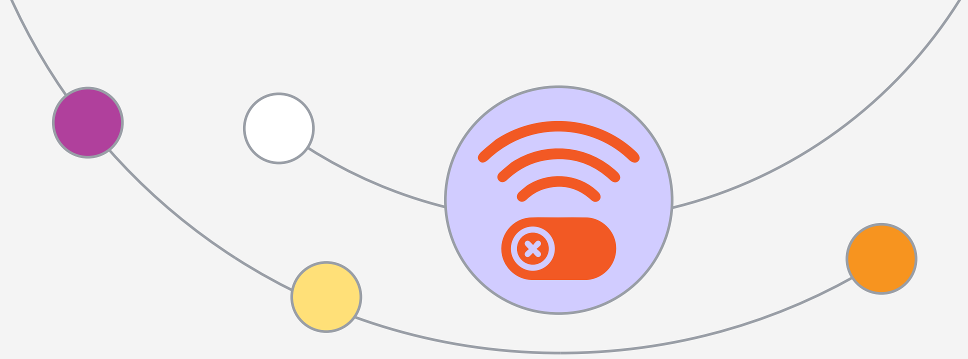
7.3.1. Governments and large tech companies should finance initiatives, including research, reporting, and infrastructure that tackles the authenticity and legitimacy challenge posed by these emerging technologies

7.4. Oftentimes misinformation, disinformation, hate speech and incitement to violence is **funded, sponsored** and **supported by governments**, semi-government, or other political actors. Multilateral organisations, national governments, large tech companies, civil society, academia, and research institutions should **mobilise resources to monitor, document, and sanction** actors engaged in **systematic and strategic** misinformation, disinformation, political intimidation, hate speech, and incitement to violence in all its forms

7.5. Tech platforms have a responsibility to their ‘consumers’. Thus, it is ultimately the **responsibility** of tech platforms like Facebook, Twitter, and others, to provide **safe spaces** on their platforms

7.5.1. Tech platforms should commit to **taking down online hate speech in a timely manner backed by a published and transparent process**

7.6. Civil Society should **raise the issue** of the suppression of women’s voices and minorities by organised state actions in **international forums** like UPR, HRC, or in bilateral meetings



8. Ending Internet Shutdowns, Censorship and Content Moderation

Internet shutdowns, censorship and content moderation are prevalent tools for authoritarian governments to control the flow of information. This presents a significant threat to the free flow of information, and the quality and sustainability of national democracies. Governments often rely on private actors in the technical aspects of these crackdowns leaving the tech sector's commitment to transparency and digital responsibility as some of the most effective ways to counter authoritarian abuses.

8.1. Digital technology providers and large tech platforms should be **committed** to transparency, and allow civil society, researchers, and academia access to social media data to **research, monitor, and document** internet shutdowns, fake-news, government requests for censorship, content moderation and online abuse and hate speech

8.2. **Intentional internet shutdowns** should be made **explicitly illegal** and **sanctionable** under a global regulatory framework and under international law

8.2.1. This will help companies withstand the pressure of governments to engage in internet shutdowns, especially large multinational corporations. Governments should commit to enforcing this principle, and support private companies in the face of authoritarian internet shutdowns

8.3. The global communication infrastructure should to a **larger extent** be built with **resilience** in mind in order to withstand **systemic failures**, such as internet shutdowns. Governments, tech platforms, and other actors engaged in the internet infrastructure should commit resources improve internet resilience, including to:

- Divest from vulnerabilities such as backdoor entrances or regional blockers
- Use resilient-enhancing technologies and infrastructure such as Mesh Networks
- Invest in methods to document internet shutdowns, including targeted shutdowns that limit access to specific sites, apps or media

8.4. Governments, the private sector, and civil society should **expand** and develop solutions to counter **internet shutdowns** or getting **online access** when electricity is out. Currently, these are primarily available in the Global North

8.5. Funding should be made available for the **public to legally challenge** internet shutdowns

8.6. Large tech platforms should be committed to providing feedback mechanisms to report censorship. If your content is being taken down, people should have the **right** to know **why and by whose request**

8.7. No '**One Size Fits All**' solutions. Not the same solution to content moderation works everywhere: measures aimed at avoiding discrimination often end up facilitating abuse of power

November 2021

Global Focus
Rysensteensgade 3, 3. sal
1564 København V

Layout/Design:
Maja Wesnæs

Tech for Democracy

GLOBAL FOCUS
- Danish CSOs for Development Cooperation