Asian Journal of Law and Society (2024), **11**, 418–434
doi:10.1017/als.2024.29

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

The Transmutation of Sovereignty: Digital "World of Warcraft" and Innovation in the Chinese Legal Order

Weidong Ji

China Institute for Socio-Legal Studies, Shanghai Jiao Tong University, China
Email: jwdlaw@sjtu.edu.cn

Abstract

This article analyses the paradoxical relationship between the relative decline and resurgence of national sovereignty in the context of economic and informational globalisation, the rise of mega-platforms, the sovereign individuals hidden within blockchains, and large model behemoths free from the feature design of programming. It highlights how the decline of sovereignty has given rise to concepts such as "the digital sovereignty" in Europe and "the sovereign blockchain" in China, while the resurgence of sovereignty has led to theories like the "surveillance society" in North America and the "electronic forbidding leave" metaphor in China. In any case, with the AI-driven era, "the Algorithmic Leviathan" is becoming an extremely powerful dominating force that countries and laws must confront. To prevent its runaway abuse, it is necessary to consolidate a basic consensus through global digital compacts and institutionalise it through legal and technical due process—this is the essence of the digital rule of law.

Keywords: digital sovereignty; platform governance; large model behemoths; the sovereignty individual; the Algorithmic Leviathan; Global Digital Compact

1. Introduction: Signs of modernisation in the domestic order and international relations

An important symbol of Western European-style modernisation was the formation of the institution of the sovereign state.

Looking back at the relevant historical background, it was with the outbreak of the Italian War in 1494 that the long and frequent wars between the Holy Roman Empire and the Kingdom of France began to revolve around the hegemony of Europe and involved many countries, such as England. In the midst of the conflagration, the countries had to strengthen their tax collection capacity, improve their administrative efficiency, and enhance their sectional organisational structure in order to adequately deploy their military expenditures and armaments, thus promoting the unification of the domestic market, as well as the centralisation of dominance. In order to do so, it was necessary to demarcate national boundaries and establish the principle and order that only the monarch could represent the state. In this process, the concept of sovereignty emerged, which constitutes the basis and symbol of the modern nation-state.

A plurality of sovereigns, in the midst of fierce competition, adopted mercantilist policies with the primary goal of enriching their countries and strengthening their armies, and a strong system of state rule known as "absolute kingship" emerged. It was under the great changes of the great powers' rivalry and capital accumulation that Jean Bodin (1530–1596) of France founded the theory of sovereignty on the independent status of sovereign

states not subject to external control, the sovereign's supreme power over citizens to make decisions above the law, and the indivisibility and transferability of ruling power (Bodin, 2008); Thomas Hobbes (1588–1679) of England, on the grounds of freeing the free individual from the state of nature of "war of all against all", particularly emphasised the absolute and supreme nature of the sovereignty of the state internally.[1] Hugo Grotius (1583–1645) of the Netherlands, on the other hand, based on the premise of this view of state sovereignty, advocated the application of the theory of natural law to the relationship between states (international conflicts are actually closer to the so-called "war of all against all"), in order to moderate the intensity of foreign killings, as well as the peace-seeking order of international law and even of the oceans (Xiong, 2014, pp. 20–27).

Thus, 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.

2. The sovereign State as a Leviathan and its constraints

The state enjoys almost unlimited power because of the idea of sovereignty, and it has become a magical god that can dominate everything. Hobbes called this sovereign state "Leviathan," the supreme spirit. He explained the underlying logic of the sovereign state in this way:

> *. . . is to confer all their power and strength upon one man, or upon one assembly of men, that may reduce all their wills, by plurality of voices, unto one will . . . This done, the multitude so united in one person is called a Commonwealth . . . This is the generation of that great Leviathan . . . to define it, is: one person, of whose acts a great multitude, by mutual covenants one with another, have made themselves every one the author, to the end he may use the strength and means of them all as he shall think expedient for their peace and common defence (Hobbes, 2013, pp. 131–132).*

Obviously, such a sovereign state is like a container of all powers. Here, law can be understood as the command of the sovereign, which also constitutes the common code of behaviour of society. Hobbes even argues that, in order to prevent a return to a state of mutual strife and to implement the emergency plan for the prevention and control of the Black Death epidemic, the authority of the State should be unshakeable and absolute, and for this reason, freedom of religion, thought and expression cannot be recognised (Hobbes, 2013, pp. 133–142).[2]

It goes without saying that Hobbes presents a design for "unlimited government." Here, the principle of contract exists, in fact, only in the mutual behaviour of individuals and does not apply to the relationship between the State and all individuals. Hobbes thus closes the door to the so-called double trust that Frederick Maitland later elaborated (Maitland, 2008). And, of course, he rejected Locke's idea of "limited government" and the right of the people to resist tyranny. Very similar to the Hobbesian view of state sovereignty were the ideas of the Chinese legalist Shang Yang (B.C. 390–B.C. 338) of the Qin during the Warring States period about the "supremacy of the sovereign and the rule of the state as a single entity." As Fukuyama points out, China has been a strong executive state since the Qin dynasty, with a certain precocious modernity. As early as the Qin dynasty, he argues, China alone created the modern state in the Weberian sense, i.e., it succeeded in developing a

[1] The relevant literature is endless; for example, Wang (2015), pp. 109–119.

[2] On the relationship between medical administration and the modern sovereign state "Leviathan", see Lan (2020), pp. 1–10; for a more specific account of the modern state's power of discipline and social domination through epidemiological and medical care, see Foucault (2011).

centralised, unitary bureaucratic government, putting an end to feudalism (Fukuyama, 2014, pp. 104–111). The Chinese social revolution of the twentieth century, in fact, created a mega-Leviathan with a long arm for the private sphere as well, building on the modern notion of sovereignty; for a while, it was as if the idea of "unlimited government" had been carried to the extreme, and the tentacles of hierarchical power had to be extended not only to all the people of society but also to their brains.

It has to be admitted that the Sovereign Leviathan, with its unlimited power, is, in fact, very dangerous for individuals, or at least it can easily stifle the vigour of innovation. In order to restrain that increasingly powerful Sovereign Leviathan, the institutional guarantees of freedoms and rights need to be strengthened in particular. To borrow Immanuel Kant's formulation, there is a need to make the individual's natural rights the cornerstone of justice and embed them in the framework of the state's rights system through the idea of contract (Zhang, 2013, pp. 5–17). Therefore, in Western Europe, under the influence of Enlightenment thought and the social revolution movement, Britain passed the "Bill of Rights" in 1689, announcing the birth of parliamentary sovereignty;[3] in 1789, France promulgated the Declaration of Human Rights, and the United States put into effect the Federal Constitution, both of which respectively clarified the design of the political framework of the "principle of popular sovereignty" and the "separation of powers."[4]

In this process, claims of sovereign superiority and claims of sovereign legitimacy collide and intermingle with each other, forming a paradox with dialectical overtones of the modern nation-state: if the state treats its citizens as political subjects, then the citizens will be happy to subject; conversely, if the state treats its citizens as objects of domination, then the citizens will choose to object.[5] In short, 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 realise 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. Nevertheless, during the three hundred years from the late seventeenth to the late twentieth century, the modern rule of law order as a whole was still based on the system of sovereign states.

However, 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. Thus, similar to Japan, China's modernisation of the rule of law was not motivated by internal spontaneous needs, but rather by the pressure of external shocks, which could easily give rise to a very strong sense of victimhood and a tendency to resolutely defend national sovereignty. 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 modernisation 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 civilisations advocated by the weaker states will easily become empty talk and even contribute to the kind of "clash of civilisations" predicted by Samuel Huntington (Huntington, 2018, p. 142). Thus, in China, as well as in many countries in the Third World, there is a certain subtle and complex tension between the claim to safeguard national sovereignty and the claim to tame the Leviathan of

[3] On the transmutation of the principle of British parliamentary sovereignty, see Xiang (2010).

[4] On the similarities and differences between French and American sovereignty in the design of the civil and state systems, see Liu (2022), pp. 82–94.

[5] This dialectical relationship is also typical of the modernisation process of transforming subjects into citizens in Japan; see Makihara (1998), pp. 15–16.

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.

3. The four forces driving the metamorphosis of sovereignty since the end of the twentieth century

The fact that the Nazi regime in Germany brutally abused and even mass-murdered its own Jews, along with the phenomena of internal racial cleansing and political purging that occurred in some countries, fully reveals 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 internationalisation of human rights protection was widely recognised, which, to a certain extent, sowed the seeds of the relativisation of sovereignty. Since the 1970s, the United States has made human rights one of the major themes of its diplomacy, and in the 1990s, it further put forward the slogan of "human rights without borders" and actively intervened in the internal affairs of other countries.[6] On the other hand, starting from the dramatic changes in the Soviet Union and Eastern Europe in 1989, the flood of globalisation in investment, trade, finance and information rapidly swept over all countries, and correspondingly, sovereignty was gradually further relativised and transformed, with the emergence of the conception of a world order of the rule of law based on the two pillars of the World Trade Organisation (WTO) and the World Wide Web (WWW). 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.

3.1 Challenges from the "Internet Platform Monster"

Based on the birth of the Internet in 1990, along with the enhancement of the functions of personal computers and mobile phones, communication among people has become more active, and their relationships with each other have grown 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 for users publishing information (defamation liability exemption framework) under Section 230 (Huang, 2021, pp. 203–218). At the turn of the millennium, the United States 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) (Wan, 2021, pp. 184–196). 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

[6] Both the Chinese Government and academics are critical of the "human rights without borders" theory and emphasise that sovereignty is the basis for human rights protection. Relevant literature includes, for example, Xu (1992), pp. 42–54; China Society for Human Rights Studies (2001). Some representative experts also emphasise that the right to life and the right to development are the first and foremost human rights; for example, Li (2019), pp. 3–7; Li (2010). On the triadic interlocking relationship between sovereignty, human rights, and hegemony, see Ji (2000), pp. 87–96.

way as the historical East India Company or contemporary giant transnational corporations. Under these legal conditions, interaction on the Internet has been very dynamic and has 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, as well as to innovations in the digital economy.

At a brainstorming forum in 2004, Tim O'Reilly, founder and president of O'Reilly Media, advocated the concept of "Internet 2.0," which involves a two-way exchange of information, attempting to cut through the previous one-way flow of information on the Internet. He stressed that Internet 2.0 has seven basic features; for example, "users can not only read but also write," and a new function: to promote enterprises to strengthen interaction with users through network computing platforms and to improve marketing and services based on the analysis of big data regarding users' whereabouts and preferences, predictions, and tailored algorithms. This algorithmic boost constitutes a powerful force that, in some cases, can even dictate and significantly improve the efficiency of the economy. Clearly, this is an enterprise perspective on the Internet of everything.

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 (Wu, 2023).

In the Internet 2.0 phase, 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 and judgement enforcement (The Supreme People's Court of the People's Republic of China, 2015). 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, and legal policies began to be adjusted in an attempt to limit the market behaviours and empowered tendencies of the "platform monsters." In 2020, Beijing took a categorical counter-attack on large-scale 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 (Shen, 2023, pp. 906–922).

In short, looking back at the development process of "Internet Plus," we can find that 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 minds as 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 cooperation mechanism.[7]

3.2 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 "Algorithmic 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 1 November 2008, a mysterious figure known as "Satoshi Nakamoto" published a paper on Bitcoin, a peer-to-peer electronic currency system and medium of exchange, via a cryptographic mailing list, demonstrating the basic principles of blockchain technology (Nakamoto, no date).[8] On 3 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 their own privacy, and the personal terminal constitutes the point of departure and the centre of communication and interaction with the entire space of information relations (Tapscott and Tapscott, 2016, pp. 2–32). In China, if all 1.4 billion people constitute terminals, weave self-centred cobwebs, and shape a "small universe," what a spectacular and complex landscape it will be!

[7] For example, see Fan and Li (2023).

[8] According to Elon Musk's Twitter revelations in early March 2022, the mysterious author is, in fact, a fictional character with the initial letters of the English names of four prominent international corporations (Samsung, Toshiba, Nakamichi, and Motorola) combined.

The use of blockchain technology not only allows for the definition and protection of individuals' legal rights to the economic value of data, but also allows for the creation of a wide variety of platforms with diverse and generalised objectives. For example, Ether, which was publicly established in late 2013, is the most widely known blockchain-based smart contract platform that can fulfil multiple layers of diverse functions. Thus, Gavin Wood rediscovered and innovated the concept of Internet 3.0 in an article tweeted on 17 April 2014 (Wood, 2014). In his view, Internet 3.0 is a decentralised Internet based on blockchain and an Internet where users enjoy autonomy and mutual trust, and therefore also a physicalised Internet for everyone. In fact, it took another six years until 2020, after the rise of Decentralised Finance (DeFi) and the explosive growth of Non-Fungible Tokens (NFTs), for humanity to truly move into the era of Internet 3.0.

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, and forms "The Sovereign Individual."[9] At the end of the nineteenth 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 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 the final analysis, it is a flexible individual sovereignty open to others, requiring a constant self-centred experimentation with power and the weaving of social relations, and, in turn, subject to the constraints of such relations with the other. But in any case, the move from state sovereignty to individual sovereignty is a qualitative change in the principles of social order induced by blockchains, Internet 3.0, and the meta-universe, which will inevitably lead to innovations in models of state governance and legal paradigms (Ji, 2023a, pp. 9–10, 45).

It is necessary to point out that in blockchain games, AI plays a very important role as a non-player controlled character (non-player character, NPC) in the virtual space, as an analyst and problem solver of huge amounts of data, or as a proxy bot (BOT, i.e., a smart tool that plays the game automatically) for certain users. In most chain games, though, proxy bots are forbidden. However, on those occasions where their use is permitted, there will be a group of people who install proxies into many computers for the purpose of showing off or profit, and through their management and manipulation, they can achieve the goal of dominating and monopolising digital resources. In this sense, the application of AI actually becomes the privilege of that small group of players, a tool to kidnap and control other users, forming a pattern of confrontation and struggle between humans and machines (AI) (Ji, 2023a, pp. 163–166).[10] Here, one can find a phenomenon similar to the "theatre state" (Geertz, 2014, pp. 490–522; Geertz, 2018, pp.12, 98ff.) described by Geertz through deep games such as the Bali cockfighting event. It can also be called a group of "algorithmic power monsters" or the so-called "privatised Algorithmic Leviathans," which activate the symbolic meaning of glory in virtual world games, subordinating all resources to shiny rituals and rules of the game.

In practice, the NPC also means that the algorithm becomes a powerful authority that makes the virtual space operate in accordance with the logic of information-based

[9] On the basic features and advantages of Internet 3.0, see Yao (2022), pp. 14–17. For a prophetic account of the sovereignisation of the individual, see Davidson and Rees-Mogg (1997).

[10] The problem of algorithmic power and algorithmic dictatorship brought about by AI has been summarised as the "Seviathan" phenomenon, which needs to be domesticated by humans through governance mechanisms and laws. For reflections on this aspect, see Gao (2018), pp. 200–206.

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 U.S. 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.

3.3 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 emerged as a vast group of large models, which in turn derive from a variety of technical architectures, modalities and 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 (Institute of Scientific and Technical Information of China, 2023), it swept the world due to its strong 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 on businesses, 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 (He and Zhang, 2023). By the end of October 2023, the number of AI big models had reached 238, almost three times in five months.

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. Four of them can be cited as follows. First, as ChatGPT-like large language models provide online dialogue services, they can collect more personal information and privacy than established Internet search engines. Therefore, in the case of "knowing too much and having conflicting interests", large language models and their operators may induce users to make choices against their own intentions and interests by controlling communication. Secondly, the current stage of the big language model will treat things that do not and cannot exist in the training data as real and describe them in an unquestionable tone in the dialogue. This is the phenomenon of "serious nonsense" that users often complain about. From a scientific and technical point of view, this is, of course, only a kind of "hallucination." The phenomenon of "hallucination" is closely related to the generalisation ability of machine learning to handle unlimited unknown data with limited training data. However, in application scenarios, this hallucination can lead to the spread of false information, which can be fatal to users or society. Once again, big language models may raise complex issues of intellectual property identification and protection when they use various data for

learning or when AI automatically generates various contents. In order to ensure the credibility of AIGC and to clarify responsibilities, digital watermarking techniques should be invented, applied, and promoted. Lastly, large language models may intentionally or unintentionally access confidential information of enterprises or government agencies, manipulate public opinion, and lead to loopholes in the security system of the central system of the State, dysfunction of the information society, or even unrest due to malicious accidents and crimes.

Much of the human processing of language and harnessing of intelligence actually takes place unconsciously. Philosopher of science, Michael Polanyi, once noted in 1964, "Man knows far more than he can say."[11] In other words, the knowledge system should also include such tacit knowledge that is not explicitly realised, or not recognised by the common sense of the society, or cannot be verbalised. This proposition has been expressed as "Polanyi's paradox" and has become the basis of the theory of artificial intelligence (Pan, 2020, pp. 23–29). This also means that AI's processing of unconscious language simply cannot design the kind of algorithms that acquire and apply all languages, and it is difficult to set clear training goals for machine learning. The now-prevailing machine learning using neural networks gradually reduces the error by continuously adjusting the neuron weights and updating the network parameters through an error back-propagation algorithm to find a positive solution to the training data. It has been found that the accuracy of AI solitaire predictions suddenly and dramatically improves when the size of the neural network is dramatically scaled up. This discovery and its conscious application brought machine learning into the deep learning stage: without the need for complex rules and learning methods, simply multiplying the size of the network can make many difficult problems solved and rapidly improve generalisation—it goes without saying that this magical effect also proves the importance of large language models. 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 big language models 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"[12] 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 civilisation are under varying degrees of threat from big language models (Harari, 2023).[13] 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 (Ji, 2023b). In terms of value alignment alone, for example, the Brookings Institution in the United States published Benjamin Larson's article "The geopolitics of artificial intelligence and the rise of digital sovereignty" on

[11] The Chinese formulation of Polanyi's paradox is quoted in Brynjolfsson and McAfee (2017).

[12] Cf. EPRS (2020); Burwell and Propp (2022).

[13] Yuval Harari, in his speech "AI and the Future of Humanity", Frontiers Forum, 29 April 2023, makes the point that large language models could undermine the operating system of human civilisation; see Harari (2023).

8 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 ideological 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 (Institute for AI International Governance of Tsinghua University, 2023). 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.

4. State sovereignty revived by the Chinese style "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. 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 (Ji, 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 twentieth 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, which 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 Bentham's conception of the Panopticon as "a new form of universal power," and fully confirms Foucault's insights into the modern state and law.[14]

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 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 (Foucault, 1999, p. 193). 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,

[14] On the architectural design of Bentham's circular prison, see Foucault (1999), pp. 224–242.

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 (Lyon, 1994, 2001, 2018). In particular, 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 surveillance 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 (Ji, 2020, pp. 565–589).

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.[15] 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,

[15] The four phases of AI development are (1) 1950s–1960s: the emergence of AI terminology, the Turing test, neural network models and the LISP language; (2) 1970s–1990:, the emergence of the PROLOG language, expert system development, AI industrialisation, machine learning, cognitive network renaissance, genetic rhyming, and reinforcement learning; (3) 2000–2022: the latest achievements include deep learning, Watson's victory over humans in question-answering contests, the 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; and (4) 2023 onwards: the development of generative AI, the rise of linguistic macromodels, and the dawn of general-purpose AI are on the horizon.

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,[16] 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 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".[17] 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" (Yuan, 2023).

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 17 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 (Sun, 2023). On 7 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 (Donews, 2023). 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

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

[17] Regarding the ins and outs of sovereign blockchain, relevant literature can be found in Lian (2020, 2022, 2023).

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, and 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.

5. Conclusion: Procedural justice in the interaction between the Algorithmic Leviathan and digital monsters

From the above analysis, it can be seen that, on the one hand, the magic of state sovereignty-based 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, sovereignised 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 Algorithmic Leviathan and its privatised variants, the principle of procedural justice of the modern rule of law will also be redefined and play a more important role (Ji, 2023c, pp. 83–99; Citron, 2008, pp. 1249–1313; Liu, 2020, pp. 64–79). 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."(Lessig, 2018, p. 7). 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."

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 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 (United Nations, 2023). China has already submitted its views on the Global Digital Compact to the United Nations (Ministry of Foreign Affairs of the People's Republic of China, 2024), and 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.

References

Bodin, J. (2008). *Zhuquan Lun [The theory of sovereignty]*, in Franklin, J. H. (ed.), Translated by Li, W. H. and Qian, J. W. Beijing: Peking University Press.

Brynjolfsson, E. and McAfee, A. (2017). *The business of artificial intelligence*. Available at: https://hbr.org/2017/07/the-business-of-artificial-intelligence (Accessed: 9 October 2024).

Burwell, F. G. and Propp, K. (2022). *Digital sovereignty in practice: The EU's push to shape the new global economy*. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2022/11/Digital-sovereignty-in-practice-The-EUs-push-to-shape-the-new-global-economy_.pdf (Accessed: 15 August 2024).

China Society for Human Rights Studies. (2001). *Lun renquan yu zhuquan: Jianbo "renquan gaoyu zhuquan" lun [On human rights and sovereignty: Refuting the theory of human rights above sovereignty]*. Beijing: Contemporary World Press.

Citron, D, K. (2008). 'Technological due process', *Washington University Law Review*, 85(6), pp. 1249–1313.

Davidson, J. D. and Rees-Mogg, W. (1997). *The sovereign individual: Mastering the transition to the information age*. New York: Touchstone Books.

Donews. (2023). *Damoxing guojiadui laile! 360, Baidu, Huawei, Ali deng ruju [The large model national team is coming! 360, Baidu, Huawei, Alibaba and others enter the game]*. Available at: https://www.donews.com/news/detail/4/3584866.html (Accessed: 15 August 2024).

EPRS. (2020). *Digital sovereignty for Europe*. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf (Accessed: 15 August 2024).

Fan, J. and Li, T. (2023). *Quanju diwei, dayou kewei! Zongli zhaokai de zhechang zuotanhui, zaixiang pingtai qiye shifang jiji xinhao [This symposium convened by the Premier releases positive signals to platform enterprises again]*. Available at: https://www.thepaper.cn/newsDetail_forward_23827347 (Accessed: 15 August 2024).

Foucault, M. (1999). *Guixun yu chengfa: Jianyu de dansheng [Discipline and punish: The birth of the prison]*. Translated by Liu, B. and Yang, Y. Shanghai: SDX Joint Punishing Company.

Foucault, M. (2011). *Linchuang yixue de dansheng [The Birth of the clinic]*. Translated by Liu, B. Nanjing: Yilin Press.

Fukuyama, F. (2014). *Zhengzhi zhixu de qiyuan: cong qianrenlei shidai dao faguo dageming [The origins of political order: From prehuman times to the French Revolution]*. Translated by Mao, J. Guilin: Guangxi Normal University Press.

Gao, Q. (2018). *Rengong zhineng: Xunfu saiweitan [Artificial Intelligence: Taming Seviathan]*. Shanghai: Shanghai Jiao Tong University Press.

Geertz, C. (2014). *Wenhua de jieshi [The interpretation of cultures]*. Translated by Han, L. Nanjing: Yilin Press.

Geertz, C. (2018). *Nijiala: 19 shiji bali juchang guojia [Negara: the theatre state in nineteenth century Bali]*. Translated by Zhao, B. Shanghai: Shanghai Renming Chubanshe.
Harari, Y. (2023). *Rengong zhineng dui women de caozong, keneng bi ni xiangde yanzhong [Artificial intelligence manipulation of us may be worse than you think]*. Available at: https://www.thepaper.cn/newsDetail_forward_23297386 (Accessed: 15 August 2024).
He, X. and Zhang, H. (2023). *Yingzao rengong zhineng damoxing chanye shengtai [Creating an industrial ecology of artificial intelligence big models]*. Available at: http://www.news.cn/tech/20230614/f23c07c4516a41e8aa8e58b9fe695381/c.html (Accessed: 15 August 2024).
Hobbes, T. (2013). *Liweitan [Leviathan]*. Translated by Li, S. and Li, T. Beijing: Commercial Press.
Huang, Y. (2021). 'Meiguo wangluo zhili zhuizong: Tongxin guifan fa di 230 tiao de lishi, xianzhuang yu weilai [Past, present and future of Section 230]', *Journal of Cyber and Information Law*, 1, pp. 203–218.
Huntington, S. (2018). *Wenming de chongtu yu shijie zhixu de chongjian [The clash of civilisations and the remaking of world order] (revised edition)*. Translated by Zhou, Q., Liu, F., Zhang, L., Wang, Y. et al. Beijing: Xinhua Publishing House.
Institute for AI International Governance of Tsinghua University (2023). *Rengong zhineng guoji zhili guancha No. 127[Observations on international governance of artificial intelligence No. 127]*. Available at: http://aiig.tsinghua.edu.cn/info/1442/1815.htm (Accessed: 15 August 2024).
Institute of Scientific and Technical Information of China (2023). *Zhongguo rengong zhineng damoxing ditu yanjiu baogao [Report on China's artificial intelligence large model map]*. Available at: https://k.sina.com.cn/article_6380588872_17c500f4801902pmz9.html (Accessed: 15 August 2024).
Ji, W. (2000). 'Cong zhuquan de shuangchong jiegou kan zhongguo yu shijie de hudong guanxi [China's interaction with the world from the dual structure of sovereignty]', Twenty-First Century, 57, pp. 87–96.
Ji, W. (2020). 'Yiqing jiankong: Yige bijiaofa shehuixue de fenxi [Epidemic surveillance: A comparative legal sociology analysis]', *Peking University Law Journal*, 3, pp. 565–589.
Ji, W. (2021). 'Jisuan faxue de jiangyu [The frontiers of computational jurisprudence]', *Social Science Journal*, 3, pp. 113–126.
Ji, W. (2023a). *Yuanyuzhou de zhixu: Xuniren, jiami zichan yiji fazhi chuangxin [Order in the metaverse: Avatars, crypto-assets, and innovations in the rule of law]*. Shanghai: Shanghai Renmin Chubanshe.
Ji, W. (2023b). *Qiang rengong zhineng de zhili yu falv tiaozhan [Governance and legal challenges of strong artificial intelligence]*. Available at: http://www.ifengweekly.com/detil.php?id=19376 (Accessed: 15 August 2024).
Ji, W. (2023c). 'Tantao shuzi shidai falv chengxu de yiyi – jujiao fengxian fangkong xingzheng de suanfa ducai yu gongzheng [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*, 1, pp. 83–99.
Lan, J. (2020). 'Jibing, shengming zhengzhi yu xiandai zhuti de dansheng – cong Huobusi dao Fuke de zhili tixi [Epidemics, biopolitics and the birth of the modern subject – the system of governance from Hobbes to Foucault]', *Seeking Truth*, 3, pp. 1–10.
Lessig, L. (2018). *Daima 2.0: Wangluo kongjian zhong de falv [Code: And other laws of cyberspace version 2.0 (revised edition)]*. Translated by Li, X. and Shen, W. Beijing: Tsinghua University Press.
Li, B. (2010). *Lun renquan [On human rights]*. Beijing: Social Sciences Academic Press.
Li, B. (2019). 'Shenme shi renquan – genju Li Buyun jiaoshou jiangzuo luyin zhengli [What are human rights – Based on the recorded lectures of Professor Li Buyun]', *Southeast Law Review*, 1, pp. 3–7.
Lian, Y., ed. (2020). *Zhuquan qukuailian 1.0: Zhixu hulianwang yu renlei mingyun gongtongti [Sovereignty blockchain 1.0: Orderly Internet and community with a shared future for humanity]*. Hangzhou: Zhejiang University Press.
Lian, Y., ed. (2022). *Zhuquan qukuailian 2.0: Gaibian weilai shijie de xinliliang [Sovereignty blockchain 2.0: New forces changing the world of future]*. Hangzhou: Zhejiang University Press.
Lian, Y., ed. (2023). *Zhuquan qukuailian 3.0: Gongxiang zhixu xia de quanqiu zhili chongou [Sovereignty blockchain 3.0: The reconstruction of global governance under the shared order of sharing]*. Hangzhou: Zhejiang University Press.
Liu, D. (2020). 'Jishuxing zhengdang chengxu: Rengong zhineng shidai chengxufa he suanfa de shuangchong bianzou [Technological due process: The double variation of procedural law and programming algorithms in the age of AI]', Journal of Comparative Law, 5, pp. 64–79.
Liu, Y. (2022). 'Liangzhong quanliguan yu meifa geming daolu – jiyu meifa quanli xuanyan de wenben fenxi [Two perspectives on rights and the according revolutionary paths in America and France: A textual analysis of the Bill of Rights and the Declarations of Rights]', *Journal of the Renmin University of China*, 1, pp. 82–94.
Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. Minneapolis: University of Minnesota Press.
Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Buckingham and Philadelphia: Open University Press.
Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Cambridge: Polity Press.
Maitland, F. W. (2008). *Guojia, xintuo yu faren [State, trust and corporation]*. Runciman, D. and Ryan, M. (eds). Translated by Fan, A. Beijing: Peking University Press.

Makihara, N. (1998). *Kyakuubun to kokumin no aida: kindai minshu no seiji yisiki [Between "object" and nation – Political consciousness of the modern populace]*. Tokyo: Yoshikawa Kobunkan.

Ministry of Foreign Affairs of the People's Republic of China (2024). *Zhongguo guanyu quanqiu shuzi zhili youguan wenti de lichang [China's positions on global digital governance]*. Available at: https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/zclc_674645/qt_674659/202305/t20230525_11083602.shtml (Accessed: 15 August 2024).

Nakamoto, S. (no date). *Bitcoin: A peer-to-peer electronic cash system*. Available at: https://bitcoin.org/bitcoin.pdf (Accessed: 15 August 2024).

Pan, B. (2020). 'Chongsi rengong zhineng de bianzhengfa: Cong rengong zhineng dao renlei weilai [Rethinking the dialectic of artificial intelligence: From artificial intelligence to the future of humanity]', *Tianjin Social Sciences*, 3, pp. 23–29.

Shen, W. (2023). 'Jishu bifenggang de shijian ji fali fansi [The practice of technology safe harbor and jurisprudential reflection]', Peking University Law Journal, 4, pp. 906–922.

Sun, S. (2023). *Kejibu qidong guojia chaosuan hulianwang bushu gongzuo [Ministry of Science and Technology launches deployment of national supercomputing Internet]*. Available at: https://insights.zhiding.cn/2023/0420/3148891.shtml (Accessed: 15 August 2024).

Tapscott, D. and Tapscott, A. (2016). *Burokkuche-n reboryu-shon: bittokoin wo sasaerugijutsuwa donoyoni bijinesutokeizai, sosite sekai wo kaerunoka [Blockchain revolution: How the technology behind Bitcoin is changing money, business and the world]*. Translated by Takahashi, R. Tokyo: Daiyamondosha.

The Supreme People's Court of the People's Republic of China (2015). *Supreme Court joins forces with Sesame Credit Network to punish breaches of trust to see results*. Available at: https://www.court.gov.cn/zixun/xiangqing/16351.html (Accessed: 9 October 2024).

United Nations (2023). *A Global Digital Compact: An open, free and secure digital future for all (Our Common Agenda Policy Brief 5)*. Available at: https://indonesia.un.org/sites/default/files/2023-07/our-common-agenda-policy-brief-gobal-digi-compact-en.pdf (Accessed: 15 August 2024).

Wan, Y. (2021). 'Zhuzuoquanfa qiangzhixing guolv jizhi de zhongguo xuanze [China's choice of compulsory filtering mechanism in copyright law]', Studies in Law and Business, 6, pp. 184–196.

Wang, Z. (2015). 'Juedui zhuquan de luoji he liefeng – lun Huobusi de guojia xueshuo [The logic and cracks of absolute sovereignty – On the state theory of Hobbes]', *Academic Monthly*, 12, pp. 109–119.

Wood, G. (2014). *DApps: What Web 3.0 looks like*. Available at: https://gavwood.com/dappsweb3.html (Accessed: 15 August 2024).

Wu, T. (2023). *Mei zuigao fayuan kaishen da keji gongsi mingyun: Shifou quxiao 27nian hulianwang baohusan? [The U.S. Supreme Court begins a trial on the fate of Big technology companies: Does it cancel 27-year-old Internet 'protective umbrella'?]*. Available at: https://www.thepaper.cn/newsDetail_forward_22061908 (Accessed: 15 August 2024).

Xiang, Y. (2010). *Yingguo yihui zhuquan yanjiu [A study of British Parliamentary Sovereignty]*. Beijing: China Social Science Press.

Xiong, G. (2014). 'Xianzhi zhanzheng: Gelaoxiusi zhuquan lilun xinjie [Restricting war: The new explanation of Grotius's Sovereignty Theory]', *Pacific Journal*, 9, pp. 20–27.

Xu, C. (1992). 'Renquan yu zhuquan [Human rights and sovereignty]', *Journal of University of Chinese Academy of Social Sciences*, 6, pp. 40–52.

Yao, Q. (2022). 'Web 3.0: jianxingjianjin de xinyidai hulianwang [Web 3.0: The approaching new generation of the Internet]', *China Finance*, 6, pp. 14–17.

Yuan, H. (2023). *Zhuquan qukuailian chengwei quanqiu zhili chonggou de qianyan liliang [Sovereign blockchain becomes a frontier force for global governance reconstruction]*. Available at: http://www.ddcpc.cn/detail/d_guizhou/11515116165400.html (Accessed: 15 August 2024).

Zhang, H. (2013). 'You geren yizhi ziyou dao gonggong yizhi ziyou – Kangde de quanli xueshuo [From individual freedom of will to public freedom of will – Kant's Doctrine of Rights]', *Global Law Review*, 3, pp. 5–17.

Cite this article: Ji W (2024). The Transmutation of Sovereignty: Digital "World of Warcraft" and Innovation in the Chinese Legal Order. *Asian Journal of Law and Society* **11**, 418–434. https://doi.org/10.1017/als.2024.29