NURTURING SUSTAINABLE DIGITAL DIALOGUE FOR A MULTIPOLAR WORLD

Miloš Jovanović

IN recent years, the digital environment has experienced a paradigm change, emphasizing the need of countries to preserve their national digital space, and safeguarding their digital sovereignty. Concerns regarding ordinary users' rights and the role of nation states on the global Internet have arisen as a result of multinational corporations' expanding power and the risk of Internet fragmentation. As a result of these concerns, the concept of sustainable digital conversation has emerged, stressing a human centered approach to digitalization, and fostering cross-national collaboration. This article investigates the relevance of technical sovereignty, artificial intelligence (AI) governance, and finding the right balance between globalization and fragmentation.

As Paul Grant explains in his 1983 essay for *Prometheus* magazine entitled "Technological Sovereignty: Forgotten Factor in the 'Hi-Tech' Razzamatazz," technological sovereignty is defined as "the capability and the freedom to select, to generate or acquire and to apply, build upon and exploit commercially technology needed for industrial innovation." This notion of sovereignty can apply not only to states but also to companies. Technological sovereignty refers to the efforts of nations and/or countries to create technologies that reduce American control over, and surveillance of, technological systems, including the Internet and use of AI in various ways like manipulating data, public opinion, and so on. It involves protecting the sovereignty of states and their citizens through the passing of laws and the development of "national" or domestic technologies. The concept of technological sovereignty is often discussed in relation to the changing role of state sovereignty in the digital age.

Miloš Jovanović is President of the OpenLink Group, an IT development corporation, and an Assistant Professor at the Metropolitan University in Belgrade, Serbia. You may follow him on X @milos002.

Data security as digital sovereignty's crucial pillar

Source: Guliver Image

Grant also criticizes Australia's failure to recognize the importance of technological sovereignty when migrating to technology-intensive activities. This emphasizes the significance of technological sovereignty in ensuring a nation's ability to develop and exploit acquired technology without contractual or legal constraints. Furthermore, the revelations of mass surveillance by Edward Snowden and Wikileaks have prompted many countries to prioritize the protection of their collective sovereignty and that of their citizens through the development of domestic technologies. For example, Germany has made efforts to counter U.S. surveillance of Angela Merkel's phone and email conversations.

This demonstrates the importance of technological sovereignty in safeguarding a nation's control over its technological systems and reducing external control and surveillance. Russian President Vladimir Putin, for example, has warned the citizens of Russia during one of his public addresses that the country that leads in technologies using artificial intelligence will dominate the globe: "Artificial intelligence is the future, not only for Russia, but for all humankind. It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world."

In addition, in his book *A Prehistory of the Cloud* (2015), Tong-Hui Hu argues that the sovereignty of nation states is reaffirmed digitally when they exercise their prerogative power to control entire populations' access to the Internet. This highlights the role of technological sovereignty in enabling nation states to assert control over the flow of information and maintain their authority in the digital realm. Importance of technological sovereignty is also seen in a need to protect personal data and solve privacy issues, because data went from being simple aspect of storing information on some medium to instruction for AI algorithms, which is enough to determine protective actions. Overall, technological sovereignty is important in the digital era, as it allows nations to protect their interests, reduce external control, and maintain control over their technological systems and information.

Technological sovereignty refers to the efforts of nations and/or countries to create technologies that reduce American control over, and surveillance of, technological systems, including the Internet and use of AI in various ways like manipulating data, public opinion, and so on.

Addressing challenges to national digital space can be complex and multifaceted. One of them is dominance of big technological companies, which have established their legitimacy and occupy a significant role in Internet governance. There is also another potential risk of AI interventions both foreign and within the system in various manners like data privacy, human rights, different policies etc. These challenges may also include the development of stable system infrastructures, regulatory frameworks, and ensuring inclusivity in digital transformation efforts. In a September 2019 article for *The Statesman*, Ishan Joshi also warns of "loss of traditional employment sectors […] causing a spike in cybercrimes and according to some, promoting deracinated, atomized existence of human beings." Joshi further quotes Malaysian-born economist Andrew Sheng, who wrote for *Asia News Network* that "no economy today can afford to be complacent […] We need a root-and-branch review of how to compete in a complex digital world."

Overall, there are four categories of challenges and opportunities. Those are: technical, business and organizational, legal compliance, and national and regional challenges. Under technical challenges there are sharing by design, digital sovereignty, decentralization, security, veracity and privacy protection, some of which have been previously mentioned.

AI and its Implications for Technological Sovereignty

AI has the potential to exert large influence on a wide range of businesses and areas, including "finance, healthcare, manufacturing, retail, supply chain, logistics, and utilities"—as laid out by Yogesh Dwivedi et al in a 2021 paper for the *International Journal of Information Management*. The fast development of AI technology brings with it both benefits and difficulties. On the one hand, AI allows new technologies that boost efficiency and production. On the other hand, it may raise disparities between and within nations, impeding the accomplishment of objectives.

The influence of AI on national identities and nationalism has received little attention, although the AI-driven "transformation of individuals into demographic data" is causing changes in state sovereignty, as J. Paul Goode notes in his 2020 essay "Artificial Intelligence and the Future of Nationalism" for *Nations and Nationalism*. The policy and strategy of countries and unions in the field of AI vary. The Eurasian Economic Union members, for example, focus on external technologies and investments, creating hotbeds of technological growth. China, on the other hand, is one of the world leaders in AI technologies, with substantial investment, achievements in computing infrastructure, and high patent and publication activity. Russia also aims to become a global leader in digital and technological development, utilizing its "scientific, political, economic, regulatory, and social resources," as Alexei Kolyanov of the St. Petersburg Electrotechnical University observes. The development of AI technologies is closely linked to ensuring national digital sovereignty, and the level of legal regulation should meet the demands of the present time.

The revelations of mass surveillance by Edward Snowden and Wikileaks have prompted many countries to prioritize the protection of their collective sovereignty and that of their citizens through the development of domestic technologies.

The benefits of AI in various sectors have been widely recognized. In the financial services industry, AI has contributed to the increased efficiency of processes and improved customer experiences. In agriculture, AI has the potential to address sustainability challenges and help achieve climate and biodiversity targets. In the healthcare industry, AI promises benefits but also poses challenges in terms of its impact on health professionals, organizations, and governments. AI also offers benefits in terms of digital financial inclusion, of which South African scholar David Mhlanga emphasizes access to formal financial services, lower transaction costs, and reduced risks of financial crimes. Along with these benefits, there are also potential risks associated with AI. The risks of AI in the public sector are relatively few compared to the extensive benefits highlighted. The discourse often focuses on the increased efficiency of public sector processes without explicitly considering the "risks to efficiency" that AI may pose; as Daniel Toll, Ida Lindgren, and researchers note in their 2020 study named "Values, Benefits, Considerations and Risks of AI in Government: A Study of AI Policy Documents in Sweden." In the context of digital online experiences, the use of AI presents significant sociotechnological risk scenarios, particularly in terms of privacy and security concerns. The use of AI in the agricultural sector also requires a reliable legal framework to address issues related to product liability, data privacy, and data security. Additionally, the dissemination of AI in the consumer society may lead to unemployment and increasing socio-economic stratification, as Pankratov, Morozov et al argue in "Digital Assistants in the Consumer Society: Global Trends and Vectors of Russia's Development."

The Role of AI Regulation

The role of AI regulation is crucial in ensuring the responsible and ethical development and use of artificial intelligence technologies. The fast development of AI necessitates appropriate policy and regulation to address potential gaps in transparency, accountability, safety, and ethical standards. Without proper regulation, there is a risk of detrimental effects on the development and sustainable use of AI.

While AI can support the achievement of many targets related to the Sustainable Development Goals (SDGs), it can also hinder the achievement of certain targets, such as by exacerbating inequalities among and within countries.

The need for AI regulation to ensure technological sovereignty arises from several key factors. Firstly, the rapid development and deployment of AI technologies have the potential to bring about both positive and negative impacts on various aspects of society, including sustainable development. While AI can support the achievement of many targets related to the Sustainable Development Goals (SDGs), it can also hinder the achievement of certain targets, such as by exacerbating inequalities among and within countries. Therefore, appropriate policy and regulation are necessary to ensure that AI development aligns with sustainable development objectives and does not undermine societal goals.

Secondly, the uncontrolled deployment of AI can create risks and challenges that need to be addressed through regulation. AI technologies, if not properly regulated, can lead to gaps in transparency, accountability, safety, and ethical standards. For example, AI systems may lack transparency in their decisionmaking processes, making it difficult to understand and address potential biases or discriminatory outcomes. Additionally, the use of AI systems may raise concerns about privacy and data protection, as these systems often rely on large amounts of personal data. Therefore, regulation is needed to establish clear guidelines and standards for the development, deployment, and use of AI technologies to ensure transparency, accountability, and protection of individual rights.

Without proper regulation, countries may become dependent on foreign AI technologies, which can have implications for national security, economic competitiveness, and the protection of citizens' rights and interests.

Furthermore, the governance of emerging technologies like AI requires the involvement of multiple stakeholders and the establishment of governance mechanisms. The regulation of AI should involve collaboration between governments, industry, academia, and civil society to ensure that the interests and perspectives of all stakeholders are taken into account. This multi-stakeholder approach can help address the complex ethical, legal, and social implications of AI technologies and ensure that regulation is comprehensive and effective.

The regulation of AI is crucial for maintaining technological sovereignty. Technological sovereignty refers to a country's ability to "develop, control, and govern its own technologies," as defined by Steven Globerman and the Science Council of Canada (1977). Without proper regulation, countries may become dependent on foreign AI technologies, which can have implications for national security, economic competitiveness, and the protection of citizens' rights and interests. Therefore, AI regulation plays a vital role in safeguarding a country's technological sovereignty by ensuring that AI technologies are developed and used in a manner that aligns with national interests and values.

Balancing innovation, ethics, and accountability in AI regulation requires appropriate policy and regulation, ethical governance, clear regulations, and the use of experimental regulatory frameworks. These measures are essential to ensure transparency, accountability, safety, and ethical standards in the development and deployment of AI technologies. Ethical principles such as accountability, privacy, fairness, and transparency should guide the design and governance of AI systems.

Sustainable Digital Dialogue: A Human Centered Approach

In recent years, there has been an increasing interest in supporting long-term digital dialogue, which refers to the use of digital technology to allow meaningful and constructive dialogues between individuals and groups. This approach highlights the relevance of human centered design concepts in the creation and implementation of digital discussion platforms, which prioritize user requirements and experiences. The implementation of inclusive design techniques is an important part of long-term digital discourse. Inclusive design strives to make digital discourse platforms accessible and usable by people of all backgrounds, skills, and preferences. Language barriers, visual impairments, and cognitive limitations are all variables to consider. Digital discussion platforms may build a more inclusive and equitable online environment by adopting inclusive design principles, allowing all persons to engage and contribute to the discourse.

The promotion of ethical and responsible use of digital technologies is another crucial part of long-term digital conversation. Addressing challenges such as privacy, data security, and algorithmic bias are all part of this. Digital dialogue platforms should prioritize user data safety and provide users control over their personal information. Platforms should also be clear about their data collecting and usage procedures, as well as take steps to reduce the possibility of algorithmic bias and prejudice. Furthermore, sustainable digital dialogue requires ongoing engagement and collaboration with users. This means actively seeking feedback and input from users and incorporating their perspectives into the design and development process. By involving users in the decisionmaking process, digital dialogue platforms can better meet their needs and preferences and create a more engaging and meaningful user experience. Sustainable digital dialogue refers to the use of digital platforms and technologies to facilitate ongoing, inclusive, and respectful conversations that promote collaboration and respect for users' rights. It involves creating an environment where diverse perspectives can be shared, and where participants can engage in meaningful discussions that lead to positive outcomes. Sustainable digital dialogue fosters collaboration by providing a platform for individuals to come together, exchange ideas, and work towards common goals. It allows for the co-creation of knowledge and the development of innovative solutions. By promoting open and inclusive dialogue, sustainable digital dialogue also ensures that users' rights, such as freedom of expression and privacy, are respected.

One of the possible advantages of long-term digital discourse is the possibility to promote technical sovereignty. The ability of a country or region to develop and govern its own technologies, independent of foreign influences, is referred to as technological sovereignty. By encouraging local innovation and information sharing, sustainable digital discourse can contribute to technical sovereignty. It enables the interchange of ideas and knowledge within a community, which can lead to the development of locally appropriate and long-lasting technical solutions. Stakeholders can work together to enhance their own technological capabilities and reduce reliance on foreign technologies by engaging in communication and collaboration. Achieving long-term digital dialogue is critical for developing collaboration and respect for users' rights. It provides a forum for different points of view to be expressed and important dialogues to take place. Sustainable digital dialogue promotes open and inclusive dialogue, which helps to build creative solutions and knowledge co-creation. Furthermore, it has the ability to promote technical sovereignty by encouraging local innovation and decreasing reliance on foreign technologies. However, further research is required to fully comprehend the impact and potential benefits of sustained digital discourse in a variety of scenarios.

> *Implementing stringent data protection laws is one method to achieve a compromise between user rights and business interests. These rules may offer businesses a framework for the appropriate and open collection and use of user data.*

Ensuring User Rights & Balancing Corporate Interests

Maintaining user rights while balancing corporate interests is a complicated and diverse undertaking that necessitates careful consideration of numerous issues. On the one hand, it is critical to safeguard users' rights and privacy, ensuring that their personal information is secure and that they have a choice over how their data is used. Companies, on the other hand, have a legitimate interest in collecting and analyzing user data in order to improve their products and services and make revenue via targeted advertising. Implementing stringent data protection laws is one method to achieve a compromise between user rights and business interests. These rules may offer businesses a framework for the appropriate and open collection and use of user data. For instance, the European Union's General Data Protection Regulation (GDPR) has established stringent guidelines for the gathering, storing, and use of personal data. Companies that conduct business in the EU must seek consumers' explicit consent before collecting personal data and must be transparent about the data's intended use. Companies can take proactive initiatives to preserve user rights in addition to regulatory ones. This may entail putting in place robust security measures to stop data breaches as well as giving consumers access to tools and choices to manage their privacy settings. Social networking platforms, for instance, can provide users with the choice to choose who can view their posts and personal information as well as to opt out of targeted advertising.

In the digital age, user rights must be protected at all costs. This involves defending personal information, safeguarding freedom of speech, encouraging fair Internet access, and boosting online safety.

Additionally, businesses might apply a more moral method of gathering and using data. This may entail being open and honest with users about how their data is being used as well as requesting their opinions on privacy practices and data rules.

Safeguarding User Rights

Protecting user rights is more crucial than ever in the digital age, therefore it is necessary. The right to privacy is one of the most important user rights that needs to be protected. Users ought to be in charge of their personal data and have control over how it is gathered, utilized, and shared. This involves safeguarding private communications, financial information, and medical records. To prevent illegal access to and misuse of personal information, governments and organizations should enact strict data protection laws and regulations. The right to freedom of speech is a crucial user right. People can share their opinions and ideas in the digital age on a variety of online channels. To ensure that this right is not violated, nevertheless, is necessary. Governments should not ban or monitor people's online activities, and neither should Internet service providers. They ought to advocate for a welcoming, open environment online where different points of view can be voiced. The ability to use and access the Internet should also be included in user rights in the digital age.

For communication, education, and information access, the Internet has emerged as a crucial resource. Thus, it is essential that everyone gets access to the Internet on an equal basis and at a reasonable cost. Governments and institutions ought to endeavor to eliminate the digital divide and guarantee that everyone has access to the Internet. Additionally, the right to online security should be included in user rights. Users need to be safeguarded from these dangers due to the rising incidence of cyberthreats such as hacking, identity theft, and online fraud. To protect user data and guarantee the integrity of online transactions, governments and companies should invest in strong cybersecurity measures. In the digital age, user rights must be protected at all costs. This involves defending personal information, safeguarding freedom of speech, encouraging fair Internet access, and boosting online safety. To protect these rights and foster an inclusive and safe online environment, governments, organizations, and people all have a role to play.

One of the key challenges in balancing globalization and digital sovereignty is the risk of information imperialism and digital colonialism.

Globalization vs. Fragmentation: Finding the Right Balance

The tension between globalization and the need for safeguarding national digital sovereignty is a complex issue that involves considerations of power dynamics, cultural imperialism, and the balance between collaboration and protection. Globalization, characterized by the increasing interconnectedness and interdependence of countries and societies, has brought numerous benefits such as economic growth, technological advancements, and cultural exchange. However, it has also raised concerns about the erosion of national sovereignty and the dominance of powerful nations or corporations over smaller or less developed countries, as Australian author Monique Mann repeatedly points out in a 2018 paper "(Big) Data and the North-in-South: Australia's Informational Imperialism and Digital Colonialism." This is particularly evident in the context of digital technologies and data practices. One of the key challenges in balancing globalization and digital sovereignty is the risk of information imperialism and digital colonialism. Powerful countries, particularly those in the Global North, may exploit their technological dominance to perpetuate colonial practices and exert control over less powerful nations in the Global South. This can manifest in various ways, such as the extraction of data from developing countries without their consent or fair compensation, the imposition of Western norms and values on digital platforms, and the concentration of power in the hands of a few global tech giants.

Finding the right balance between globalization and safeguarding national digital sovereignty requires a comprehensive and coordinated global approach. This involves promoting inclusive and equitable digital governance frameworks that respect the rights and interests of all nations, particularly those in the Global South. It also requires empowering countries to exercise control over their digital infrastructure and data through initiatives such as Indigenous Data Sovereignty. Additionally, international cooperation and collaboration are crucial in addressing common challenges and ensuring that the benefits of globalization are shared more equitably.

The Path to Sovereignty (and its Pitfalls)

In establishing a multipolar world in the digital age, developing technological sovereignty and fostering sustainable digital communication are essential. In order to safeguard national interests, lessen external control, and retain control over their technical systems and information, states must have technological sovereignty, which is described as the capacity to create and regulate their own technologies. The value of technological sovereignty is evident in efforts to protect personal information, preserve national digital spaces, and deal with issues brought on by AI interventions and hegemonic multinational businesses.

As its impact on societies increases, AI plays a vital role in technological sovereignty. While addressing possible hazards and problems through appropriate regulation, the creation and application of AI technology should be in line with sustainable development goals. For AI development to be transparent, accountable, safe, and ethical while maintaining technical sovereignty, AI regulation is essential. The cooperation of numerous parties and the implementation of governance structures are necessary to strike a balance between innovation, ethics, and accountability in the regulation of AI. Forging collaboration, upholding user rights, and fostering technological sovereignty all depend on sustained digital dialogue that is characterized by ongoing, inclusive, and respectful conversations. It enables knowledge and idea exchange within communities, fostering local innovation and lowering reliance on foreign technologies. Human-centered design ideas, inclusive design principles, and the ethical and responsible use of digital technologies should be given top priority in any sustainable digital dialogue.

It is crucial to respect users' rights, such as privacy and data protection, while acknowledging the legitimate business objectives of corporations, when attempting to strike a balance between user rights and corporate interests. Setting up strict data privacy regulations, like the GDPR, can offer a framework for the proper gathering and use of user data. Businesses can also actively protect user rights by putting in place robust security measures, giving customers the means to control their privacy settings, and pursuing more moral data gathering and usage procedures.

The establishment of technological sovereignty is a key component of the overall national sovereignty of each state. In the light of geopolitical tensions and with the goal of establishing a multipolar world, the key question is how to ensure one's own production of hardware, without which it is not possible to ensure technological sovereignty. Given the situation with the production of microchips in the world—the limited transfer of technology considered critical for each country—the key focus of each sovereign nation must be placed on the production of its own microarrays and microchips for commercial use with a focus on relying on its own forces and friendly scientific partners community. Additionally, the development and assurance of technological sovereignty cannot be achieved without adequate cryptological mechanisms, and the application of digital certificates issued by national certification bodies. The perspective also brings progress in the development of quantum cryptography, where we use quantum mechanics, that is, quantum physics, to enable secure communication. In essence, we are talking about the creation of an information sequence that is known only to the communicating parties and that can be used as a key for encryption and decryption of messages where the ability of communicating users to detect the presence of a third party comes into play. This is extremely important for adequate protection of the communication channel. In the end, it is necessary to create a national technological ecosystem with its own products that would represent a closed circle of hardware-software-cryptological mechanisms at the protocol level, and it is especially important at the legislative level to establish redundant systems and a high level of control of the critical infrastructure of the national space.