

制定数据主权政策的基本原则 (Fundamental principles of data sovereignty policy making)

Shan Yin, Peking University

摘要

如何制定可行且有效的数据主权政策，是各国监管机构在互联网治理相关政策领域的关注重点，其中的焦点在于：如何在维护国家数据主权的同时不会妨碍数据的有序流动，以免互联网的“巴尔干化”。面对这一问题，本文通过回顾数据主权的产生提出了几项制定政策的基本原则。一方面，数据主权政策源自国家主权、认可国家对本国内部数据事务的管辖权；另一方面，数据主权应当更具创新性和灵活性。我们认为，充分包容性的数据治理体系能够充分照顾各国的多样化互联网治理需求。

Abstract

How to formulate feasible and effective data sovereignty policies is a key focus of regulatory agencies in the field of internet governance. The crux of the issue is how to maintain national data sovereignty without hindering the effective flow of data, so as to avoid the 'Balkanization' of the internet. In the face of this problem, this article proposes several basic principles for formulating data policies by reviewing the origins of data sovereignty. On the one hand, data sovereignty policies stem from national sovereignty and recognize a country's jurisdiction over its internal data affairs. On the other hand, data sovereignty should be more innovative and flexible. We believe that an inclusive data governance system can fully adapt to the diverse internet governance needs of different countries.

随着人工智能、物联网、区块链等数字化技术的广泛使用，数据越来越被视为经济发展、社会治理的重要因素和我们认识时代的途径。所有社会生产活动都可以“数字化”（ITU 2005）。据统计，2022 年全球产生、交换和消费的数据总量为 79 泽字节（Djuraskovic 2022）。这催生了数字经济的蓬勃发展、加速了社会的数字化进程。由于缺少物理世界的“硬边界”，海量数据的跨境流动不可避免的产生，对国家主权的影响逐渐引起了各国互联网（或数字）监管机构的关注、成为了互联网治理相关公共政策的讨论热点。在这方面，政策制定者面临着挑战一方面，数据主权一方面要满足国家主权、尤其是网络主权的要求；另一方面由要防止过度的政策干预对数据有序自由流动带来的影响、从而影响数字经济发展和社会的数字化进程。面对这一挑战，本政策简报将首先回顾数据主权问题的诞生，继而向涉及政策制定的利益相关方，主要是各国监管机构、平台企业（Banker 2016）、代表消费者利益的民间社会等提供数据主权政策制定的几项基本原则，力图构建一个安全、繁荣的全球数据生态系统。

数据主权的诞生：一个动态和包容的概念

“主权”这一术语源自近代国际法和国际关系的形成，体现着民族国家政府对本国领土范围内所辖事务的对内权威性和对外独立性诉求（Krasner 2001），是国家权力自上而下的集中体现。网络主权的讨论可以追溯到冷战时期。基于当时的地缘政治格局，一些第三世界国家希望寻找一条有别于殖民统治的“现代化道路”，借助现代信息技术实现社会发展、构建身份认同。这些国家提出构建“世界信息与传播新秩序”（Carlsson 2003），其关注焦点是“全球信息流动”、实现“全球信息流的再平衡”。从这些国家的角度来看，不受限制的信息流动无疑会冲击国家主权，这一议题也成为了日后互联网治理政策讨论的焦点。

随着互联网的发展，“网络主权”这一提法也随之诞生。从字面来看，网络主权就是国家对本国互联网实施绝对性和排他性管理的最高权力（Jensen 2015）。快速发展的数字化技术等让数据的收集和使用更加容易，是的数字化社会成为一种现实。技术的飞跃使数据的收集和使用变得更加容易，大大降低了数据挖掘

的成本。几乎所有的人类行为都可以通过“数字化”来实现，并在网络空间中产生“数字孪生”（Jones et al. 2020）。这些数据可以不受国界限制在全球网络空间流动，从而与国家对本国境内数据资源的控制权产生碰撞，数据主权问题由此浮现，从而进入到了政策制定者的视野。进一步而言，数据主权关系到国家、公民、消费者等多个主体，涉及对数据和数据基础设施的所有权、控制权、隐私权等多项权利（Hummel et al. 2021）。由此可见，数据主权是不同主体所拥有的权利的“混合体”，是一个动态和包容的概念。

制定数据主权政策的几项原则

如同导言部分所讨论的，数据主权议题涉及多个维度和主体，这也揭示了数据主权政策制定的复杂性。与此同时、作为互联网治理的重要组成部分，本简报也认为数据主权概念体现了充分的包容性。因此，我们认为各国的数据主权政策制定应当遵循如下原则：

监管机构应当树立创新和灵活性的网络主权理念。由于数据主权源于网络主权，因此如何看待网络主权又涉及到数据主权政策制定。主权国家依然是当今国际关系的主要行为体。因此，尊重各国监管机构对本国内部互联网的管辖权是十分重要的。同时，数据主权应当更加具备创新性和灵活性。在这一点上，学界的探讨已经引起了关注。有学者提出的“三视角理论”可以提供参考（Hao 2017）。该理论将网络空间分为核心层、基础设施层和应用层，网络主权在不同层次产生有不同的范围。在核心层，国家行为体可以发挥主要作用；在另外两个层面，平台企业、民间社会等主体能够在数据基础设施、数字经济、隐私保护等方面扮演重要角色，推动政策的完善。因此，监管机构应当树立创新和灵活的网络主权理念，理解其开放性和包容性。

推进基于多利益相关方模式的政策制定。从2003年和2005年的“信息社会世界峰会”议程开始，“多利益相关方模式”便被视作互联网治理的主流模式（Savage and McConnell 2015）。根据该模式，“互联网治理的定义是由政府、私营部门和民间社会在各自的角色中制定和应用共享的原则、规范、规则和计划，来塑造互联网的发展和利用”（WSIS 2006）。该模式充分考虑了各利益相关方的角色和利益诉求，有利于形成能为各方所接受的共识性规则。在数字化程度较高的经济体，作为私营部门的平台企业掌握着大量数据资源，它们通过研讨、游说、听证等多种方式对政策

产生影响。此外，政策制定也应当充分吸纳代表消费者利益的民间社会的立场，保证个体的隐私权等个人权利。这会产生相对公平与合理的数据主权政策，不会因为政策歧视导致某个利益相关方被排斥在外。

可信和可持续的的国际合作。数据主权事务涉及到国际合作。实现可信的国际合作，对于完善各国的数据主权政策十分重要。各国应当意识到，数据主权政策应当保障数据安全、积极利用数据驱动创新，实现安全、有效的数据使用，推动人类社会的数字化进程。为实现这一目标，推动可信和可持续的国际合作十分重要，因为这有助于弥合各国政策不一致带来的信任危机，推动数据主权国际共识的形成（Nugraha and Sastrosubroto 2015）。这将有利于实现数据的安全、有序和自由流动，实现国家安全、公共利益和个人权益的统一。在这一点上，《全球数据安全倡议》^①等战略值得借鉴。以该份文件为例，它十分重视国际合作，充分回应了构建“网络空间命运共同体”（Li 2016）。由此可见，政策制定者完全可以通过可信的国际合作，让数据主权的包容性兼顾“数据安全有序自由流动”和“国家主权”，实现二者的共存。

政策建议/结论

上述讨论揭示了数据主权源于传统的国家主权，且存在一定的创新性和灵活性。数据主权政策可以成为数据治理国内实践和对外合作的交汇点，各国可以在此寻求“共识”。在这个过程中，包括政府、平台企业、民间社会的各利益相关方应当充分认识到，数据主权政策是多种因素平衡后的产物。

对于政策制定者来说，数据主权制度是一个逐渐完善的过程，其具体条款应当既满足国家主权要求、又符合数据跨境流动需求，通过数据安全有序流动实现数字经济的繁荣。

通过本文讨论可以发现，数据主权政策应当适应整个社会的数字化进程；数据主权制度不宜否定全球网络空间的互联互通。各国应当在这一议题上进行充分对话，对国际合作预留充分的空间。

数据政策既是复杂的，也应当是开放和包容的。数据不应成为技术政治的武器，也不应当成为隐私监控的工具。。政府、平台企业和民间社会应当密切合作，让各方都能充分受惠于这一政策制定和实践的过程。在人类社会的数字化浪潮中，我们认为：人类不应该

^① *Global Initiative on Data Security*. [online] https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202009/t20200908_679637.html

成为技术的奴隶，技术应该为人类服务，人类应该通过技术进步获得自由。

[English] With the widespread use of digital technologies such as artificial intelligence, the Internet of Things, and blockchain, data is increasingly regarded as a critical factor for economic development, social governance, and our understanding of the era. All social production activities can be "digitized" (ITU 2005). According to statistics, the total amount of data generated, exchanged, and consumed globally in 2022 was 79 zettabytes (Djuraskovic 2022). This has led to the booming development of the digital economy and accelerated the process of digitization in society. Due to the lack of "hard boundaries" in the physical world, the inevitable cross-border flow of massive data has gradually attracted the attention of internet (or digital) regulatory agencies in various countries and become a hot topic in the discussion of public policies related to internet governance. In this regard, policy makers face challenges: on the one hand, data sovereignty needs to meet the requirements of national sovereignty, especially cyber sovereignty; on the other hand, it should prevent excessive policy intervention from affecting the orderly free flow of data and thus impeding the development of the digital economy and the process of digitization in society. Faced with this challenge, this policy brief will first review the origins of the issue of data sovereignty, and then provide several basic principles of data sovereignty policy to stakeholders involved in policy making, such as regulatory agencies, platform companies (Banker 2016), and civil society representing consumer interests, in an effort to build a safe and prosperous global data ecosystem.

The Birth of Data Sovereignty:

A Dynamic and Inclusive Concept

The term "sovereignty" originated from the formation of modern international law and international relations, reflecting the domestic authority and external independence of nation-states in relation to their territorial affairs (Krasner 2001), and represents a top-down concentration of state power. Discussions on cyber soverei

gnty can be traced back to the Cold War period. Based on the geopolitical landscape at that time, some third world countries sought to find a "modernization path" different from colonial rule, using modern information technology to achieve social development and construct identity. These countries proposed the construction of a "New World Information and Communication Order," (Carlsson 2003) with a focus on "global information flow," aimed at achieving a "rebalancing of global information flow." From the perspective of these countries, unrestricted information flow undoubtedly challenges national sovereignty, and this issue has also become a focal point of future discussions on internet governance policies.

With the development of the internet, the concept of "cyber sovereignty" emerged. Literally, cyber sovereignty refers to the highest authority of a nation-state to implement absolute and exclusive management of its own internet (Jensen 2015). The rapid development of digital technologies has made data collection and usage easier, making digital society a reality. Technological leaps have made data collection and usage much more accessible, greatly reducing the cost of data mining. Almost all human behavior can be achieved through "digitization," generating "digital twins" in cyberspace (Jones et al. 2020). These data can flow freely in the global cyberspace without national borders, thus colliding with the state's control over data resources within its own territory. Therefore, the issue of data sovereignty has thus emerged, entering the policymakers' field of vision. Furthermore, data sovereignty involves multiple stakeholders such as states, citizens, consumers, etc., and encompasses ownership, control, privacy, and other rights related to data and data infrastructure (Hummel et al. 2021). It can be seen that data sovereignty is a "hybrid" of rights held by different entities, and it is a dynamic and inclusive concept.

Principles for Formulating Data

Sovereignty Policies

As discussed in the introduction, the issue of data sovereignty has involved multiple dimensions and subjects. This also highlights the complexity of formulating data sovereignty policies. At the same time, as an important component of internet governance, the concept of data sovereignty embodies inclusiveness. Therefore, this policy briefing illustrates that the formulation of data sovereignty policies in each country should adhere to the following principles:

Regulatory agencies should establish the concept of innovative and flexible cyber sovereignty. Since data sovereignty stems from cyber sovereignty, how to view cyber sovereignty also involves the formulation of data sovereignty policies. Sovereign states are still the main actors in contemporary international relations. Therefore, respecting the regulatory jurisdiction of each country's domestic internet by regulatory agencies is of great importance. At the same time, data sovereignty should be more innovative and flexible. At this point, academic discussions have attracted attention of policy makers. The "Three-Perspective Theory" proposed by some scholars can provide reference (Hao, 2017). This theory divides the cyberspace into the core layer, the infrastructure layer, and the application layer, and cyber sovereignty has different scopes at different levels. At the core level, the state actor could play a major role; at the other two levels, platform company, civil societies can play important role in data infrastructure, digital economy, privacy protection, etc., and promote the improvement of policy formulation. Therefore, regulatory agencies should establish an innovative and flexible concept of cyber sovereignty, understanding its openness and inclusiveness.

Promote policy formulation based on a multi-stakeholder model. Since the agenda of the "World Summit on the Information Society" in 2003 and 2005, the multi-stakeholder model has been regarded as a mainstream approach to internet governance (Savage and McConnell 2015). According

to this model, "internet governance is defined as the development and application of shared principles, norms, rules, and decision-making procedures by governments, private sector, and civil society in their respective roles, to shape the development and use of the Internet" (WSIS 2006). This model takes into consideration the roles and interests of various stakeholders, and is conducive to forming consensus-based rules that are acceptable to all parties. Platform companies as private sector entities hold a large amount of data resources and exert influence on policies through various means such as discussions, lobbying, and hearings. In addition, policy formulation should also fully incorporate the stance of civil society representing consumer interests, ensuring individual rights such as privacy rights. This will result in relatively fair and reasonable data sovereignty policies that do not discriminate against any particular stakeholder and exclude them from the policy-making process.

Trustworthy and sustainable international cooperation. The issue of data sovereignty involves international cooperation. Achieving trustworthy international cooperation is crucial for improving countries' data sovereignty policies. Countries should realize that data sovereignty policies should ensure data security, actively use data to drive innovation, achieve safe and effective data use, and advance the digitization of human society. In order to achieve this goal, promoting trustworthy and sustainable international cooperation is essential, as it helps bridge the trust deficit caused by inconsistent national policies and facilitates the formation of international consensus on data sovereignty (Nugraha and Sastrosubroto, 2015). This will facilitate secure, orderly, and free flow of data, and harmonize national security, public interests, and individual rights. In this regard, strategies such as "Global Data Security Initiative" are worth considering. Taking this document as an example, it attaches great importance, and fully responds to the need to building a "community of common destiny in cyberspace" (Li 2016). This shows that policymakers can promote

inclusivity of data sovereignty by balancing “safe, orderly and free flow of data” and “national sovereignty” through trustworthy international cooperation, and achieve the coexistence of the two.

Policy recommendations/conclusions

The above discussion reveals that the issue of data sovereignty arises from the traditional national sovereignty, and has some degree of flexibility and innovation. Data sovereignty policies can serve as a convergence point for domestic practices and international cooperation of data governance, where countries can seek “consensus”. In this process, all stakeholders including governments, platform companies, and civil society should fully recognize that the formulation of data sovereignty is the result of balancing multiple factors.

For policymakers, the system of data sovereignty is a gradual process of improvement, and its specific provisions should both meet the requirements of national sovereignty and the needs of cross-border data flows, in order to achieve prosperity of the digital economy through secure and orderly flow of data.

From the discussions in this article, it can be concluded that data sovereignty policies should adapt to the digitalization process of the entire society; the system of data sovereignty should not deny the interconnectedness of the global cyberspace. Countries should engage in full dialogues on this issue and reserve ample space for international cooperation.

Data policies are complex and should also be open and inclusive. Data should not be used as a weapon of technological politics or as a tool for privacy monitoring. Governments, platform companies, and civil society should collaborate c

losely to ensure that all parties can fully benefit from the process of policy formulation and implementation. In the wave of digitization in human society, we believe that humans should not become slaves of technology, but rather technology should serve humanity, and humans should gain freedom through technological progress.

参考文献/ References

1. International Telecommunication Union (ITU), 2005, *The Internet of The Things 2005*, [Online] <https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf>
2. Djuraskovic, O., 2022, Big Data Statistics 2022: How Much Data is in The World?. FSG. Accessed on: May, 23.
3. Banker, S., 2016, *The Rise of Platform Enterprise*. [online] <https://www.forbes.com/sites/stevebanker/2016/07/28/the-rise-of-the-platform-enterprise/?sh=64a8d90d5731>. In the context of internet governance, they are also called ‘private sectors’.
4. Krasner, S. D., 2001, Abiding sovereignty. *International political science review*, 22(3), 229–251.
5. Carlsson, Ulla, 2003, ‘The rise and fall of NWICO’: 31–67. [Online] https://www.nordicom.gu.se/sites/default/files/kapitel-pdf/32_031-068.pdf
6. Jensen, E. T., 2015, Cyber sovereignty: The way ahead. *Tex. Int’l LJ*, 50, 275.
7. Jones, D., Snider, C., Nassehi, A., Yon, J., & Hicks, B., 2020, Characterising the Digital Twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology*, 29, 36–52.
8. *What is data infrastructure?* [online] <https://www.hpe.com/us/en/what-is/data-infrastructure.html>
9. Hummel, P., Braun, M., Tretter, M., & Dabrock, P., 2021, Data sovereignty: A review. *Big Data & Society*, 8(1), 2053951720982012.
10. Hao, Y., 2017, A three-perspective theory of cyber sovereignty. *Prism*, 7(2), 108–115.
11. Savage, J. E., & McConnell, B. W., 2015, Exploring multi-stakeholder internet governance. *B*

- rown University Bruce W. McConnell, *EastWest Institute*. [online] [https://www.eastwest.ngo/sites/default/files/Exploring% 20Multi-Stakeholder% 20Internet% 20Governance_0. pdf](https://www.eastwest.ngo/sites/default/files/Exploring%20Multi-Stakeholder%20Internet%20Governance_0.pdf).
12. World Summit on the Information Society, 2006, *Final Report of the Tunis Phase of the WSIS*. [online]<https://www.itu.int/net/wsis/docs2/tunis/off/8rev1.doc>.
 13. Nugraha, Y., & Sastrosubroto, A. S., 2015, May, Towards data sovereignty in cyberspace. In *2015 3rd international conference on information and communication technology (ICoICT)* (465–471). IEEE.
 14. *Global Initiative on Data Security*. [online]https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202009/t20200908_679637.html
 15. Li, Z., 2016, *Why is a Cyber Community of Shared Destiny Important?* [online]<https://www.chinausfocus.com/peace-security/why-is-a-cyber-community-of-shared-destiny-important>