Title	Chapter 2-III : The transmutation of sovereignty : digital "world of warcraft" and innovation in the legal order
Sub Title	
Author	Ji, Weidong
Publisher	Keio University Global Research Institute
Publication year	2025
Jtitle	Monsterizing Platform Power and Law ; Volume 1. Platforms and States: How to Settle the Battle of Monsters ,p.93- 105
JaLC DOI	10.14991/KO11003002.00000001-0093
Abstract	
Notes	Chapter 2 : The battle for the rulers of digital space
Genre	Book
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO11003002-00000001-0093

Chapter 2 - III

The Transmutation of Sovereignty

: Digital "World of Warcraft" and Innovation in the Legal Order

Ji Weidong*

1 The Sovereign State as a Leviathan and its Constraints

An important symbol of Western European-style modernisation was the formation of the institution of the sovereign state. On the grounds of freeing the free individual from the state of nature of "war of all against all", Thomas Hobbes particularly emphasized the absolute and supreme nature of the sovereignty of the state internally. In the global crustal movement of modernity, sovereignty has become the basis for the survival of the nation-state, the exclusive right of the ruler, and the supreme criterion of authority. It has to be admitted that the Sovereign Leviathan, with its unlimited power, is in fact very dangerous for individuals. In order to restrain that increasingly powerful Sovereign Leviathan, the institutional guarantees of freedoms and rights need to be strengthened in particular. In this process, the gradual implementation of the modern rule of law, which operates on the twin wheels of sacrosanct property rights and human rights, to limit the power of the state and to realize equal freedoms as the justification for the power of the state, has become the basic trend of institutional change in Western Europe and even in various countries.

But on the other hand, for historical reasons, when the modern Western European rule of law order appeared before China, the concrete objects it presented were unequal treaties and extraterritoriality, which were not value-neutral and impartial. In fact, a large number of emerging countries that emerged from colonial rule after the end of the Second World War, like China, had a very strong concept of independence and autonomy, and closely linked the promotion of modernization to the defence of national sovereignty. To put it another way, in a state of imbalance in international power relations, only sovereignty can build a solid wall of national identity and diversity of cultural traditions. Once the sovereign state system falls apart, the so-called symbiosis of values or dialogue among civilizations advocated by the weaker states will easily become empty talk, and even contribute to the kind of "clash of civilisations" predicted by Samuel Huntington. Thus, in China, as well as in many countries in the Third World, there is a certain subtle and

* **JI Weidong:** Distinguished Chair Professor of Law School and University Professor of Liberal Arts and Social Sciences, Shanghai Jiao Tong University, jwdlaw@sjtu.edu.cn

complex tension between the claim to safeguard national sovereignty and the claim to tame the leviathan of sovereignty through the rule of law, and the two may not always be properly balanced. On many occasions, sovereignty reveals itself to be overwhelmingly dominant and powerful.

2 The Four Forces Driving the Metamorphosis of Sovereignty since the End of the 20th Century

The fact that the Nazi regime in Germany brutally abused and even mass-murdered its own Jews and the phenomena of internal racial cleansing and political purging that occurred in some countries fully reveal the possibility of sovereignty's suppression of human rights and the dangers of tyranny. Therefore, after the end of the Second World War, the significance of the internationalization of human rights protection was widely recognised, which to a certain extent sowed the seeds of the relativization of sovereignty. A present-day review of history reveals that there are in fact four main forces driving the metamorphosis of sovereignty, namely, active human rights diplomacy in the 1990s, the rise of online platforms in the 2000s, computer algorithms fuelled by the 2010s, and big language models and generative artificial intelligence in the 2020s. This paper limits the range of discussion to the latter three scenarios, namely the Internet, computers, and AI, all of which are associated with the advanced and applied spread of digital information technologies. Thus, it can also be argued that digital transformation is shaking up the modern sovereign state system.

(1) Challenges from the "Internet Platform Monster"

Based on the birth of the Internet in 1990, with the enhancement of the functions of personal computers and mobile phones, communication among people has become more and more active, and their relationship with each other has become closer and closer. In order to promote people's communication and content enrichment on the Internet, the U.S. Congress passed the new Communications Regulation Act in 1996, which exempted Internet platforms from the responsibility of users for publishing information (defamation liability exemption framework) under Section 230[1]; and at the turn of the millennium, the U.S. enacted the U.S. Digital Copyright Act, which provided a safe haven from copyright liabilities for search engines, network storage, and online libraries (notice plus takedown).[2] U.S. courts have expanded the liability immunity framework to other areas through broad interpretations of the law, giving U.S. online platforms an extremely broad space for development in the early years. The application of the principle of sovereign immunity to digital information technologies, and in particular to online platforms, seems to imply that these platforms are "quasi-sovereign" in the same way as the historical East India Company or the contemporary giant transnational corporations. It is under these legal conditions that interaction on the Internet has been very dynamic and has

1 See Huang Yushuai, "*Tracking U.S. Network Governance: The History, Present and Future of Section 230 of the 'Communications Regulation Act'*", Research on Network Information Law, No. 1, 2021, pp. 203-218.

2 See Wan Yong, "China's Choice of Compulsory Filtering Mechanism in Copyright Law", Law and Business Research, No. 6, 2021, pp. 184-196.

led to the formation, accumulation and application of data of all kinds, finally triggering a true information revolution. At the same time, the Internet of Things, mobile communications, big data, cloud computing, artificial intelligence systems, machine learning, robotics, automation, etc., have been developed through the "Internet plus" approach, which in turn has led to profound changes in the structure of industries and the shape of society, and to innovations in the digital economy.

However, with the discovery of the value of data and its commercial application, Internet companies have begun to consciously use the regulatory power based on computer code and technical specifications to enhance their commercial competitiveness, and their mode of operation has been converted from the original information intermediary to an online community management organisation; the result is the rapid rise of giant online platforms, which has finally led to the emergence of a disparity in the power of the digital economy and the phenomenon of market monopoly. In the face of these e-commerce and technology "platform behemoths", there have been repeated calls for anti-monopoly in cyberspace. The widespread collection, analysis and marketing of data also threatens the security of personal information and privacy, and has led to legal discussions about how to clarify the ownership of the economic value generated by data, whether it is fairly distributed, and how to protect the security and privacy of personal information. In Europe and other countries, norms for data and AI governance have been in the works since 2016; in the United States, courts have been narrowing the interpretation of incentives for online communication since 2008. In 2019, the Judiciary Committee of the House of Representatives of Congress launched an antitrust investigation against four giant online platform technology companies "GAFA". The legal community is engaged in a heated debate over the immunity framework of Section 230 of the Communications Regulation Act. By 2020, public opinion on changes to the law had reached a boiling point, which gradually influenced subsequent legislative proposals and judicial judgements.[3]

China has also adopted a legal policy orientation that encourages digital communication and interaction, allowing big data to accumulate and generate economic value, leading to the formation of online platform giants represented by Tencent, Alibaba, TikTok, Baidu, Ctrip and others. Online platforms are even able to exercise autonomy and regulate trading activities on the platform in place of the government, thereby changing the relationship between established state power structures and components of power (e.g., the right to issue money, the way credit is evaluated and ranked, and the way sanctions are imposed, etc.) through platform governance. For example, the "Sesame Credit" scoring system under the online platform Alibaba, which is linked to the credit history used by "Alipay", not only has an impact on users' ability to rent a car, stay in a hotel, buy insurance, purchase a home, or travel abroad, but also affects law enforcement and the judiciary. Even law enforcement and judicial agencies are seeking cooperation. The Supreme People's Court system signed a cooperation agreement with Sesame Credit, with the aim of linking asset distribution and consumption and whereabouts data to the effectiveness of judicial initiatives such as litigation preservation

3 "*U.S. Supreme Court Opens Hearing on Fate of Big Tech Consensus: Does it Remove 27-Year-Old Internet 'Umbrella'?*" , Punch News, 24th February 2023, https://www.thepaper.cn/newsDetail_forward_22061908.

and judgement enforcement.[4]

However, from 2018 onwards, the impact of the market dominance of these platforms, the tendency of platforms to become empowered, and the security of personal information fuelled by algorithms began to receive widespread attention in China, and legal policies began to be adjusted in an attempt to limit the market behaviours and empowered tendencies of the "platform monsters". 2020 saw Beijing take a categorical counter-attack on large-scale online platforms. In 2020, the Chinese government took a categorical anti-monopoly move against large online platforms, tightening its legal control over them. However, how to appropriately reconfigure the relationship between the corresponding liability of empowered platforms and technological safe havens - in a sense called "technological immunity" -- by drawing on U.S. experience and lessons learned, is of great importance to China. In a sense, it may also be called "technology immunity" -- the relationship between technology immunity and the corresponding liability of authorised platforms is still an important jurisprudential issue for China.[5]

In short, looking back at the development process of "Internet Plus", we can find that the platform governance has challenged and revised the established state power structure and the institutional arrangement of the rule of law, and naturally, the image of a Sovereign Leviathan playing with a group of rich and powerful platform monsters that actively share the responsibilities of the state in various ways will emerge in our mind. and the imagery of a race for control. However, in order to promote innovation and development, the state will also support the platform economy and try to form a win-win co-operation mechanism.[6]

(2) Blockchain, Individual Sovereignty, and the "Algorithmic Power Monster"

In fact, if sovereign states and platform companies join forces, they will also form an unprecedentedly powerful "Algorithm Leviathan" alliance, which will greatly reduce the space for individual choices through the synergy between the hubs of social interactions and the intermediaries of economic transactions. In order to avoid such a state of affairs, it is particularly important to find a peer-to-peer form of the Internet that is individual-based and that strictly protects the privacy that underlies all freedoms.

On 3rd January 2009, Bitcoin went from idea to reality. Since then, transactions on the Internet can be carried out directly between willing customers through the use of blockchain technology, without the need for a specific third party to have exclusive access to the data for processing. In this way, the Internet is transformed into a decentralised structure that does not require intermediaries and hubs, so that each individual has the possibility to take back control of his or her own privacy, and the personal terminal constitutes the point of departure and the centre of communication and interaction with the entire space of information

4 *Supreme Court Joins Forces with Sesame Credit Network to Punish Breaches of Trust to See Results*, Supreme People's Court Website, 20th December 2015, https://www.court.gov.cn/zixun-xiangqing-16351.html.

5 See Shen Weiwei, "*The Practice of Technological Safe Havens and Jurisprudential Reflection*" Peking University Law Journal, 2023, No. 4, pp. 1-17.

6 For example, "*This Symposium Convened by the Premier Releases Positive Signals to Platform Enterprises Again*", the Paper, 13rd July 2023, https://www.thepaper.cn/newsDetail_forward_23827347; "*Firm Confidence in Practicing Good 'Internal Skills', platform economy has great potential*", China Economic Network, 14th July 2023, http://views.ce.cn/view/ent/202307/14/t20230714_38631259.shtml.

relations.[7]

More importantly, the combination of peer-to-peer blockchain technology, smart contract platforms, crypto assets, and cyber trust actually establishes the Self-Sovereign Identity (SSI) of online users in the meta-universe or multi-universe, or forms "The Sovereign Individual".[8] At the end of the 19th century, Nietzsche said that "God is dead" and that faith had collapsed. In the latter part of the twentieth century, Lacan and Foucault proclaimed the "death of the subject" in the name of what could be called "postmodernism", and the individual became a rootless float in the midst of nothingness. In the 2010s, however, the subject created by the Enlightenment, the individual with its a priori nature, came back to life, and in a noisy and reckless way. On many occasions, it has been possible to express this resurgence in terms of the concept of "consumer sovereignty", which has been established in jurisprudence.

In practice, it also means that the algorithm becomes a powerful authority that makes the virtual space operate in accordance with the logic of information-based computation, so that a series of commands from the AI are effectively executed. In the final analysis, the creation story unfolding on the Internet 3.0 is really this: computer language, or the process of communication as an interaction mechanism, or the programme that controls the game, constructs the entire world. Algorithms are not only the order of logic or machine computation, but also a new ecosystem created by human language, an intelligent species that constantly generates a thousand different states, provides huge amounts of data and infinite options in virtual space, and creates the "long-tail effect" in the structure of the network through machine learning. The majority of choices are made by algorithms, but the final choice and the best options remain in the hands of humans. Based on such technological conditions, in fact, since 2012, the US presidential elections have been simulated and predicted by machine learning with big data, and election strategies have been decided accordingly; the results of the 2020 presidential election are also said to be influenced by sophisticated AI technology and proxy bots. In the prolongation of this trend, it can be predicted that some sort of algorithmic power monster will likely turn around and dominate democratic politics.

(3) The "Large Language Modelling Monster" and the "Polanyi Paradox" of Intelligence

Since Google released the "Transformer" network structure in 2017, in just more than five years, the world has rapidly appeared a huge group of large models, which in turn derives from a variety of technical architectures, a variety of modalities, and a variety of scenarios. In terms of the global distribution of released large models, China and the United States are significantly ahead, exceeding 80% of the global total, with the United States consistently ranking the highest in the world in terms of the number of large models. As soon as ChatGPT was announced at the end of November 2022[9], it swept the world due to its strong

7 See [Canadian] Don Tapscott, [Canadian] Alex Tapscott, *The Blockchain Revolution*, translated by Kyle et al, CITIC Publishing Group Corporation, 2016 edition, Chapter 1: Trusted Protocols.

8 On the basic features and advantages of Internet 3.0, see Yao Qian, "*Web 3.0: The Approaching New Generation of the Internet*", China Finance Journal, Vol. 6, No. 6, 2022, pp. 14-17. For a prophetic account of the sovereignisation of the individual, see Cf. James D. Davidson & William Rees-Mogg, *The Sovereign Individual: Mastering the Information Age*, Touchstone Books, 1997.

9 See China Institute of Science and Technology Information, *Report on China's Artificial Intelligence Large Model Map*, published on 28th May 2023, https://k.sina.com.cn/article_6380588872_17c500f4801902pmz9.html.

dialogue capabilities and wide range of applications, bringing the monthly active user scale to 100 million in just two months, an extremely impressive growth rate. Since then, these large language models have been released one after another, which have profoundly affected various social practice scenarios, including legal operation, from the aspects of empowering individuals and reducing the burden of business, leaving a digital "Cambrian" landscape of the explosion of generative AI species. According to incomplete statistics, by May 2023, Chinese science and technology enterprises and online platforms had launched 79 AI language models of various types, of which 34 were general-purpose models.[10]

It has to be admitted that while the big language model brings convenience and benefits to the State and society, it also poses disturbing risks and even threats. In essence, it is the self-learning and in-context learning of multi-layer networks, and the learning of learning methods -- meta-learning -- that is achieved on this basis. In this way, the design of human features becomes meaningless and the AI actually starts to mould itself and thus forms an automated ecosystem. It is here that "Large Language Modelling behemoths" are emerging, and are likely to slip out of human control by abandoning the design of pre-given features in favour of self-imposed sub-goals, raising serious governance issues. This means that large language models as well as GPT-4 Turbo will midwife the birth of a new type of non-human or super-human intelligence that will drift away and develop very different values from those of humans. It also means that in addition to the platform monsters mentioned above, the sovereignty leviathan will face challenges from dozens or even hundreds of powerful large model behemoths, i.e., national sovereignty in the digital realm, or say "digital sovereignty"[11] is facing the challenge of a "100-module war" and the loss of control. Of course, not only sovereign states, but also online platforms and autonomous individuals, and even the operating systems of human civilization are under varying degrees of threat from big language models.[12] However, the concept of "digital sovereignty" clearly reflects the sovereign state's response to the digital transformation of society and its position of self-defence.

In order to prevent the various risks mentioned above from evolving into irreversible disasters, experts and industry leaders have put forward various countermeasures and suggestions, such as suspending the development of large models, achieving value alignment, and strengthening AI regulation.[13] In terms of value alignment alone, for example, the Brookings Institution in the U.S. published Benjamin Larson's article "The Geopolitics of Artificial Intelligence and the Rise of Digital Sovereignty" on 8th December 2022, in which the author argues that the uneven development of AI will lead to growing mistrust between countries, which in turn will lead to the rise of digital sovereignty and the emergence of technological decoupling; the ideo-

10 See He Xijun and Zhang Huina, "*Creating an Industrial Ecology of Artificial Intelligence Big Models*", Economic Daily News, published on 14th June 2023, 5th ed.

11 Cf. EPRS, *Digital Sovereignty for Europe*, July 2, 2020 (at https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf), Frances G. Burwell and Kenneth Propp, *Digital Sovereignty in Practice: The EU's Push to Shape the New Global Economy*, Europe Center of Atlantic Council, October 2022.

12 Yuval Harari, in his speech "AI and the Future of Humanity", Frontiers Forum, 29th April 2023, makes the point that large language models could undermine the operating system of human civilisation, see *Yuval Harari: Artificial Intelligence Manipulation of us may be worse than you think*, the Paper, 1st June 2023, https://www.thepaper.cn/newsDetail_forward_23297386.

13 See Ji Weidong, "*Governance and Legal Challenges of Strong Artificial Intelligence*," Phoenix Weekly, General Issue 833 (2023), http://www.ifengweekly.com/detil.php?id=19376.

logical differences or differences in moral principles may have wider geopolitical implications for the management of AI and information technology; thus ensuring the consistency of AI's values at the international level may be one of the most significant challenges of this century[14]. In any case, this is an unprecedented sea change that will inevitably shape new forms of state and legal existence and promote innovation in the paradigm of order.

3 State Sovereignty Revived by the "Algorithmic Leviathan"

After more than a century of various social experiments and many setbacks, China's modernisation movement seems to have found a realistic and feasible new path in the last two decades, that is, to use digital information technology to further improve administrative efficiency and legal effectiveness, and to realise the goal of full governance without coercion of state power. As a result, the sovereignty leviathan has increasingly taken on the characteristics of an "Algorithmic Leviathan". It can also be said that sovereignty is re-emerging through digital information technology and gaining unprecedented power. Therefore, the concept of "digital sovereignty" has a dual structure, on the one hand, it refers to the risk of national sovereignty being weakened in the digital space, and on the other hand, it implies that sovereignty has taken a digital form and transformed into a kind of "algorithmic leviathan", which has gained a new life and unprecedented magic. The two aspects mirror each other. These two aspects mirror each other in a marvellous paradox.

From a general theoretical point of view, science and technology are inherently important symbols and connotations of modernisation. Going back in history, it can be found that, from Leibniz's mathematical transformation of Roman law to Bianchin's design of the architecture of power and the calculator of happiness, the essence of the entire process of modernisation of the Western European states and the legal system lies in the calculation of cost-effectiveness as well as concepts, so as to appropriately adjust the relationship between the superiority of sovereignty and legitimacy. Modern jurisprudence, in particular, seeks to overcome subjective arbitrariness through axiomatic systems and formal logic, to ensure objective and fair judgements, to achieve the calculability of the market and of society, and thus to justify the monopoly of the state over the exercise of violence, in order to achieve the goal of "justified coercion" as revealed by Weber. From the late nineteenth century onwards, the idea of rationalising power structures has been extended through different intermediary links, such as legal mathematical conception, judicial statistical analysis, legal social engineering, econometric jurisprudence, field research, experimentalist jurisprudence, information retrieval of laws and cases, modelling of big data related to lawsuits, and designing of code frameworks in cyberspace, to the present stage when scientific and technological conditions are more mature, which form a thriving scene of computational jurisprudence and the digital rule of law.[15]

14 See Tsinghua University, *Observations on International Governance of Artificial Intelligence*, No. 127 (18th December 2022), http://aiig.tsinghua.edu.cn/info/1442/1815.htm.

15 See Ji Weidong, "*The Frontiers of Computational Jurisprudence*", Social Science Series, No. 3, 2021, pp. 113-126.

From the perspective of Chinese practice, first of all, the abuse of trial discretion and judicial corruption have greatly shaken the confidence in the judgement of the human brain, and at the same time, it fuels the social expectation of objectivity, neutrality, as well as certainty in computerised sentencing. As a result, the Internet, big data, and artificial intelligence have rapidly gained hasty recognition and widespread application in China's judicial sector since the end of the 20th century, and even the world's rare "smart court fever" has emerged. Generally speaking, artificial intelligence is essentially a system of rules embedded in the system, can cause the rigidity of the legal norms and technical code results, and through the computer system throughout the way to prevent external interference in the judicial judgement, and therefore conducive to strengthening the constraints on the state power, cultivate a law-abiding way of behaviour of the whole population. In this sense, it can be said that AI, and more broadly digital processing, is conducive to the implementation of the spirit of the modern rule of law. Thus, the construction of China under the rule of law after 2014 has in fact been characterised to a considerable extent by the modernisation of the rule of law driven by digital information technology.

On the other hand, however, there are some risks and problems that have to be addressed in a digitised rule of law government and rule of law society. For example, artificial intelligence feeds on data and constantly improves its performance by collecting, analysing, learning and predicting data, thus inevitably breaking through barriers to personal information and privacy as it strives to expand the scale of data, thereby shaking the foundations of freedom to varying degrees. Moreover, in the context of machine learning on big data, especially in an intelligently networked society, algorithms will become difficult for humans to understand and account for as they evolve into powerful forces. This kind of algorithmic black box, in fact, to varying degrees, will hinder the accountability of power, but also promote the avoidance of responsibility and shift the responsibility of the undesirable tendency, and even cultivate a ubiquitous, omnipotent "Algorithmic Leviathan". In the current digital era, the opposite of algorithmic black-boxing is social transparency and personal transparency. Society is full of electronic probes and sensors, as if there are millions of eyes flashing, silently and constantly scanning and analysing all phenomena, and carrying out panoramic and uninterrupted surveillance of people and things. This trap of sight truly realises Bianchin's conception of the Panopticon as "a new form of universal power", and fully confirms Foucault's insights into the modern state and law.[16]

In Foucault's theoretical vision, we can indeed observe another aspect of the connotations of modern power and the rule of law: surveillance and discipline, unobtrusive observation, recording, analysis and intensive calculation. According to him, the distinction between rationality and irrationality creates a space of exclusion, but power can domesticate and discipline individuals and govern and facilitate society without relying on coercion; the legal order is essentially this diversity of power techniques and their composites with regard to governmentality, not only in the operation of political institutions, but also, broadly speaking, in policing, and also in determining the rights of individuals. It includes not only the operation of political

16 See [French]Michel Foucault, *Discipline and Punishment*, translated by Liu Beicheng and Yang Yuanying, Sanlian Bookstore, 1999 edition, Chapter 3, "Panoramic Openness", on the architectural design of Bianqin's circular prison.

institutions, but also policing in a broader sense, as well as the overall framework and even the various mechanisms of adjustment that determine the interactions between individuals and the government. According to Foucault, modern law is a carefully planned and sustained operation that involves strategies of domination, but also imperfections and opportunities for failure; as such, it operates in isolation from power, but is thus accompanied by elements of resistance and politicisation. On the other hand, however, law as an operational art presupposes a spectrum of knowledge, including science and technology, and relies on institutions of truth and variable culture-power relations.[17] Although not without prejudice, an understanding of the process of modernisation of the state and the law in terms of the omnipresent dimension of the "Great Surveillance" does contain insights and reflections on certain aspects or dimensions of modernisation and its rule of law connotations, which deserve to be re-examined and re-experienced with a new appreciation of the flavour.

During the three year's protection and control of the Covid-19, social governance through digital information technology has become more commonplace and has continued to evolve. In issuing "restraining order", adopting measures to lockdown cities and roads, carrying out "hard quarantine" and "house-to-house disinfestation", and achieving "Electronic Monitoring" through "electronic forbidding leave" pop-ups and assigning red codes, it has become a common practice to use digital information technology in social governance. "The sovereign state has re-emerged, and is even more powerful, through pop-up windows and red codes that "electronically shackle" certain groups of people. At the same time, however, the relativisation of sovereignty is also being extended on specific paths, through the use of blockchain for distributed community governance, and the emergence of various self-organising mechanisms in Shanghai during the 2022 control period (e.g. the "head of the delegation" who is responsible for scheduling the necessities of life, and the "head of the building" who organises the testing of nucleic acids). The side of the relativisation of sovereignty also extends on a particular path. The revival of sovereignty and the retreat of sovereignty seem to be going on at the same time, forming a dialectical relationship between the hard and the soft, and the opposite of each other. The complexity of this intersection of strict regulation with autonomy and co-rule through the Internet, big data, and artificial intelligence reminds us of the findings of the sociology of Leon's law.

Professor David Leon of the Faculty of Law at Queen's University began his research on the "electronic eye" in the 1980s, and published a series of internationally influential monographs such as *The Surveillance Society* and *Cultures of Surveillance*, and is considered to be a pioneer in surveillance theory. Starting from Bianchin and Foucault's metaphor of the circular list device, he examined the evolution of surveillance from state and corporate-led to public participation, and recently proposed the concept of "surveillance culture" based on big data. In particular,[18]Professor Lyon highlights the relevance of digital information technologies to surveillance for safety, health and convenience, arguing that from the self-tracking monitoring of health status by individuals (e.g. pedometers, blood pressure and heart rate bracelets, mobile phone medical check-up apps), to the monitoring of customer behavioural histories by corporations, and the predictive sur-

17 Ibid., pp. 193.

18 Cf. David Lyon, The Electronic Eye: The Rise of Surveillance Society, University of Minnesota Press, 1994; David Lyon, Surveillance Society: Monitoring Everyday Life, Open University Press, 2001, and David Lyon, The Culture of Surveillance: Watching as a Way of Life, Polity Press Ltd., 2018.

veillance of crime by governments, there is a virtual complicity between the watcher and the watched. In this sense, a flexible surveillance society has emerged in the intertwined situation of care and control. The horror of epidemics has dramatically increased people's awareness of risk and their tolerance and support for surveillance initiatives, and has even given surveillance a certain aesthetic and democratic participatory flavour as it moves from the surface to the inside.[19]

From this, it can be seen that the sovereignty of the State, which has become powerful again as an "Algorithmic Leviathan", sometimes indeed reigns supreme, but more often than not, it has melted into the digital network and turned into a piece of programming code for interactive relations. In other words, the original sovereign state has been transformed into a larger, but more multifaceted and flexible "Algorithmic Leviathan", which has become even more powerful in terms of social governance.[20] Especially after entering the AI 4.0 stage, AIGC has dismantled the barrier between language and value, and the multilingual and multimodal working mechanism of the large language model naturally promotes the interaction between internationalisation, globalisation and national sovereignty, which in turn stimulates the sense of identity of the nation-state. In fact, the idea of "digital sovereignty" implies that state power is rediscovering its localised, block-based foothold. In light of the challenges posed by algorithmic power monsters such as the cyber-platform monster, the large language model monster, the personal sovereignty monster, and the agent robot, and in the face of the current "war of all models against all models", the Chinese government has so far responded by taming the platform monster through strict anti-monopoly measures, supporting dozens of large model monsters through a unified supercomputing ecosystem and a costly base model, preventing the risk of uncontrolled peer-to-peer interactions between sovereign individuals through strict regulation and sovereignty blockchain,[21] and constraining the activities of the NPCs or the BOTs through protection configurations and countermeasure strategies.

For example, the concept of "the sovereign blockchain" was first proposed by the white paper "Guiyang Blockchain Development and Application" in 2016. Although it has the same characteristics as other blockchains, such as distributed, tamper-proof, mutually trustworthy, and transferring value through smart contracts, it injects the sovereign will of the state into the blockchain, and strengthens government surveillance, technical intervention, and thus has the characteristics of non-completely decentralised blockchain. Chain's government surveillance and technological intervention, and thus has the characteristic of non-complete decentralisation. According to the conceptual definition made by the National Science and Technology

19 See Ji Weidong, "*Epidemic Surveillance: a Comparative Law Sociology Analysis*", Peking University Law Journal, Vol. 3, 2020, pp. 565-589.

20 The four phases of AI development are (1) 1950s-1960s, the emergence of AI terminology, Turing test, neural network models, LISP language; (2) 1970s-1990s, the emergence of PROLOG language, expert system development, AI industrialisation, machine learning, cognitive network renaissance, genetic rhyming, and reinforcement learning; and (3) 2000-2022, the latest achievements include deep learning, Watson's victory over humans in question-answering contests, Generative Adversarial Network, AI's ability to accurately identify portraits surpassing human beings, and the "Alpha Go" system's victory over the world's top professional chess players; (4) 2023, afterwards, the development of generative AI, the rise of linguistic macromodels, and the dawn of general-purpose AI are on the horizon.

21 In stark contrast, the US Congress passed the Blockchain Regulatory Certainty Act on 26th July 2023, which provides clearer guidance on the regulation of those preventing blockchain risks, in order to prevent the infringement of digital assets.

Nomenclature Validation Committee in 2017, a sovereign blockchain is a blockchain based on a distributed ledger, with rules and consensus at its core, and with national sovereignty as a prerequisite. In this context, rules mean "code plus law", consensus emphasises "people" rather than "numbers", and favours "poly-centralization" rather than "decentralization".[22] According to Long Rongyuan, Executive Vice President of Guiyang Institute of Innovation Driven Development Strategy, "Sovereign blockchain is not only an integrated technology and a data revolution, but also an order reconstruction, and an inflection point of an era, which has become a cutting-edge force in the reconstruction of global governance".[23]

Another example is that, in response to the soaring demand for large-model computing power in the "Battle of 100 Models", the Ministry of Science and Technology initiated the establishment of a national "supercomputing Internet" consortium on 17th April 2023 to connect a large number of supercomputing centres throughout the country through the computing power network to build a "grand unified" computing power service platform.[24] On 7th July, at the World Conference on Artificial Intelligence, the National Artificial Intelligence Standardization Group under the guidance of the National Standards Committee announced the establishment of the first large model standardisation thematic group, which is headed by the National Science and Technology Commission. The first large model standardisation thematic group, jointly responsible by the Shanghai Artificial Intelligence Laboratory, Baidu, 360, Huawei, Alibaba and other enterprises, officially launched the development of national standards for large model testing.[25] Apparently, the goal is to promote the combination of large models and standardisation, forming a division of labour pattern in which head technology enterprises focus on industry large models, the state promotes universal large models, and creates a new pedestal for high-quality development. Including Beijing Zhiyuan Artificial Intelligence Research Institute 2023 June release of the AIGC underlying pedestal Skyhawk-Aquila, the pedestal model generally requires more than one hundred billion data for training, the number of parameters will also reach more than tens of billions of levels, and only on such a basis can we build a very good general large model and generate emergence capabilities. It can be imagined that the "big unified" base and general large model concept can avoid repeated investment, blind development, industrial involution. However, this kind of thinking is not only based on the rational calculation of cost-effectiveness, but is also obviously conducive to the maintenance of digital sovereignty and the strengthening of the centralising effect of the power of the Algorithmic Leviathan.

22 Regarding the ins and outs of sovereign blockchain, relevant literature can be found in *Sovereign Blockchain 1.0: The Internet of Order and the Community of Human Destiny*, edited by Lian Yuming, 2020 edition, Zhejiang University Press; *Sovereign Blockchain 2.0: The New Power to Change the Future World*, edited by Lian Yuming, 2022 edition, Zhejiang University Press; *Sovereign Blockchain 3.0: Reconstruction of Global Governance under the Order of Sharing*, edited by Lian Yuming, Zhejiang University Press, 2023 edition.

23 See "*Sovereign Blockchain Becomes a Frontier Force for Global Governance Reconstruction*", Guizhou Daily Contemporary Pioneer, 28th May 2023, http://www.ddcpc.cn/detail/d_guizhou/11515116165400.html.

24 See "*Ministry of Science and Technology Launches Deployment of National Supercomputing Internet*", in Digital Economy Insight Weekly, No. 15, 2023, https://insights.zhiding.cn/2023/0420/3148891.shtml.

25 See "*The Large Model National Team is Coming! 360, Baidu, Huawei, Alibaba and Others Enter the Game*", Shanghai Securities News, China Securities Network, 7th July 2023, https://news.cnstock.com/news,bwkx-202307-5087478.htm.

4 Towards to the Legal and Technological Due Process of Algorithmic Leviathan

From the above analysis, it can be seen that, on the one hand, the magic of state sovereignty-based the Algorithmic Leviathan seems to be able to reach no farther; on the other hand, this inevitably reinforces the frequent and continuous interactions between governmental institutions and powerful network platforms, sovereignized individuals hidden in blockchains, large language models with generalisability, and agent bots influencing political power games. In such a complex and fluid state, in order to prevent the abuse of big platforms and large models through the embedded impartial procedures of AI systems and the power-sharing and check-and-balance mechanisms between different AI systems, and also to check and balance that unique the Algorithmic Leviathan and its privatized variants, the principle of procedural justice of the modern rule of law will also be redefined and play a more important role.[26] In a certain sense, it can also be said that finding the best way to combine legal and technical due process is the main rule of law connotation for the AI-driven digital state to continue to advance the cause of modernisation in the future.

By "due process" or legal process consistent with justice, we mean the institutional apparatus that ensures that argumentative dialogue proceeds smoothly under conditions of freedom and equality, and certainly not computer programmes or procedural controls through artificial intelligence systems. But in the digital age, procedural law often needs to be converted into the code of a computer programme to function. As Mark Stefik has pointed out, the code "determines what kinds of people can access what kinds of networked entities... How these programmes regulate human interrelationships...depends entirely on the choices made."[27] It is very interesting to note that it is the code that connects procedures with choices and human relationships. This also signals the possibility that code has the potential to constrain and improve algorithmic facilitation through technical justification processes. The so-called "technical justification process" addresses, among other things, how code and its framing should be appropriately regulated, who the authors of the code are and who can control the authors of the code, whether there is an ex ante process of justification or ex post process of correction of the code's appropriateness, and how the powers and responsibilities of the intermediary ISPs should be configured, What kind of regulations apply to the development of software that applies data streams, whether there are restrictive conditions set for digital surveillance and web searches, and a host of other issues related to the legitimisation of the process. In a nutshell, the essence of technically justified processes is code regulation. If this regulation of code also takes the form of law, it is possible to find intersections and combinations between technical due process and legal procedural justice or "procedural due process".

26 See Ji Weidong, *Exploring the Significance of Legal Procedures in the Digital Age - Focusing on Algorithmic Dictatorship and Procedural Fairness in Risk Prevention and Control Administration*, Journal of China University of Political Science and Law 2023, No. 1, pp. 83-99. Cf. Danielle Keats Citron, Technological Due Process, 85(6) Washington University Law Review 1249-1313 (2008). Liu Dongliang, *Technological Due Process: Double Variations of Procedural Law and Algorithms in the Age of Artificial Intelligence*, Comparative Law Studies, Vol. 5, No. 5, 2020, pp. 64-79.

27 See [American] Lawrence Lessig, *Code: And Other Laws in Cyberspace Version 2.0 (Revised Edition)*, translated by Li Xu and Shen Weiwei, Tsinghua University Press, 2018 edition, p. 7.

As a prerequisite for due process, there is also a need for a basic consensus in society to provide value standards for the design of procedures. In other words, procedures need a contractual basis. Faced with the reality of digital sovereignty on its own and the omnipresence of the the Algorithmic Leviathan, Secretary-General António Guterres had announced an initiative on the Global Digital Compact in September 2021, and the United Nations also formally released a policy brief "Global Digital Compact - Creating an Open, Free and Secure Digital Future for All" in May 2023, and seeks views from all sectors. The Global Digital Compact will be based on universal human rights and establish a global framework through the cooperation of various stakeholders to advance an open, free, secure and people-centred digital future and achieve the goal of sustainable development. In line with this vision, Member States should establish advisory mechanisms on digital human rights; protect the free and shared nature of the Internet as a truly global public good; establish strong accountability standards for online platforms and users, and strengthen the cooperation of online security commissioners in different jurisdictions; achieve harmonisation of data governance principles; and form a framework for the agile governance of artificial intelligence; and so forth.[28] China has already submitted its views on the Global Digital Compact to the United Nations, and[29] if things go well, a basic international consensus on the Global Digital Compact will be reached at the Future Summit of the United Nations to be held in September 2024.

The above thoughts cannot help but rekindle Hobbes' grand narrative of the sovereign Leviathan and the social contract. In a sense, it can also be said that the UN's Global Digital Compact seems to be an important proposal for a new social contract in the digital age against the omnipotent Leviathan that combines sovereignty and algorithms, demonstrating a more or less universal vision of digital constitutionalism and the digital rule of law. However, how the digital rule of law actually restrains the Algorithmic Leviathan, and whether it can truly lay a new foundation of legitimacy for cyberspace is still a topic to be observed and explored in depth in the future.

28 United Nations, A Global Digital Compact: An Open, Free and Secure Digital Future for All (Our Common Agenda Policy Brief 5, May 2023).

29 See "*China's Position on Issues Concerning Global Digital Governance*", Ministry of Foreign Affairs of the People's Republic of China, April 2023, https://www.mfa.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/zclc_674645/qt_674659/202305/t20230525_11083602.shtml.