

YOUTH 4 DIGITAL SUSTAINABILITY



BACKGROUND PAPER

SUSTAINABLE INTERNET
GOVERNANCE



Sustainable Internet Governance

Table of contents

Recommendations.....	2
Artificial Intelligence.....	3
Data localization and splinternet.....	6
Possible Solutions.....	9
References.....	9

Recommendations

SUSTAINABLE INTERNET GOVERNANCE

10

We urge states to pursue cross-border alliances in the governance of the Internet as a shared resource based on democratic ideals. Entities collecting and managing data should adopt alternative forms of data governance that grant individuals greater control over their data.



11

Rules for AI and standards for ethical AI should be formulated through a multistakeholder approach rather than by technology companies. AI systems should be audited based on these rules by external parties for fairness and their working should be made transparent to the public.



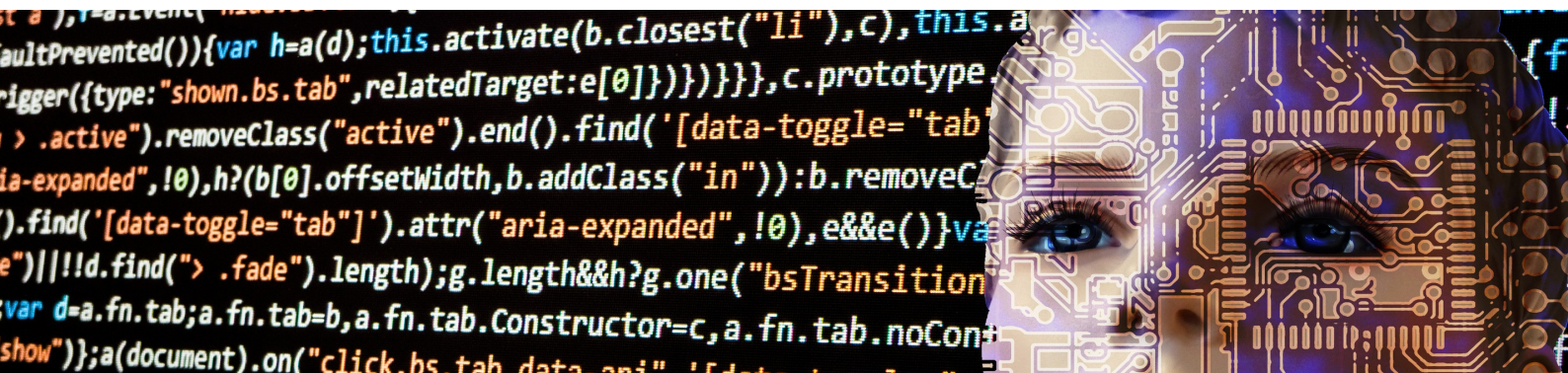
12

The companies that develop and sell AI systems should be held accountable for them and any entity that uses these systems should implement a comprehensive monitoring and evaluation system throughout the lifetime of the system.



Artificial Intelligence

Artificial Intelligence has the potential to bring benefits to the society and to cause harm; this has been known for many years. Nevertheless, no clear regulations exist. While some stakeholders continue to emphasize ethics of AI, others emphasize that innovation for social development should be the priority. Recently, there has been a move towards a risk-based assessment approach. While a risk-based assessment can be useful, it needs to be specific. The proposals so far have been vague and do not consider complex risks.



What we need are clear enforceable rules and implementable policies that address different kinds of risks and harms that AI can cause. Is the system fair, is its working transparent? The rules should also provide guidelines on who should audit these systems and not rely on the companies that develop AI systems, who should be held accountable. Furthermore, the guidelines should not consider AI as a standalone system. These systems interact with many of the existing systems such as healthcare, advertising, etc., and the risk assessment should account for this diversity. Additionally, a human rights assessment of the systems should be performed before these systems are used, especially when they are deployed to solve social problems.

A more wholesome approach that accounts for the technical understanding as well as social equity should be used when it comes to interrogating the fairness of AI. Therefore, the Internet Governance Forum can function as a platform, bringing together all the different stakeholders and encouraging a vivid dialogue between these different groups. Furthermore, AI systems have to be audited for fairness of outcomes. In the past, several cases of an AI discriminating groups of people were made public. Cognitive biases, missing training data or unrepresentative sampling are recurring biases.

First of all, the companies are obliged to ensure that their AI is as unbiased as possible and that their training data sets include data from all different groups of people. It has to be assured, that the used data mirrors the society. Second, the companies have to have their AI tested before putting it into use. An AI should be evaluated either by authorities or private companies specialized on checking such systems. The testing authorities have to ensure that the AI meets all the rules formulated by the multi-stakeholder group. Only if these entities come to the conclusion that the AI does not contain biases and works as intended, the AI is allowed to be utilized. In case that a company is changing major parts of their code or their used data sets during the usage of the AI, the company has to get their AI examined again. Bug fixes and small changes that do not affect the functionality of the program do not have to be monitored.

However, for a transparent usage of AI, its workings have to be made accessible to the broad public. This can foster trust in AI and increase the acceptance of AI among people. Therefore, the company providing the AI should release a statement of use formulated in a way lays can comprehend. We also suggest that governments and stakeholders provide special classes and courses teaching lays the basics of AI so that they can further understand its working, advantages and downsides.

Nevertheless, if an AI does not work as intended, the company providing the AI has to be held accountable. It has to be chargeable if a company is not letting it's AI be reviewed or make their program available without publishing a statement of use. Moreover, it has to be ensured that the testing authorities constantly monitor and evaluate the AI thoroughly. If an AI contains bias or comes to the wrong conclusions, the company has to report this to the authorities and make such failures public. Only by publication of these issues, people harmed by these wrong decisions can become aware of the situation and act accordingly.

Nevertheless, if an AI does not work as intended, the company providing the AI has to be held accountable. It has to be chargeable if a company is not letting it's AI be reviewed or make their program available without publishing a statement of use. Moreover, it has to be ensured that the testing authorities constantly monitor and evaluate the AI thoroughly. If an AI contains bias or comes to the wrong conclusions, the company has to report this to the authorities and make such failures public. Only by publication of these issues, people harmed by these wrong decisions can become aware of the situation and act accordingly.

Member states as guarantors of fundamental rights and freedoms should uphold digital sovereignty to ensure protection of human rights as against AI in their laws, policies and regulations through its agencies, from the different actors within their state and its borders, especially in light of the digital economy and AI.

Data localization and splinternet

In a dispensation where ubiquitous computing and troves of data gathering is the norm, states are responding to this phenomena by asserting the idea of data sovereignty through data localisation.



Definition

Data Localisation has been saddled with different definitions and forms but in essence, it involves efforts to keep data within national borders by putting barriers to the free flow of information. It aims at both data ‘at rest’ and ‘in transit’

Motivating factor

States have proposed data localisation measures as an effort to address concerns of privacy, security, surveillance, and law enforcement

What is at Stake

ISOC through its “Internet way of Networking Project” mapped out critical properties that define the functioning of the internet and how mandatory data localization impacts the Internet Way of Networking.

The project highlighted the following:



If the trend towards data localization continues, it will create a more constricted and less resilient network, retrofitted to comply with national borders. Businesses will have to narrow their choices and capabilities, and network operators may be forced to use uneconomic and less resilient ways to route traffic. Cybersecurity may suffer as organizations are less able to store data outside borders with the aim of increasing reliability and mitigating a wide variety of risks including cyber-attacks and national disasters. Countries trying to forcibly localize data will impede the openness and accessibility of the global Internet. Data will not be able to flow uninterrupted on the basis of network efficiency; rather, special arrangements will need to be put in place in order for that data to stay within the confines of a jurisdiction. The result will be increased barriers to entry, to the detriment of users, businesses and governments seeking to access the Internet. Ultimately, forced data localization makes the Internet less resilient, less global, more costly, and less valuable.



Data localization laws, such as those considered in India and Vietnam, typically target the processing and use of specific categories of personal and business information at the application level of the Internet, for example, cloud computing applications. They do not target the Internet's infrastructure providers directly by requiring traffic passing through networks to conform to national borders. However, countries with more extreme data sovereignty or localization policies, such as China and Russia, could at their most extreme impose policies that seek to restrict data flows. So, while data localization policies focusing on commercial and personal data do not directly create barriers to networks joining the Internet, by adopting its common protocols, they are a step in that direction on the most visible application layer, and may lead to fragmentation at the infrastructure level if the trend continues.




The Internet is a “network of networks” with no centralized control or coordination. Although there is a range of approaches to data localization, it means policy measures would concentrate on the services and application layer of business decisions of how to process personal and commercial data. As such, localization may require Internet intermediaries to impose additional requirements on routing policy. Depending on how extreme the data localization policy is, it may impact how information is transmitted between networks, including the goals of reducing latency, providing redundancy and replication to distribute data closer to its destination, and other threatening basic traffic engineering and traffic-optimization goals. This would reduce network operators’ routing autonomy and their ability to optimize connectivity. Overall, aligning routing policy with the requirements of different jurisdictions creates needless complexity and inefficiency, as routing would no longer serve the technical requirements of connectivity, resilience and optimized flow.




Harsher data localization regimes would bring a greater need for coordination between companies and governments to determine what data networks are carrying, and between networks to ensure specified traffic flows follow national borders. Any additional requirements based on all operators understanding the nature of the data/content would make the network more specialized and less general purpose, needing additional functionalities such as deep packet inspection, and would more narrowly prescribe the functions of networks overall. The loss of simplicity and basic functionality at the Internet’s transit layers caused by data localization measures would make networks more complex and less efficient, with an increased need for coordination. This would undermine the Internet’s model of permissionless innovation and create barriers to entry for new network operators and Internet infrastructure providers.

Possible Solutions



Alternative data governance approaches; viewing data governance in the lens of its potential to affect other people



Creating trusts and unique data governance between:

- a) People and Government
- b) Companies and People and
- c) Companies and Governments

References

1. Anupam Chander, Uyên P. Lê, 'Data Nationalism', Emory Law, Journal (Vol. 64, 2015)
2. Anupam Chander, 'Is Data Localization a Solution for Schrems II?' Journal of International Economic Law, 2020, 23, 1–14.
3. ISOC, Internet Way of Networking Use Case: Data Localization
4. Freedom House, "User privacy or Cyber sovereignty"
5. W. Kuan Hon, 'Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens'
6. Scott Malcomson, 'Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web'.



**YOUTH
INTERNET
GOVERNANCE
FORUM**

German Informatics Society

Office Berlin
Spreepalais am Dom
Anna-Louisa-Karsch-Str. 2
10178 Berlin

E-Mail: mail@yigf.de
 [/YouthIGFSummit](https://twitter.com/YouthIGFSummit)
Web: <https://yigf.de/>

Authored by
Working Group Sustainable
Internet Governance

Supported by:



GERMAN
INFORMATICS SOCIETY



Federal Ministry
for Economic Affairs
and Energy

on the basis of a decision
by the German Bundestag