• Article •

Interpreting the Global Digital Compact: Charting a New Vision Towards a Multi-Stakeholder Governance Model

Qifan Jiang[1], Yuhang Ma[2*]

[1] Leiden Law School, Leiden University, Leiden, The Netherlands; School of International Law, East China University of Political Science and Law, Shanghai, China

[2] Leiden Law School, Leiden University, Leiden, The Netherlands

[*] Corresponding Authors: Yuhang Ma. Email: mayuhang0308@163.com

Received: 9 November 2024 Accepted: 29 November 2024 Published: 25 February 2025

Abstract: The "Global Digital Compact" (GDC) published by the United Nations highlights that "multi-stakeholder" actors are the implementers of this compact, serving as a breakthrough for interpreting it. The multi-stakeholder governance model can effectively regulate the Internet; however, the roles played by various stakeholders differ significantly in practice, with governments and enterprises often dominating Internet governance while civil society remains in a disadvantaged position. The stakeholders referenced in GDC are not limited to governments and enterprises; civil society emerges as a third core stakeholder in the digital age, with its interests articulated as fundamental values of digital human rights. Based on this value order, the implementation of the multi-stakeholder governance model in GDC can be reflected in both horizontal and vertical interactions between the other two stakeholders: horizontal interactions aim to establish an international digital cooperation framework among governments through treaties and agreements, bridging the international digital divide between developed and developing countries, forming international standards for artificial intelligence governance, and promoting the sharing of technology and knowledge; vertical interactions aim to create a meta-regulatory relationship between governments and enterprises, achieving interaction and coordination between self-regulation and government regulation through risk assessment mechanisms and diverse accountability mechanisms.

Keywords: Global Digital Compact; Multi-Stakeholders; Digital Human Rights; Global Governance

1. Introduction

"It was the best of times, it was the worst of times." There is no doubt that digital technology is changing society and people's lifestyles in both breadth and depth, but while it has brought rapid development opportunities to the world, it has also created many problems. For example, there are a series of challenges such as privacy and personal information protection issues at the individual level,

digital platform monopolies and the problem of big data raising prices for frequent users at the corporate level, and automated decision-making and the digital divide at the national level. Under the backdrop of the digital age, the UN Secretary-General's report Our Common Agenda released in September 2021 proposed that an agreement on GDC be reached at the Future Summit to be held in 2023 (now postponed to 2024), with a view to building an open, free and secure digital future for all people in the world.

From the perspective of international law, the legal influence of GDC is currently unclear. To be more specific, the Compact has not come into force under international law, but merely an initiative document issued by the United Nations to promote international digital governance. However, despite its lack of effectiveness, it does not deny the forward-looking role of the document in future global digital regulation and governance. In particular, by influencing national legislation and international treaty negotiations, its pioneering and inspiring framework for promoting global digital governance will indirectly have an impact on future global digital governance.

GDC seeks to address fragmented digital governance and foster cooperation across various entities, establishing "multi-stakeholders"—Member States and Stakeholders (including digital platforms, private sectors, alliances, and civil society organizations)—as the core actors. This model builds on the multi-stakeholder governance concept introduced at the 2003 World Summit on the Information Society, which emphasized decentralization and inclusivity. By encouraging a collaborative approach among governments, private sectors, and civil society, the GDC envisions an "open, free, secure, and people-oriented" digital future. Achieving this vision, however, depends on recognizing civil society's vital role within global digital governance, beyond mere symbolic inclusion, to ensure a robust, interactive framework for digital governance in the modern era.

2. Literature Review

GDC aims to address the fragmented landscape of digital governance by promoting a multi-stakeholder approach that includes governments, private sectors, and civil society. The GDC emphasizes cooperation among these groups, with member states primarily responsible for implementation, supported by stakeholders such as digital platforms, private entities, and civil organizations. This shift away from centralized governance models seeks to decentralize and democratize digital governance, enabling a more participatory framework that integrates diverse voices.

The concept of multi-stakeholder governance in digital policy was first formalized in the 2003 World Summit on the Information Society (WSIS) Geneva Plan of Action. The Tunis Agenda of 2005 further established this approach by defining distinct roles for governments, the private sector, and civil society. Over time, the model has evolved to challenge the U.S.-centric governance of the Internet, especially after the 2013 Snowden revelations, which intensified calls for ICANN's transition to a multi-stakeholder model. In response, the U.S. Department of Commerce began a phased relinquishment of its control, underscoring the importance of shared governance. This shift marked a significant step toward a globally inclusive Internet governance system.

The GDC reinforces the significance of a multi-stakeholder approach, recognizing that achieving an open, secure, and inclusive digital future necessitates balancing power among entities and empowering civil society as a full partner in governance. Existing literature critiques the dominance of governments and businesses in regulatory roles, often marginalizing civil society's input. GDC's framework, therefore, represents an opportunity to reimagine digital governance by embedding civil society's role more centrally, advocating for digital human rights and collaborative policymaking that aligns with the needs of all stakeholders.

3. The Transmutation of Civil Society in the History of Internet Governance

As shown earlier, civil society stands merely no position in the "multi-stakeholder" governance model, which has largely prevented the "multi-stakeholder" governance model from achieving its purpose in global digital governance. In fact, there has been a process of transmutation in the role of civil society in Internet governance. The logic of civil society's decline in the multi-stakeholder model can only be understood in the context of historical evolution. Overall, since the born of Internet, it has gone through three stages: the period of "civil society autonomy", the period of "cyber sovereignty" of countries with the United States at the core, and the period of global governance represented by "multi-stakeholder".

3.1 Civil Society Autonomy: Utopia in Cyberspace

The ARPANET, the Internet's precursor, emerged during the Cold War era of the 1960s and 1970s. The U.S. Defense Advanced Research Projects Agency funded its development to secure military communication systems against potential Soviet attacks. Initially, ARPANET management was handled by several organizations: the Internet Configuration Control Board (ICCB) in 1979, followed by the Internet Advisory Board (IAB) in 1983, the Internet Activities Board (also IAB) in 1986, and the Internet Engineering Task Force (IETF). The IETF remained the primary body overseeing Internet governance until 1998.

The IETF is neither a government agency nor an international organization. It is merely a loosely organized group of engineers dedicated to Internet technology. These engineers mostly hold a political orientation of the New Left, which rejects government regulation and advocates independence and freedom. Their core belief in terms of Internet governance is that cyberspace should be independent from government and corporate intervention, so as to realize the free nature of the Internet. Obviously, this view implies that the Internet is not only the object of governance, but also the subject of governance. That is, civil society on the Internet can achieve self-government without the supervision and intervention of governments and businesses. It can be seen that the concept of "civil society autonomy" originated from the trend of freedom supreme at the birth of the Internet.

The concept of "civil society autonomy" reached a milestone in 1996. In that year, John P. Barlow, known as the "Jefferson of Cyberspace", issued "A Declaration of Independence of Cyberspace" at the Davos Forum in Switzerland and Proclaiming that cyberspace should be free from government control and should be autonomous. "A Declaration of Independence of Cyberspace" separates civil society on the Internet from the physical world, arguing that the former has its own culture, ethics and laws, and can achieve self-governance without the intervention of power from the physical world, thus codifying the concept of "civil society autonomy".

The concept of "civil society autonomy" represented by A Declaration of Independence in Cyberspace was also supported by the US judiciary at the time. In the case American Civil Liberties Union v. Reno (hereinafter referred to as the "Reno" case), a group of engineers represented by Barlow appealed to the Supreme Court to protest against the Communications Decency Act enacted by the US Congress in 1996. This law was the first attempt by the US government to regulate the Internet through legislation, and some of its provisions prohibit users from disseminating obscene information or materials to minors via the Internet, otherwise the disseminator may bear criminal liability. Barlow and others believed that the Communications Decency Act would lead to government suppression of freedom of speech in cyberspace and violate the independence of cyberspace. The US Supreme Court ultimately sentenced that the Communications Decency Act was invalid because it violated the "freedom of speech" of the First Amendment to the US Constitution, supporting the Internet as a democratic forum free from government regulation. In her concurrence, Justice O'Connor evoked the "masquerade" image that was very popular on the early Internet: on the Internet, no one knows you're a dog.

The Reno case legally confirmed the validity of the Declaration of Independence of Cyberspace and, to some extent, supported the idea of "civil society autonomy". At that time, the mighty "electronic American revolution" seemed to have succeeded.

3.2 Civil Society and Cyber Sovereignty: Autonomy and Heteronomy

As mentioned above, although the Internet's "civil society autonomy" has initially been recognized by the US government, the Internet has been closely related to politics since its inception (the Cold War between the United States and the Soviet Union). Therefore, as American constitutional scholar Sunstein said, "despite many people's claims that the Internet has been or should be free from government control, virtual space is no different from physical space. Regulation and the power of the government are still omnipresent."

Before 1998, the IETF, composed of engineers, dominated the management of the Internet. However, in the late 1980s, the US Department of Defense privatized the Internet domain name system through bidding, thus sharing control and management of domain names. It can be seen that although the United States has always maintained that the Internet does not belong to any single country, the US government has long held the notion of cyber sovereignty and has implemented governance measures on the Internet through various direct or indirect means. "Civil society autonomy" has become an ideal utopia (the ideal of autonomy), while the Internet is still under the control of national sovereignty (the reality of heteronomy).

Facing the control of internet sovereignty, the internet civil society group actively carrying out autonomous practices to resist. In the 1990s, with the commercialization of the internet, the regulation of internet market order (such as domain name registration) became even more important. The Internet Association is an autonomous institution representing the Internet community. At the same time, there has been a movement in society for "civil society autonomy". There is even a so-called "the Internet Constitution" in the private sector. Its preamble is based on the wording of the preamble to the US Constitution, and begins: "We, the people of the Internet community, in order to promote better collaboration between the various networks of the Internet, maintain a harmonious relationship between the networks, and ensure that all networks participating in the Internet can enjoy freedom and happiness, hereby enact and establish this constitution...."1 ISOC's efforts represent the practice of self-

government by the Internet civil society. However, the US government does not agree with the so-called self-government of the Internet community without a doubt, and has continuously made its clear position on maintaining control of the Internet clear through interviews with key ISOC figures.32 The violent conflict between civil society and network sovereignty came to an end with the submission of the Internet Society to the will of the US government, which ultimately established its comprehensive control over the Internet.

In 1998, a global organization called the Internet Corporation for Assigned Names and Numbers (ICANN) was formally established, comprising groups such as URL registration authorities, contact groups, academics, and representatives of interest groups. Under public pressure against the "American-centric" model of Internet governance, the US government announced in a white paper, which was released the same year, to would hand over the right to govern the Internet to ICANN. Thus, ICANN's "networked governance model" is activated.

ICANN's greatest feature is "multi-party participation." That is, ICANN's policy formulation process is a "multi-stakeholder model" involving "business stakeholders, civil society, the technical community, academia, Internet end users, and governments." It can be seen that civil society, which has been suppressed by cyber sovereignty, has been "revived" in the "multi-stakeholder" governance model.38 However, this governance model is neither simply "civil society autonomy" nor heteronomy centered on cyber sovereignty, but rather "co-governance" by multiple subjects.

3.3 Decentralization of Network Sovereignty: The Decline of Civil Society

It is worth noting that, while ICANN represents the "multi-stakeholder" governance model, it remains under U.S. government oversight. A memorandum of understanding between the U.S. Department of Commerce and ICANN outlines specific policy tasks for ICANN to carry out, with priorities and milestones that align with U.S. government interests. Thus, despite its global status, ICANN still significantly reflects U.S. national interests. When ICANN's agreement with the Department of Commerce ended on September 30, 2015, "multi-stakeholder" governance officially became the internationally recognized approach for global Internet governance.

Civil society has reshaped its new position in the "multi-stakeholder" governance model. The "multi-stakeholder" governance model is characterized by the diversification of governance entities, that is, the governance of the Internet is no longer simply "government-centralism" but reflects "regulatory pluralism" (government, business, civil society) in the digital age. This article will introduce regulatory theory for further development.

The conventional approach holds that classic bureaucratic "government regulation" can maximize the concentration of regulatory resources to achieve specific public policy goals. However, the limitations of the effectiveness of this "government regulation" have been criticized by academia. Its dominant flaw is that the centralized approach of concentrating power cannot effectively face the increasingly complex regulatory needs. The criticism of traditional regulatory theory is based on the assumption that regulatory resources are not only in the hands of the government which represents the power of the state but are also dispersed among various non-governmental entities in the government and society. In the era of Web 3.0 and big data, the data deluge is driving the digital transformation of almost all enterprises. In the process of transformation, the value of data (especially big data) is further revealed, and data has begun to appear on the market as a resource, becoming a recognized competitive advantage for enterprises.

In this case, there are two transformations of power relations: in the case of the enterprise and the government, data has become a regulatory resource for the enterprise, and these regulatory resources have given the enterprise a considerable degree of informal power. This informal power can even have a significant impact on the government's formal power order, i.e., the government and the enterprise share regulatory power. In the case of enterprises and civil society, although they are both non-governmental entities, there is still a significant gap in the regulatory resources they control. Which means, as the most dynamic market players, enterprises often also have a huge wealth advantage and information advantage, and the big data resources they control in the era of algorithms are obtained from users in civil society. The digital wave has further created a factual power gap between enterprises and civil society.

As a result, the theoretical (as shown in Figure 1 below) and practical (as shown in Figure 2 below) aspects of the "multi-stakeholder" governance model gradually became misaligned, and civil society gradually faded away in this misalignment: in the theoretical aspect, civil society, along with governments and businesses, exercised regulatory power as a mainstay of Internet governance. In the practical aspect, due to the huge gap in regulatory power with the government and enterprises, civil society's status as a governance entity has been formalized. At the same time, civil society itself has become the target of governance by the government and enterprises, that is, it has been"objectified" (externalized).

Figure 1: Theoretical Aspects of the Multi-Stakeholder Governance Model

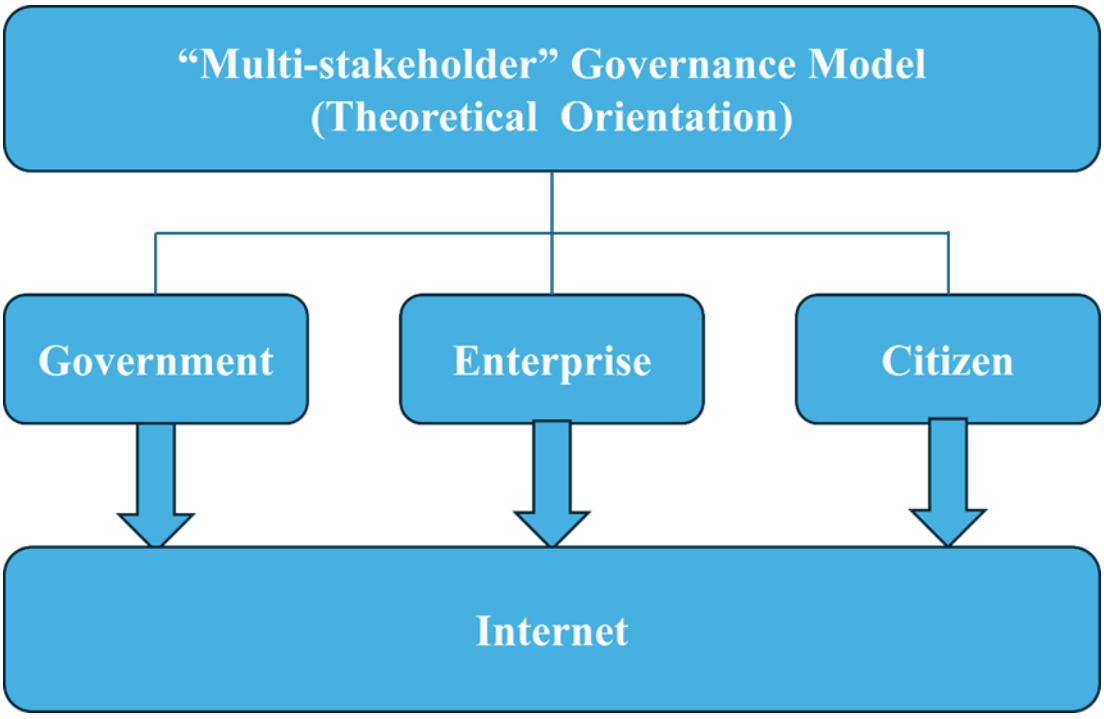
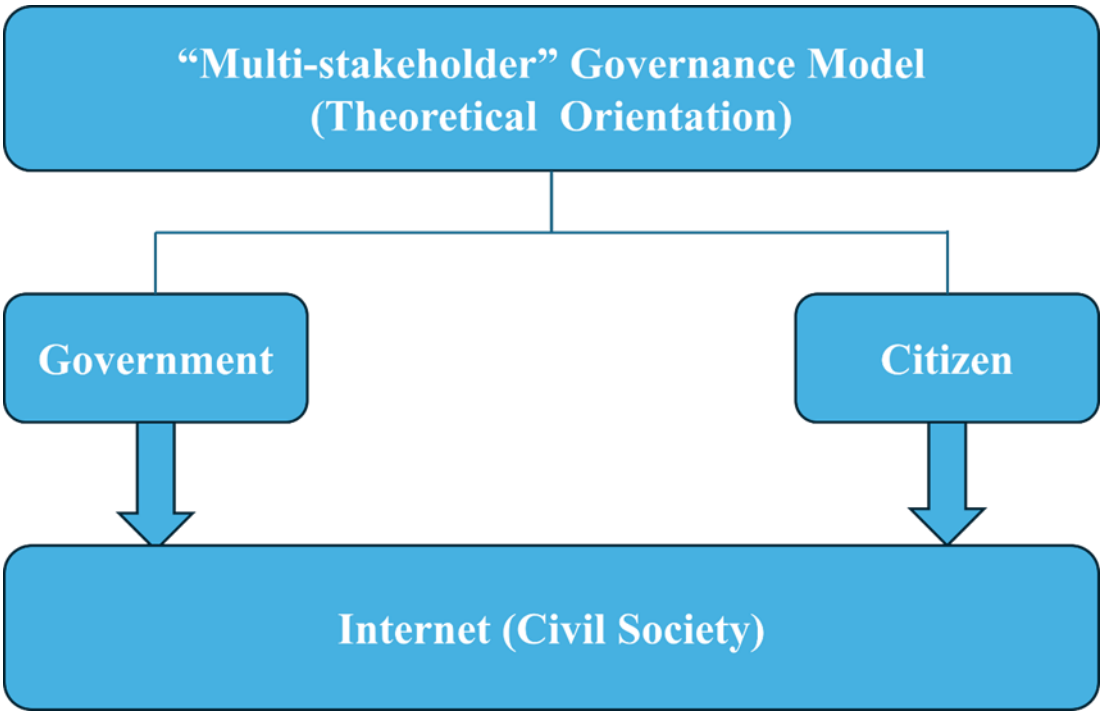


Figure 2: Practical Orientation of the Multi-Stakeholder Governance Model



4. The Global Digital Compact's Revival of the Idea of Civil Society

Civil society, which is gradually fading away, needs to be revitalized in the digital age, thereby realizing a new picture of the "multi-stakeholder" governance model. In this regard, an interpretation of the times for GDC will be crucial.

To "revive" civil society in the digital age, it is necessary to return to the value basis of this group. Civil society on the Internet represents the public interest of the vast number of Internet users, and this public interest is generally represented in practice by civil organizations with public welfare. However, compared with governments and enterprises, which have huge regulatory resources, civil organizations are often unable to advocate for the public interests they represent. Therefore, to change this situation, it is necessary to transform the form of representation of civil society's interests.

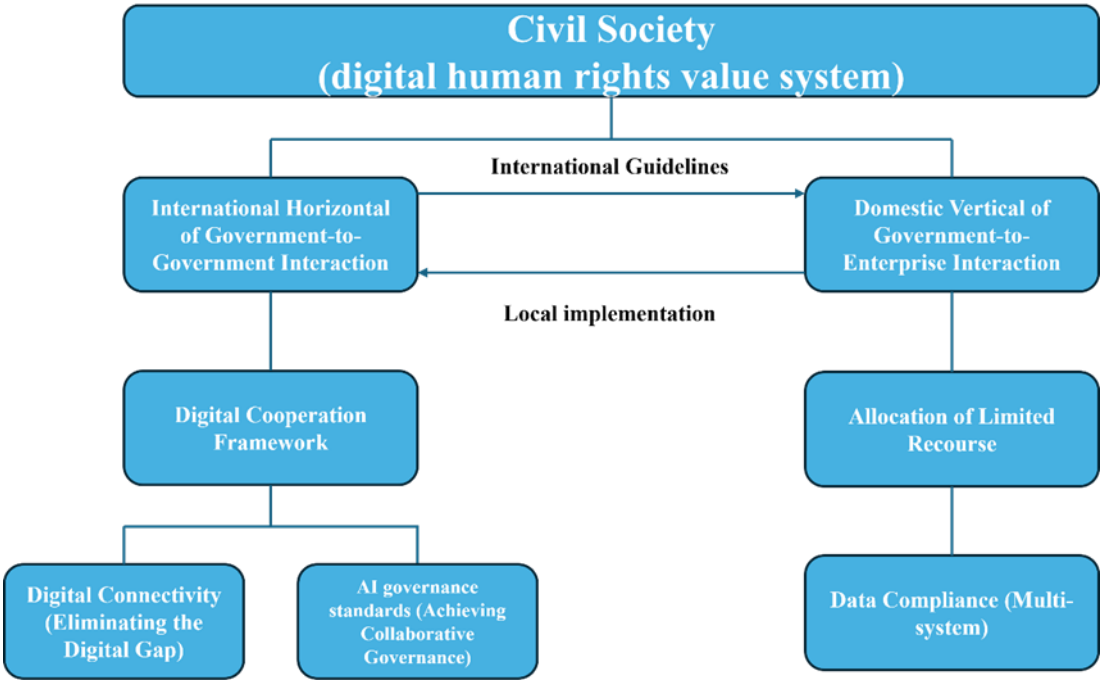
Take the basic constitutional rights as an example. It has undergone a conceptual shift from "negative protectionism" to "positive protectionism" in the macro sense. The former advocates that the public power of the state should not interfere with citizens' exercise of basic rights, while the latter advocates that the public power of the state should take the initiative to provide material assistance and support for citizens to exercise their basic rights. When people see the protection of the interests of civil society on the Internet, what civil society in the "multi-stakeholder" governance model wants is the right to actively govern the Internet. The vast number of Internet users can participate in the formulation and implementation of Internet rules, thus achieving a certain degree of autonomy. Therefore, the interests of civil society require a "positive protectionism" protection concept, and the governments and enterprises outside civil society that enjoy a lot of regulatory power need to assume the obligation to protect the interests of civil society.

Therefore, the further question is: what is the basis for the obligation of the government and enterprises to safeguard the interests of civil society? This article believes that GDC proposes "digital human rights" as the answer to this question. Digital human rights are the main basis for governments and enterprises to safeguard the interests of civil society on the Internet. Digital human rights, as a value order, constitute the implementation premise and a new picture of the "multi-stakeholder" governance model.

5. Interaction Between "Stakeholders" Under the Framework of the Global Digital Compact

The GDC represents a groundbreaking initiative in the quest for cohesive and inclusive digital governance. By outlining a framework that incorporates diverse stakeholders—governments, enterprises, and civil society—the GDC aims to address the fragmented approaches to digital regulation that currently prevail. This section delves into the overarching principles and objectives of the GDC, setting the stage for a closer examination of its proposed interactions and governance mechanisms.

5.1 General Overview of the Global Digital Compact



5.2 Horizontal Interaction: International Digital Cooperation Framework

In horizontal interaction, governments need to continuously negotiate and form a digital cooperation framework through government-to-government negotiations. As stated in GDC, the United Nations is only a convening body that has facilitated GDC, and the specific implementation of the compact still requires the support and cooperation of governments. The international digital cooperation framework formed between governments has two main objectives: first, to form digital connectivity between governments to eliminate the digital divide between countries, especially between developed and developing countries (Global Digital Compact Initiative A). Specific methods include providing

online resources (Global Digital Compact Initiative B) and ensuring cyber security (Global Digital Compact Initiative D). Second, governments should reach a basic consensus on the concept of AI governance and codify it, so as to formulate international standards for AI governance and provide general guidance for national AI governance.

5.2.1. Digital Connectivity (Eliminating the Digital Gap)

Digitalization indeed brings opportunities for enhanced efficiency, transparency, and accountability, yet significant infrastructure challenges remain. Additionally, surveillance risks and other potential threats to human rights persist. To bridge the Digital Divide, urgent international cooperation is necessary. As digitalization advances, there is an increasing risk that the gap between urban and rural areas will widen, leading to a surge in the number of people without access to digital technologies and services. Key digital technologies play an essential role in enabling access to resources, jobs, healthcare, education, and public services, positioning the digital divide as an emerging human rights issue. In line with the UN 2030 Agenda for Sustainable Development, it is vital that technological advancements are inclusive of all. With internet demand rising sharply during the COVID-19 pandemic, nations should aim to expand internet access as widely as possible. Closing the Digital Divide, including addressing the gender digital gap, is critical to delivering essential services. As countries outline their ambitions in artificial intelligence and digital transformation, they must prioritize societal needs and ensure that diverse groups have fair access to digital technologies, making genuine efforts to promote inclusivity.

Member states shall commit to crafting policies and new financial strategies that incentivize telecommunications providers to deliver affordable connectivity in underserved regions. Additionally, they should work on enhancing or creating public education programs to improve digital literacy and cross-disciplinary skills, while promoting lifelong learning opportunities for workers. In this context, China has demonstrated a strong approach to addressing the digital divide. Since the inception of the Belt and Road Initiative, digital collaboration has rapidly progressed over the past decade, yielding numerous results, such as the gradual establishment of a digital cooperation framework, notable improvements in digital connectivity, the rise of e-commerce along the Silk Road as a new driver of trade and development, expanded mobile payment networks facilitating easier currency transactions, and a growing public sense of benefit from digital cooperation. For further details on specific achievements, please refer to the table below.

Table 1: Digital Cooperation Systems Directly Signed by Governments Between China and Countries Along the Belt and Road

Name of the Systems	**Participating countries**	**Content and Meaning**

"Belt and Road" Initiative on International Cooperation in the Digital Economy	China, Egypt, Laos, Saudi Arabia, Serbia, Thailand, Turkey, United Arab Emirates	Propose key areas, implementation mechanisms and main principles for international cooperation in the digital economy along the Belt and Road.
Cooperation Agreement in the Field of Informatization and Digitalization	China and Russia	Encourage both sides to strengthen cooperation in the digital field
Memorandum of Understanding on Building a "Digital Silk Road"	China and 17 other countries, including Turkey, Saudi Arabia, Laos and Cuba	Cooperate in human resources development, technology transfer, and regulatory development.
Memorandum of Bilateral E-commerce Cooperation	China and 30 other countries, including Italy, Argentina, Russia and Austria	Partners will work together on multi-level and multi-field cooperation in policy communication, planning integration, and industrial promotion, and jointly explore new areas of economic and trade cooperation in the building of the Belt and Road.

Data sources: Chinese government website, China Belt and Road website.

Table 2: Digital Cooperation Systems Signed by China and Countries Along the Belt and Road Through International Organizations

Name of the systems	**Participating countries or organizations**	**content and meaning**
APEC Initiative for Internet Economy Cooperation, APEC Cross-Border E-Commerce Innovation and Development Initiative, APEC Roadmap for the Internet and the Digital Economy, APEC Framework for the Facilitation of Cross-Border E-Commerce, APEC Digital Economy Action Plan	China and the Asia-Pacific Economic Cooperation (APEC)	Systems and priority areas for digital economy cooperation under the APEC framework have been identified, and 37 digital economy cooperation projects have been led.
"International Code of Conduct for Information Security" updated text	China and the Shanghai Cooperation Organization (SCO)	The first comprehensive and systematic international document to set out norms of behavior in cyberspace. It has made an important contribution to promoting the formulation of norms of behavior in cyberspace.
G20 Digital Economy Development and Cooperation Initiative	China and the Group of 20 (G20)	It elaborates on the concept of the digital economy, clarifies the principles and priority areas of digital economic cooperation, and is the world's first digital economic policy document

		signed by leaders from multiple countries.
Agreement on Trade and Economic Cooperation between China and the Eurasian Economic Union	China and the Eurasian Economic Union (EAEU)	Aims to improve trade facilitation, promote the in-depth development of economic and trade relations between China and the Eurasian Economic Union and its member states, bring benefits to enterprises and people of both sides, and provide institutional guarantees for bilateral economic and trade cooperation.
China-Arab Data Security Cooperation Initiative	China and the League of Arab States (LAS)	This marks a new stage in strategic mutual trust and pragmatic cooperation in the field of digital affairs between the two sides. The two sides are willing to take this as an opportunity to continuously deepen cooperation and jointly promote global digital governance and international rule-making.
G20 Action Plan for Digital Innovation Cooperation	China and the Group of 20 (G20)	The aim is to promote the innovative application of digital technology and achieve inclusive sharing of innovation. The two sides will work together to build a global digital economic structure that is inclusive, balanced, coordinated, win-win and prosperous.

Data sources: Chinese government website, China Belt and Road website.[47]

5.2.1.1 Providing Online Resources

The internet resource provisioning initiative, introduced by GDC, focuses on two main objectives. The first goal is to invest strategically in digital public infrastructure and services, fostering a global awareness of digital public goods and sharing best practices to drive progress toward the Sustainable Development Goals. The second goal is to harness data as a powerful tool to advance these goals by ensuring it is inclusive, interoperable, and accessible. Key areas of action include uniting data resources, artificial intelligence expertise, and infrastructure across borders to innovate in support of specific Sustainable Development Goal targets and creating a sustainable environment by establishing globally consistent digital standards and protections for environmental sustainability.

Member States and stakeholders should develop a framework for inclusive, sustainable digital public infrastructure based on best practices and clear safety standards. This includes creating a global repository for digital service insights, dedicating funds for digital transformation, and addressing data gaps for tracking SDGs with a goal of 90% public data accessibility by 2030. Supporting open data ecosystems is crucial for effective disaster response, aided by UN and WMO initiatives. Priority areas for collaborative data and AI research include agriculture, education, energy, health, and sustainability. A secure global platform should also be created to provide researchers and policymakers with necessary data, licenses, and safeguards to support green digital progress.

Multilateral organizations are encouraged to create pooled funds to support governments in planning and developing digital public infrastructure. This includes expanding the OECD's purpose code to track funding for digital transformation aligned with the Sustainable Development Goals. A forthcoming UN digital transformation blueprint will provide a step-by-step guide, while the new digital window in the SDG Joint Trust Fund should support national digital projects with assistance from Resident Coordinators and UN Country Teams.

5.2.1.2 Ensuring Network Security

There are two major cores to ensuring network security. First of all, safeguarding the free and shared nature of the Internet, so that it becomes a unique and irreplaceable global public asset that is not unreasonably restricted by public power or capital.

In this regard, Member States should pledge to avoid broad Internet shutdowns, as such actions undermine efforts to close the digital divide. Instead, any restrictive measures should be proportional, non-discriminatory, applied only when essential, and accompanied by transparent reporting on their purpose and legal basis, in alignment with international human rights standards. Under the UN cyber diplomacy framework, there is a commitment to avoid disrupting critical infrastructure essential for cross-border services and the global stability of the Internet. Stakeholders should also pledge to uphold

network neutrality, fair traffic management, standardized technical protocols, and interoperability across infrastructure, data, platforms, and devices to ensure an open, interconnected Internet.

5.2.2 International Standard for Artificial Intelligence Governance

While digital technologies and AI systems offer notable benefits for individuals and society, they also present certain risks that may impact human rights in the digital realm. These risks include the use of facial recognition for mass surveillance, algorithmic biases, and a lack of transparency that can lead to unfairness, privacy violations, data misuse, and the spread of disinformation through deepfakes. Governments and officials, in particular, bear a "special responsibility" to uphold human rights when deploying AI and automated decision-making systems, as highlighted by a landmark ruling in the Netherlands. In response, an increasing number of countries and international organizations are working to establish global standards for AI governance to manage and regulate its impact.

From the perspective of extra-territorial and international law, many important data and artificial intelligence legislative initiatives have been proposed within the European Union, such as the "Proposal for a Regulation of the European Commission on an AI Regulatory Framework" (EU AI Act).

This draft regulation centers on managing the "impact" of AI systems on individuals, while other related EU initiatives include the Digital Services Package and the 2020 European Data Strategy. In 2019, the OECD introduced the Recommendation on Artificial Intelligence, outlining principles for governing trustworthy AI. The OECD also serves as the secretariat for the Global Partnership on Artificial Intelligence (GPAI), launched in July 2020, aiming to foster responsible AI development that respects human rights, inclusiveness, diversity, innovation, and economic growth. At the EU level, CAHAI was established to explore a legal framework for AI systems that aligns with human rights, democracy, and the rule of law. Acknowledging the limits of self-regulatory ethical codes, CAHAI aims to safeguard these values through binding legal measures. This initiative involves all Council of Europe departments and includes tools like the Charter of Ethics on the Use of Artificial Intelligence in the Justice System, developed by CEPEJ.

At the United Nations, UNESCO's Commission on Social and Human Sciences has endorsed an "Ethical Recommendation for Artificial Intelligence," marking the first global framework to address AI's ethical implications. Similarly, UNICEF has drafted a "Policy Guidance for Artificial Intelligence for Children," offering recommendations for creating AI policies and systems that uphold children's rights and ensure the protection of their data and privacy. Numerous international and regional organizations, including the United Nations, have also established their own standards to regulate and govern AI within their specific domains.

Member States should consider the High-level Advisory Committee on Effective Multilateralism's recommendation to create a fund supporting research and preparation for existential risks posed by unregulated AI advancement and to establish a high-level AI advisory body under the Global Compact on Data. This body could bring together experts from Member States, relevant UN agencies, industry, academia, and civil society, meeting regularly to assess new AI governance frameworks across regions,

countries, and industries. It would offer guidance on ensuring that ethical, safety, and regulatory standards align with and support universal human rights and the rule of law. This advisory group could publicly share its findings and, when applicable, recommend governance strategies and international standards for AI. Additionally, agreements with industry associations could be pursued to create sector-specific guidelines, ensuring that technology developers and users have tailored guidance for the design, application, and review of AI-driven tools in various settings.

5.3 Vertical Interaction: Domestic Regulation of Resource Allocation

In vertical interaction, there needs to be a virtuous coordination between the government and enterprises regarding the allocation of regulatory resources. The "multi-stakeholder" governance model not only means the diversification of governance entities, but also the coordination and cooperation between them. As stated in Action Line E of GDC, there should be enhanced cooperation between governance entities such as governments and enterprises to formulate and implement common domestic digital governance rules.

5.3.1 Risk Assessment System (Supervised Self-Regulation)

After the enterprise has established a basic data compliance system, it needs to conduct a risk assessment of the data processing procedures under the compliance system, which is to some extent a verification of the effectiveness of the data compliance system.

Article 35 of the EU GPDR stipulates that a "data protection impact assessment" shall be conducted when the data controller's data collection activities may pose a high risk to the natural person's right to freedom. As for the specific content of the assessment, some scholars have summarized three main parts: objective setting, scope and methods, and assessors.

In China, the normative basis for the data compliance risk assessment mechanism for personal information protection is the "personal information protection impact assessment" stipulated in Articles 55 and 56 of the Personal Information Protection Law. At the theoretical level, some scholars have proposed that impact assessments can be carried out based on aspects such as application scenario investigation, personal information classification, interest impact analysis, and system risk assessment.

This article argues that the current discussion on the data compliance risk assessment system mainly focuses on its specific construction and practical application, and lacks discussion on the effectiveness of the system, i.e., what legal effect does the result of the risk assessment have? How does it connect with other systems? Returning to the basic principles of data compliance, data compliance is not only a form of self-regulation by enterprises, but also an incentive for government regulation. Specifically, the data compliance risk assessment system can be linked to the leniency system for enterprises involved in cases. Taking Article 3 of the Shenzhen Enterprise Data Compliance Guidelines as an example, the result of the data compliance risk assessment can be used as the standard for fulfilling the obligation to "fulfill data compliance obligations" in Paragraph 1 of the Article. If the result of the data compliance risk assessment is good, it should be considered as proof of effective compliance in the

"effectiveness standard" in Paragraph 3 of the Article. It should be noted here that the data compliance risk assessment mechanism is based on a risk assessment of the entire data life cycle, involving multiple stages such as data collection, data transmission, data storage, data processing, data exchange, and data destruction. Therefore, the corresponding risk assessment results should also be phased, i.e., the determination of the data compliance risk assessment results should not be determined as a "package" but should be determined separately for each stage.

5.3.2 Pluralistic Accountability System (Self-Regulation of Being Held Accountable)

Risk assessment as "supervised self-regulation" supervises the enterprise's self-regulation from the perspective of ex-ante prevention by urging the enterprise to independently assess the risks under the data compliance system, thereby achieving supervision of the enterprise's self-regulation. Pluralistic accountability in this part is a restriction imposed on the enterprise's self-regulation from the perspective of ex-post relief. Compared with the previous two links, pluralistic accountability as "enforced self-regulation" more reflects the mandatory nature of public power intervention and serves as a bottom-up guarantee.

Specifically, for enterprises that have legal risks such as infringement of information data due to non-compliance with data compliance standards, corresponding accountability mechanisms should be established. At the regulatory level, Article 5 of the GDPR, which is extraterritorial, clearly stipulates the accountability mechanism for enterprises as data processors. Article 51 of the domestic Personal Information Protection Law requires that personal information processors fulfill corresponding information protection compliance obligations. Organizational measures such as the adoption of security technical measures such as encryption and de-identification, as well as the identification of a person responsible for personal information protection and regular security education and training for employees should be implemented.

The "pluralistic accountability" advocated in this article mainly refers to "multiple forms of accountability". As a self-regulatory model, data compliance benefits from legal incentives for its smooth implementation. Therefore, regulatory accountability for data compliance should not be overly coercive (one-size-fits-all). When considering the cost and impact of law enforcement, regulators and the regulated often prefer a regulatory approach at the bottom of the enforcement pyramid, that is, encouraging companies to self-regulate. Therefore, accountability for data compliance can adopt a "enforcement pyramid" mindset, and different levels of responsibility can be determined and adjusted according to the attitude and response of the enterprise to accountability. According to the general corporate compliance theory, the compliance services provided by domestic lawyers for lawyers generally include three parts: creating a compliance plan, providing compliance investigations, and responding to law enforcement investigations. Correspondingly, the "enterprise-government" binary interaction in data compliance can be reflected at each stage, to determine the responsibility that the enterprise should bear when it fails to self-regulate.

6. Conclusion

GDC issued by the United Nations has a certain mission for the times. It aims to update the governance concept of the "multi-stakeholder" governance model and formulate common principles for building an open, free and secure digital future for all mankind.

Although GDC has not yet obtained the clear force of international law, in today's world, which relies more than ever on digital technology for interconnection and socio-economic prosperity, and the significance of GDC for the times is becoming increasingly prominent.

In the specific implementation of GDC, attention should be paid to the value order of digital human rights in civil society as the core foundation governing global digital governance, thus distinguishing between "government-government" international horizontal interaction and "government-enterprise" domestic vertical interaction. Horizontal interaction aims to form an international framework for digital cooperation between governments, eliminate the international digital gap between developed and developing countries, and form international standards for the governance of artificial intelligence. Vertical interaction aims to form multi-regulatory interaction between governments and enterprises, and achieve interaction and coordination between self-regulation and government regulation through risk assessment mechanisms and multiple accountability mechanisms.

Looking back at the world at the beginning of the 21st century, the world trade system with the WTO at its core gradually improved, and the wave of globalization, which represents barrier-free and free flow, swept through almost every country. In contrast, in the Internet era today, the wave of de-globalization is impacting on the framework and order of global digital governance. Under this background, this article hopes to promote GDC to activate the "multi-stakeholder" governance model through theoretical analysis and outlook, to achieve a new view of global digital governance.

Acknowledgement

The authors would like to express their heartfelt gratitude to Junxi Duan for providing valuable insights and inspiration that greatly contributed to the research direction of this paper. Without such guidance and encouragement, this work would not have been possible.

Funding Statement

None.

Author Contributions

Qifan Jiang: writing original draft, validation, investigation.

Yuhang Ma: methodology, writing review and editing supervision.

All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials

None.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1]. 47 U. S. C.§223(a)(1)(B)(ii) (1994), 2, (223) (d).

[2]. Assembly, G. (2015). Transforming our world: the 2030 Agenda for Sustainable Development, A/RES70,1.

[3]. Ayres, I & Braithwaite, J. (1992). Responsive Regulation: Transcending the Deregulation Debate, Oxford University Press.

[4]. Baran, P. (1964). On Distributed Communications Networks, 12 IEEE Transactions on Communications Systems 1,1-9.

[5]. Baran, P. (1964). On Distributed Communications Networks, 12 IEEE Transactions on Communications Systems 1,1-9.

[6]. Barlow, J. (2001) Tsinghua Legal Theory Review, (X. Li, & X. Li, Trans.) Tsinghua University Press.

[7]. Berners.L.T., Cailliau, R., Luotonen, A., Henrik Frystyk, N.A., & Arthur Secret. (1994) The World-Wide Web, Communications of the ACM 37 (8), 76-82.

[8]. Chapelle, B. (2009), Internet Governance: Infrastructure and Institutions, Oxford University Press, 256-270.

[9]. Chapelle, B.D. (2009) Internet Governance: Infrastructure and Institutions, Oxford University Press

[10]. Chen, R. (2022). Basic Theory of Corporate Compliance, Law Press.

[11]. Council of Europe and European Commission for the Efficiency of Justice, (Ed.) (2018) European Ethical Charter on the use of artificial intelligence in judicial systems and their environment, https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.

[12]. DeNardis, L. (2014). The Global War for Internet Governance, Yale University Press, 8; 69; 66; 36; 223; 226-227.

[13]. Dickens, C. (1859). A Tale of Two Cities.

[14]. Digital Silk Road Accelerates World Modernization (Ed.) China Belt and Road Network, High-Quality Joint Construction of the Belt and Road Has Achieved Remarkable Results remarkable, in China.gov.cn, https://www.gov.cn/xinwen/2022-01/25/content_5670280.htm.

[15]. Digital Silk Road Accelerates World Modernization (Ed.) China Belt and Road Network, High-Quality Joint Construction of the Belt and Road Has Achieved Remarkable Results remarkable, in China.gov.cn, https://www.gov.cn/xinwen/2022-01/25/content_5670280.htm.

[16]. ECNL, Council of Europe Ad Hoc Committee on Artificial Intelligence (Ed.) (2021). Public consultation (survey) --ECNL Answering Guide, https://ecnl.org/sites/default/files/2021-04/CAHAI%20Survey_ECNL%20Answer%20Guide_0.pdf.

[17]. Edwards, P. (1996). The Closed World: Computers and the Politics of Discourse in Cold War America, MIT Press.

[18]. European Commission (Ed.) (2020) The European Data Strategy. https://ec.europa.eu/commission/presscorner/api/files/attachment/862109/European_data_strategy_en.pdf

[19]. European Commission, (Ed.) (2021). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, https://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206

[20]. Goldsmith, J & Wu, T. supra note 5, 37-38

[21]. Goldsmith, J & Wu, T., supra note 5, 41.

[22]. Goldsmith, J. & and Wu, T. supra note 5, 22.

[23]. Goldsmith. J, & and Wu, T. (2000), supra note 5, (X. Wang, Trans.) Peking University Press.

[24]. He, H. & Zhang, Y. (2023). Conflict of Interest and Mitigation in the Reasonable Use of Personal Health Information in the Digital Age: Taking 'Design Protection' as an Approach, Science & Technology and Law, (4), 48.

[25]. ICANN. (Ed.) Bylaws for Internet Cooperation for Assigned Names and Numbers. https://www.icann.org /resources/pages/governance /bylaws-en.

[26]. Information Commissioner's Office,Conducting Privacy Impact Assessments Code of Practice, (2017). Information Commissioner's Office, UK.

[27]. Johnson, D. & Post, D. (1996), Law and Borders: "The Rise of Law in Cyberspace",48 Stanford Law Review,1367; Wu, S., T. Cyberspace Sovereignty, 10 Harvard Journal of Law and Technology,467

[28]. Kahn, P, (2009). American Exceptionalism, Popular Sovereignty, and the Rule of Law, in Michael Ignatieff ed, American Exceptionalism and Human Rights, (198-222.). Princeton University Press.

[29]. Kleinwächter, W. (2011), Editorial in MIND Co: laboratory Discussion Paper Series, 2.

[30]. Liu, H. (2016). Domain Name System, Network Sovereignty and Internet Governance, Chinese and Foreign Law, 2, 527.

[31]. Liu, H. (2016). Domain Name System, Network Sovereignty and Internet Governance, Chinese and Foreign Law2, 528.

[32]. M． Kummer.Multis take holder Cooperation (Ed.): Reflections on the Emergence of a New Phraseology in International Cooperation. http://www.internetsociety.org/blog/2013 /05/multistakeholder-cooperation-reflectionsemergence-new-phraseology-international.

[33]. M. Kummer.Multis take holder Cooperation9(Ed.): Reflections on the Emergence of a New Phraseology in International Cooperation. http://www.internetsociety.org /blog /2013 /05/multistakeholder-cooperation-reflectionsemergence-new-phraseology-international.

[34]. Mathiason, J. (2009), Internet Governance: The New Frontier of Global Institute (pp. 70-96.) Routledge,

[35]. Mathiason, J., (2009). Internet Governance: The New Frontier of Global Institute, Routledge, 70-96.

[36]. Mueller,L.M. (2015). Networks and States: The Global Politics of Internet Governance, (Z., Chen. et al. Trans). Shanghai Jiao Tong University Press.

[37]. Mueller,L.M. (2015): Networks and States: The Global Politics of Internet Governance, (Z., Chen. et al. Trans). Shanghai Jiao Tong University Press.

[38]. OECD, Recommendation of the Council on Artificial Intelligence.

[39]. Oever, N.T., Moriarty.,K. (Ed.) (2012.) The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force. https: / /www.ietf.org /about /participate /tao /

[40]. Political Declaration at the Occasion of the UN's 75th Anniversary (2020). https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/248/80/PDF/N2024880.pdf?OpenElement.

[41]. Rachovitsa, A. &Johann, N. (Ed.) (2022) The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case, Human Rights Law Review 22, 2. https://doi.org/10.1093/hrlr/ngac010.

[42]. Somnstein, k. (1966). The Networked Republic: Democracy in the Age of the Internet (Huagn, W, Trans.). Shanghai People's Publishing House.

[43]. Stevens, J. (1997). American Civil Liberty Union v. Reno, 521 U.S.844, 851.

[44]. Szucs, A. (Ed.) (2021). NATO defense ministers adopt strategy on artificial intelligence, Anadolu Agency, https://www.aa.com.tr/en/world/nato-defense-ministers-adopt-strategy-on artificial-intelligence/2400087.

[45]. The Global Partnership on AI. (Ed.) (2023). https://oecd.ai/en/gpai.

[46]. The original Internet, the Arpanet, was born in the midst of the Cold War between the United States and the Soviet Union. Its original design concept was closely related to the political struggles and military struggles between sovereign states.

[47]. UNDP (2023). The impact of digital technology on human rights in Europe and Central Asia: Trends and challenges related to data protection, artificial intelligence and other digital technology issues. Istanbul: United Nations Development Programme.

[48]. UNDP (2023). The impact of digital technology on human rights in Europe and Central Asia: Trends and challenges related to data protection, artificial intelligence and other digital technology issues.

[49]. UNESCO(Ed.) Recommendation on the ethics of artificial intelligence. https://en.unesco. org/artificial intelligence/ethics; UNICEF (Ed.) (2021). Policy guidance on AI for children 2.0, https://www.unicef. org/globalinsight/reports/policy-guidance-ai-children; UN Global Pulse (Ed.). Expert Group on Governance of Data and AI, https://www. unglobalpulse.org/policy/expert-group-on-governance-of-data-and-ai/; EU Reporter (Ed.) (2021). Distinguished leaders from

Boston and Balkan regions to collaborate for Global Law on AI and Digital Rights, https://www.eureporter.co/world/us/2021/10/01/distinguished-leaders-from-boston-and-balkan-regions-to-collaborate-for-global-law-on-ai-and-digitalrights/

[50]. UNICEF (Ed.) (2021). Policy guidance on AI for children 2.0. https://www.unicef. org/globalinsight/reports/policy-guidance-ai-children,

[51]. United Nations. A Global Digital Compact-an Open, Free and Secure Digital Future for All. 11.

[52]. United Nations. A Global Digital Compact-an Open, Free and Secure Digital Future for All. 19.

[53]. United Nations. A Global Digital Compact-an Open, Free and Secure Digital Future for All. 12.

[54]. United Nations. A Global Digital Compact-an Open, Free and Secure Digital Future for All. 12.

[55]. United Nations. A Global Digital Compact-an Open, Free and Secure Digital Future for All. 11.

[56]. United Nations. A Global Digital Compact-an Open, Free and Secure Digital Future for All. 19.

[57]. United Nations. A Global Digital Compact-an Open, Free and Secure Digital Future for All. 14.

[58]. United Nations. A Global Digital Compact-an Open, Free and Secure Digital Future for All. 14.

[59]. United Nations. A Global Digital Compact-an Open, Free and Secure Digital Future for All. 14.

[60]. Wang, J. (2017), Introduction to the Economics of Government Regulation: Basic Theory and Its Application in Government Regulation Practice, The Commercial Press.

[61]. Xie, Z. & Zhang, J. (2023). The international community praises the Digital Silk Road, China Social Sciences Journal.

[62]. Zhang, J. (2022) Research on a Designed Personal Information Protection Mechanism, Law Science, 3, 42

[63]. Zhang, T. (2021), Metaregulation of 'Protecting Data by Design' in the Era of Big Data, Journal of Dalian University of Technology (Social Sciences Edition), 2, 86.

[64]. Zhao, Q. (2023). Multi-Party Cooperation to Bridge the Global Digital Divide, China Social Sciences Journal 1.

[65]. Zhao, X. (Ed.) The End of the Masquerade. Humanities and Social Sciences Network. http:// wen. org. en/modules/article/view, article. php/1249.

[66]. Zou, J, (2016). Reconstruction of Global Internet Governance Models, China's Opportunities and Participation Paths, Journal of Nanjing Normal University, 3.

[67]. Zou, J. (2016), Reconstruction of the Global Internet Governance Model, China's Opportunities and Participation Path, Journal of Nanjing Normal University. https: / /en.wikipedia.org /wiki /ICANN.

disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.