Davide Clementi

Between digital surveillance and individual protection: a juridical and comparative history of the Cyberspace Administration of China

(doi: 10.53227/115058)

Rivista di Digital Politics (ISSN 2785-0072)
Fascicolo 2, maggio-agosto 2024

Ente di afferenza:
()

Davide Clementi

Between digital surveillance and individual protection: a juridical and comparative history of the Cyberspace Administration of China*

BETWEEN DIGITAL SURVEILLANCE AND INDIVIDUAL PROTECTION: A JURIDICAL AND COMPARATIVE HISTORY OF THE CYBERSPACE ADMINISTRATION OF CHINA

With the advent of Internet technologies, as well as new opportunities and risks, the issue of national sovereignty within cyberspace – or cyber-sovereignty – has always been sensitive for Chinese official outlets and policymakers. Even before the promulgation of the cyberspace security law, which serves as the basic law of the Internet in China and digital infrastructures, with decree no. 33/2014, the government decided to reorganize its existing offices with Internet-related responsibilities and created the Cyberspace administration of China (Cac). The Cac functions as the highest governmental authority and the Communist party's office, given its nature as a «one institution with two names» This paper examines the history of the Cyberspace administration of China, comparing it to the Us and its role as a non-independent administrative authority. It will also explore the new powers granted to it under the cybersecurity law, the data security law, and the personal information protection law. Additionally, the Cac's role in controlling and monitoring citizens while also protecting and preserving individual rights in the context of establishing a digital socialist rule of law will be evaluated.

KEYWORDS *People's Republic of China, Cyberlaw, Cyberspace Administration of China, Individual Protection, Digital Surveillance.*

1. Introduction

For a long time, the Internet has been considered «intrinsic to globalization, or rather to the Us empire, it is its virtual side, its parallel dimension»

* Unless otherwise indicated, all translations from Chinese to English have been rendered by the author.

Davide Clementi, University of Macerata – Piaggia dell'Università 2, 62100 Macerata, Italy, email: d.clementi1@unimc.it orcid: 0000-0002-5734-8580.

ISSN 2785-0072

(Fabbri 2018, 9)[1]. Today's reality illustrates a markedly different economic, cultural, social, and digital reality, where globalization – the process of shrinking distances and times worldwide (Larsson 2001, 9; Birch and Wellen 2023, 203) – alongside the development and implementation of Information and communication technologies (Ict), has made it possible to shop for products on Alibaba or Shein, stream videos on Tiktok, all seamlessly connected through networks powered by Huawei's cutting-edge technologies and infrastructure. In essence, China's rapid economic development and entry into the global market, once encouraged by the United States (Us) in the hope that liberal-democratic systems and the rule of law would bloom in the People's Republic of China (Prc) alongside the exchange of goods, services, and capital, now matures into a fierce challenge to Us economic, military, but also legal and digital primacy (Milutinović and Nikolić 2023). Thus, China and the Us maintain a substantial duopoly in cyberspace control through their respective digital champions (Mueller and Farhat 2022, 350) and through the progressive adoption of a legal framework (Kettemann 2020) that reaffirms the centrality of public interests and state control over the digital sphere.

Given the enduring assumption that China constitutes a legal system that knows «neither god nor law» (Granet 1934; Bourgon 2021, 1), the cyber-normativity of the Prc was often disregarded, while it can provide further impetus to understand the overall functioning of the socialist rule of law with Chinese characteristics (*Zhongguo tese shehui zhuyi fazhi* 中国特色社会主义法治). This system is already contesting the Washington-led international and normative order through norms and institutions spreading from China to other legal systems and disseminating globally, prompting discussions about a «Beijing effect» (Kastner and Saunders 2012; Erie and Streinz 2021, 163-177; Ikenberry 2024, 129-130).

Through the lenses of comparative legal method, this article will help clarify the digital regulations in force in China by an in-depth examination of the regulatory framework governing the Internet in China. The comparative legal method involves both horizontal comparison between Chinese cyber laws with those of the Us and by analyzing how each system addresses digital surveillance and individual rights, and a vertical comparison, by assessing how these laws are implemented and enforced at different levels.

The study utilizes both primary and secondary sources. Primary sources include official documents, legislative texts, government reports, and speeches by key figures (such as President Xi Jinping), due to their leading role in con-

[1] See, among others, Stockwell (1990), Tucker and Hendrickson (1992), Omae (1995), Falk (1995), Rupert (2000), McWhinney (2000).

structing the guiding thoughts and ideologies of the party-State. Secondary sources include academic articles, institutional reports from international organizations, and media sources.

Central to better understanding China's current approach to the regulation of the cyberspace is identifying the functions and powers of the Cyberspace administration of China (Cac) and closely analyzing the interactions between this unique supervisory and regulatory body and the rights of natural and legal persons. This analysis evaluates the dual functions of the Cac: firstly, by directly controlling, monitoring, and censoring natural and legal persons, and secondly, by indirectly protecting individuals, especially in their consumer behaviors.

The analysis is structured around several key themes. It begins with an exploration of the early development of the Internet, tracing its roots back to Paul Baran's proposals in the 1960s and the establishment of Arpanet by Darpa, highlighting the influence of cold war dynamics on its evolution. The narrative transitions into the commercial and public adoption of the Internet in the Nineties, marked by significant events such as the decommissioning of Arpanet and the rise of web browsers like Netscape.

The article then delves into the regulatory challenges posed by the Internet's expansion, focusing on the United States' approach to Internet governance. It discusses the dichotomy between private economic interests and public authorities, emphasizing the minimal regulatory stance enshrined in the telecommunications act of 1996 and the role of federal agencies like the Fcc and Cisa in cybersecurity.

In contrast, the article examines China's initial regulatory response to the Internet, emphasizing the government's early recognition of its potential for both economic growth and ideological challenges. It outlines the development of China's regulatory framework, starting with decree no. 195 of 1996 and leading to the comprehensive cybersecurity law of 2017. The role of the Cyberspace administration of China in enforcing these regulations and ensuring compliance with national security and ideological goals is highlighted. Case studies, such as the Cac's handling of prominent tech companies (e.g., Didi), illustrate the practical enforcement of rules, providing a tangible insight into cyber laws and the interplay between state interests and corporate behavior.

Finally, the concluding remarks will try to take stock of similarities and differences between China and Us, assessing a global convergence between Beijing's regulatory model and the approaches of Western liberal nations, signaling a move towards legal interventionism in cyberspace and a more complex balance between state control and protection of individuals' rights.

2. The Us Internet (un)regulation between federal government and private enforcers

The birth year of the Internet could theoretically be backdated to 1962 when Paul Baran, a Polish-American engineer deeply involved in pioneering computer network development, proposed that government institutions «start thinking about a new and possibly nonexistent public utility, a common user digital data communication plant explicitly designed for the transmission of digital data among a large set of subscribers» (Baran 1962, 42).

During the cold war, the rivalry between the United States and the Soviet Union was fueled by political and economic aspirations and a challenging technological race. The Ussr achieved a historic feat on October 4, 1957, by successfully launching the first artificial earth satellite, Sputnik 1. The Ussr achieved a landmark on October 4, 1957, when it successfully launched the first artificial earth satellite, sputnik 1. Time magazine's response was fear and panic, grimly referring to it as a «red moon over the Us». Concerned about the potential collapse of traditional communication networks in the event of a Soviet atomic attack, Baran proposed the creation of a distributed network of communication stations instead of centralized switching structures. This concept received funding from another Us federal agency, the Defense advanced research projects agency (Darpa). As early as 1969, Darpa connected multiple computers for the first time through Advanced research projects agency network (Arpanet), the first wide-area packet-switching network. In 1974, Darpa partnered with the Uk royal mail to develop the first transatlantic network communication program, Satnet (Ryan 2010, 36). This partnership with Royal Mail arose because At&t, the only telecommunications company in the United States at the time, had declined to participate (Mazzucato 2015, 111). From the 1970s through the 1990s, the funding and development of what we now know as the Internet were entirely under the account of the Defense communications agency (Dca), a division of the Us Department of defense (Ryan 2010, 99).

In 1990, Arpanet was decommissioned, which marked the end of the military era of the Internet. The growth of the Internet continued, reaching over two million users by 1993. By this time, all major operating systems had browsers capable of accessing the world wide web, which was developed by Tim Berners-Lee at Cern using Html.

Two years later, on August 9, 1995, Netscape communications Inc., a web browser company, saw the value of its shares double on its first day of public trading (Shinal, 2005), marking the beginning of the dot-com era.

As with any innovative social phenomenon, the Internet has presented significant challenges in terms of how people engage in their public lives, negotiate contracts, establish businesses, commit crimes, and pursue legal matters. Many argue that during its uncontrolled and disorderly expansion, as the Internet emerged as a social, economic, and legal phenomenon in its early stages, both Internet users and even states chose not to regulate it, leaving it without a *nomos*[2]. However, even during those early years, the essential tension that would fuel debates and actions regarding the Internet as a space for legally relevant activities had already been identified: the collision between private economic interests, often referred to as «the market», and public authorities, known as «the government» (Litant 2011, 1045-1085)[3].

The conceptualization of the Internet has long been accompanied, almost as a corollary, by the notion of borderlessness. While this idea was – and in some cases still is – reinforced by the presence of hackers and pirates who navigate the web and engage in various forms of wrongdoing to the detriment of individuals, private economic actors, and public powers, the latter have set themselves against an unspecified «rise of global "a-centric" and "self-regulatory" structures» (Von Bernstorff 2003, 512) of the Internet, which some of its late adopters have declared to be independent (Barlow 1996).

Besides addressing issues primarily related to the attribution of Internet domain names, numbers, or technical standards (Werle and Iversen 2006)[4], national governments worldwide have been enacting a series of regulations with various goals in mind. These objectives include enhancing or restricting freedom on the Internet, promoting commerce and industry, digitizing public administrations, upholding their legal frameworks, and pursuing cybercriminals. In a nutshell, national public powers, faced with the new challenges of regulating an *a-nomic* space they saw as their own, have extended their sovereignty to the Internet, encompassing it within their legal jurisdictions.

[2] We are referring herein to Schmitt (1950). Published in the aftermath of the second world war, Schmitt notoriously discussed the theoretical conception of the «world order», since a «new» one was in the making in these times. According to Schmitt, the new world order is a juridical phenomenon, albeit with political overtones.

[3] The author talks about four main issues which would be dealt with on the Internet: privacy, intellectual property protection, taxation, and open access to high-speed or broadband networks. Litant doubts that these issues would be resolved either by market forces or by government alone, nevertheless suggesting that «policymakers» first instinct should be to rely on markets and technology to address some troublesome issues and to act only if there are identifiable market failures that can be corrected usefully by some type of government intervention'.

[4] It is assessed that pure technicality creates conscious or unconscious interests, preferences, and moral judgements in private or public operators, as in the case of Ipv6. From the European point of view, see also Meyer (2012).

Even the Us, a country that has witnessed the swiftest adoption of the world wide web among its population and has allowed for extensive self-regulation by private economic actors, has seen government interventionism in its cybersphere, beginning with defining what cyberspace is. During its «defense period», Us government agencies entirely developed, programmed and maintained the Internet. These agencies were either directly managed or funded by the Department of defense. Today, Us cyberspace has undergone a transformation due to privatization, being transformed into a group of privately owned and regulated spaces (Segura-Serrano 2006, 26).

As a common law country, the courts were the first to define the Internet and cyberspace while deciding cases. In *Reno v. American civil liberties union*, the Supreme court of the United States described the Internet as «an international network of interconnected computers [...] [which] now enable[s] tens of millions of people to communicate with one another and to access vast amounts of information from around the world» (Supreme court of the United States of America 1997)[5]. In the same judgment, the Court defines cyberspace as «located in no particular geographical location but [is] available to anyone, anywhere in the world, with access to the Internet [...]. Cyberspace undeniably reflects some form of geography; chat rooms and web sites, for example, exist at fixed *locations* on the Internet. Since users can transmit and receive messages on the Internet without revealing anything about their identities or ages [...], cyberspace is malleable. Thus, it is possible to construct barriers in cyberspace and use them to screen for identity, making cyberspace more like the physical world and, consequently, more amenable to zoning laws» (Supreme court of the United States of America 1997).

In 1996, the Us Congress approved the telecommunications act of 1996, which president Bill Clinton signed into law on February 8, 1996. The purpose of the act was «to promote the competition and reduce regulation to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies» (United States 1996). The telecommunications act of 1996 was described as «the watershed event that marked the end of the telephone age and the beginning of the internet age in the public policy realm» (Ehrilich 2014, 5).

The regulatory aspects, as was aptly and laconically well summarized as early as the end of the last millennium (albeit with a touch of provocation toward the American leadership of that era), have always revolved around «sex, lies, and taxes» (Morrison 1998). Except for a series of laws aimed at curbing

[5] Cyberspace is described as a «vast democratic forum of the internet».

hateful criminal behaviors that harm vulnerable individuals or distort market competition, Us Internet legislation, rooted in the first amendment of the Us constitution and its principle of freedom, has not embraced comprehensive regulation that imposes specific obligations to protect and safeguard individual interests in the context of cyberspace (Palfrey 2008, 241).

Due to their dominance in the ownership of critical infrastructure (Sales 2003), private firms often obstruct the formulation of comprehensive cyber laws and corresponding federal regulatory bodies for their enforcement. Presently, only two federal agencies exist for cybersecurity-related purposes: the Federal communications commission (Fcc) and the Cybersecurity and infrastructure security agency (Cisa). The Fcc has a long history of making «available so far as possible to all the people of the United States, without discrimination based on race, color, religion, national origin, or sex, rapid, efficient, nationwide, and worldwide wire, and radio communication services with adequate facilities at reasonable charges» (United States 1996), with the additional «purpose of the national defense». The latter was recently established during the Trump administration to address cybersecurity threats and aims to «protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents» (United States 2018).

Instead of promoting the creation of agencies with specific powers for safeguarding, the Us approach to cyber law focuses on two distinct actions: firstly, preventing the involvement of «nation-state actors who are foreign adversaries to the United States» (Chen 2022, 181)[6], and secondly, allowing large private oligopolistic companies to exercise their own legal enforcement power over people's daily lives through online moderation and adjudication (Tosza 2021)[7]. The ultimate goal of this unregulated approach is to foster and boost industrial innovation (Ohlhausen 2012; Yoo 2010, 79), secure market share and revenues for private companies while allowing individual liberties to flourish without excessive government control (Supreme court of the United States of America 2017; Harvard Law Review 2023)[8].

[6] Chen (2022, 181) signals «two pairs of dilemma» that the Us government is faced with «on the one hand, it is emphasizing the importance of privacy and data security against foreign adversaries; on the other hand, its respect for Us users' privacy and data security are lacking at best, and legislative efforts by the Federal government to protect user privacy are nowhere near to be complete».

[7] The author concludes that «their tasks are currently moving from compliance towards more proactive enforcement and they are also playing an adjudicative role, making them similar to public actors».

[8] According to the Harvard Law Review (2023), the Supreme court «characterized social media as a contemporary version of the quintessential public forum for exchanging views, such as "a street or a park"».

3. A window not so open: China's initial regulatory dilemma on the Internet

During the reform and opening up era (*gaige kaifeng* 改革开放) China's paramount leader, Deng Xiaoping, eloquently remarked that «if you open the window to fresh air, you have to expect that some flies will blow in» (d*akai chuanghu, xinxian kongqi he cangying jiu hui yiqi jinlai* 打开窗户, 新鲜空气和苍蝇就会一起进来). Early on, some Chinese scholars observed that the Internet would be an «uncontrollable medium» (*buke kongzhi meijie* 不可控制媒介) (Cai 2002, 91) for the Cpc, fearing that, as Deng metaphorically envisioned, through the window of the Internet, not only economic advantages would come in, but also some flies of democratic institutions. Due to the inherent fluidity of Internet technology, Western observers had hoped that «greater access to information brought about by this new technology would also encourage political expression and democracy in China» (Lum 2006, 2).

China, too, has been tempted by the notion that cyberspace constitutes a distinct realm from real society (*xianhai shehui* 现实社会), where traditional legal norms could not be digitally enforced, as the cyberspace was perceived free from the constraints and obligations of conventional law. It is noteworthy that the *Declaration of independence of cyberspace* has also found resonance within Chinese theoretical and legal discourse (Gao 2004, 509-511).

In this phase, political discourse and academic reasoning diverged: on the one hand, Chinese highest officials have always foreseen the Internet as a key component of the national economic growth strategy and a challenge to their authority and legitimacy. Chinese president Jiang Zemin noted, as early as January 2000, that the Cpc «need[s] to strengthen» its «supervision over the fields of publicity, ideology, and culture, including supervision of newspapers and periodicals, especially minor publications, books, television and film, the Internet, and other media», also to curb the spread of «gossip and political rumors [...] in minor newspapers and periodicals as well as on the Internet» (Jiang 2012, 559).

On the other, scholars have been variously inveigled by the needlessness of a sound and coherent regulation of the Internet, advocating instead for governance by companies rather than state regulators (Dong 2007). Despite being acutely aware of the proliferation of illegal activities (*weifa xingwei* 违法行为), they acknowledge that completely eradicating such activities in cyberspace remains an impractical endeavor (Wang 2007, 8).

Nevertheless, consistent with its historical policies and practices of controlling and censoring traditional communications and telecommunications and due to its unique economic, political, and social structures, the Chinese

government has applied its experience in managing traditional communications and telecommunications to the digital world.

Even before president Jiang delivered the abovementioned speech, the Chinese central government issued decree no. 195 of 1996 to «strengthen the control over computer information networks connecting to the international network, safeguard the healthy development of international computer information exchange» (State council 1996). According to this first Internet regulation, the Chinese State «carries out the principles of overall planning, unified standards, managing by different levels and promoting the development of the international connection» (State council 1996, art. 4).

The State acted through the Economic information leading group (*Guojia xinxihua lingdao xiaozu* 国家信息化领导小组) (State council 1996, art. 5), which included members from major economic, educational, and technological offices, as well as representatives from the Cpc's Central propaganda department, State council information office, Ministry of public security, State secrecy bureau, and the People's liberation army (Qiu 2003, 11). This group was eventually disbanded following the restructuring of leading ministries (State council 2008). Simultaneously, decree no. 195 of 1996 was issued by the State council, addressing «law-breaking or criminal activities that may endanger national security or divulge State secrets; or producing, consulting, duplicating or propagating information that may disturb social order or pornographic information» (State council 1996, art. 13).

These initial measures marked the beginning of the construction of China's new digital great wall, a part of the broader Golden shield project (*jindun gongcheng* 金盾工程). The entire project, which would later become known, especially in Western media, as the Great firewall of China (*Fanghuo Changcheng* 防火长城), was implemented in various phases. Starting with decree no. 195/1996, the initial Chinese Internet regulation required Internet service providers (Isps) «to verify every user's Id information [...] to be able to keep track of every user's online activities» (Chandel *et al.* 2019, 112).

One year later, the State council established the informatization office, headed by the Premier himself, with responsibilities such as generating policy proposals, coordinating strategies, implementing drafted laws and regulations, setting standards, and developing plans (Hanna and Zhen-Wei Qiang, 2010).

In 2000, the State council adopted decree no. 292 «in order to regulate Internet information services activity and to promote the healthy and orderly development of Internet information services» (State council 2000). These new rules introduced significant restrictions and prohibitions. Internet information service activities related to news, publishing, education, healthcare,

pharmaceuticals, medical equipment, and more must be examined and approved by relevant supervisory departments (State council 2000, art. 5).

State authorities were granted the power to request and store electronic records from Internet information service providers (Iisps), including user online times, account numbers, Internet addresses, domain names, and primary phone numbers (State council 2000, art. 14). Art. 15 expanded the list of prohibitions, requiring Iisps not to produce, reproduce, distribute, or disseminate content that violated constitutional principles, endangered national security, disclosed state secrets, subverted state sovereignty, jeopardized national unity, damaged the reputation and interests of the state, disrupted religious activities, or disturbed social order and stability. Iisps had to «immediately discontinue transmitting such information, keep relevant records, and make a report to relevant State authorities» (State council 2000, art. 16). If any activity specified in art. 15 also constituted a crime, criminal responsibility would be prosecuted in accordance with the law (State council 2000, art. 20).

Later that year, Us president Clinton mocked the Chinese attitude toward Internet regulation as a rickety and mocked attempt to «nail a Jell-O to the wall» in the face of liberty, which would have been «spread by cell phone and cable modem» (C-Span 2000, video-format). In the meanwhile, the fifth plenary session of the 15th central committee of the communist party of China established a strategy of «promoting industrialization through informatization» (Hanna and Zhen-Wei Qiang 2010, 130).

4. Nailing the Jell-O to the wall: the cybersecurity law as the basic law for China's digital realm

In the realm of cyberspace, China tends to consider law (*fa* 法), particularly cyberlaw (*Wangluo Fa* 网络法) above all, as «an important ammunition in the arsenal of governments to deal with cyberspace legal and policy issues» (Duggal 2020, 185; Xu 2016, 338). This legal instrumentalism was echoed by the Chinese academy of cyberspace studies, which asserted that «the internet has been developing [in China] on the principle of cyber governance with the rule by law (*fazhi* 法治) (Moccia 2009; Castellucci 2012), following the trend of digital economy development and the combination of security and development» (Chinese academy of cyberspace studies 2020, 103). This approach is not without controversy, as scholars and activists in China and worldwide highlight that legal norms displayed in the construction of the China's digital rule by law have never stated that Chinese citizens have a right to access to the Internet (Svensson 2019), but just another space to rule. Thus, the cyberspace,

rather than «an exotic land» (*yiyu* 异域) different from reality due to its interconnectivity and virtual nature, represents mere electronic facilities beneath the world of bits that exist in the physical world and within the territories of specific sovereign states. As stated by Zhang and Xu, «cyberspace is not an extralegal enclave» (*fawai feidi* 法外飞地), but «all possible evil (*e* 恶) of the real world are reflected in a distorted manner within it and even expand due to the characteristics of anonymity and cross-regionality. Hence, the key issues are not whether sovereign states can appear in cyberspace, but in what manner they exercise their power» (Zhang and Xu 2016).

Consequently, the notion of cyberspace as an ungoverned domain was refuted, and the debate centered on the modalities through which state power and legal frameworks are applied in this realm. This perspective inherently challenges the assertion of cyberspace as a distinct and separate entity from traditional state control, underscoring the importance of sovereign authority in regulating and securing digital spaces and developing into the notion of cyber-sovereignty (*wangluo zhuquan* 网络主权). This concept first emerged in the People's daily, Cpc's official house organ, where it was referred as a «natural extension of national sovereignty in the cyber environment» but also «inevitable issues for the very assertion of national sovereignty in the Internet age» (Wang and Xin 2014)[9]. This perspective has subsequently been appreciated by Chinese doctrine, avoiding the differences and contradictions between virtual space and real territory, and explicitly contesting the «Western assertions» that denied state sovereignty over cyberspace (Ruo 2014; Zhi 2016, 5).

To «safeguard cyberspace sovereignty and national security, and social and public interests», and «promote the healthy development of the informatization of the economy and society», the Standing committee of the national people's congress enacted the Cybersecurity law, Csl (*Wangluo anquan fa* 网络安全法), which came into force on 1 June 2017 (Standing committee of the national people's congress 2016, art. 1).

[9] It is worth noting the publication on the official website of the Cyberspace administration of China of a paper entitled «Cyber-sovereignty: Theory and Practice (version 2.0)», written in collaboration with many institutions (among others, Wuhan University, the China Institute of modern international relations and the Shanghai Academy of social sciences) in which, in addition to reiterating the above definition of cyber-sovereignty, its characteristics, and principles are outlined: central to the present analysis is the jurisdiction of the sovereign state in the digital space, which also includes «network data and information within its borders in accordance with the law», toward which states have «duties of prudence and prevention» in order to prevent third countries from endangering national security and interests. See Wuhan University *et al*. (2020); Tai and Zhu (2022).

The Csl operates as the basic law governing the Internet in China[10]. It is applied to all individuals and entities in China, irrespective of their ownership or nationality, and without exceptions related to industrial activities (Csl, art. 12, para. 2). This implies that not only the It industry but also all types of business and individuals, both within and outside the Internet, are subject to the Csl.

According to the definition, network operators (*Wangluo yunying zhe* 网络运营) encompass «network owners, managers, and network service providers» (Csl, art. 76). Given the assumption that many businesses opt to establish their in-house Virtual private networks (Vpns), most enterprises fall into this category. According to notice no. 32/2017 issued by the Ministry of industry and information technology to all Internet operators in mainland China, the creation of unapproved dedicated lines or other information channels for cross-border activities and the provision of Vpns to users without official permission are prohibited (Ministry of industry and information technology 2017)[11].

Enterprises can also be categorized as Critical information infrastructure operators (Ciios), subject to additional security measures and protection obligations (Csl, artt. 31-39). The law places emphasis on protecting critical information infrastructure in «public communications and information services, energy, finance, transportation, water conservation, public services, and e-governance, as well as other critical information infrastructure that could cause serious damage to national security» (Csl, art. 31).

The State disciplines Internet activities that jeopardize national security, unity interests, stability, core socialist values (Csl, art. 12, para. 2), and the well-being of minors (Csl, art. 13). Interestingly, everyone has the right to report such activities, and State departments are required to «promptly process them in accordance with law» or transfer them to an empowered department when they are not competent (Csl, art. 14).

The Csl places significant emphasis on the protection of personal information. It defines personal information (*geren xinxi* 个人信息) as «all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity». This includes, but is not limited to, «full names, birth dates,

[10] Similarly, on the topic, we find China Netcom, 6/2022, General secretary Xi Jinping's guide to my country's Cybersecurity work documentary, where the Csl was defined as the «first basic, framework and comprehensive law in the field of cybersecurity».

[11] In May 2019, a company faced fines for using an illegal «proxy» to access overseas websites, violating Miit decree 32/2017 Li 2021, 67-87.

national identification numbers, personal biometric information, addresses, telephone numbers, and more» (Csl, art. 76(5)).

Under the Csl, individuals have the right to request that network operators correct or delete their personal information (Csl, art. 43). Network operators are obligated not to misuse, disclose, tamper with, or destroy the personal information they collect (Csl, art. 42). They must also publish rules for collecting and using personal data, clearly stating the purposes, methods, and scope of data collection or usage. Furthermore, they must obtain consent from the individuals whose data they collect (Csl, art. 41; Zhang 2019).

The fourth and final chapter of the Chinese cybersecurity law outlines the penalties for breaches of cybersecurity protection duties. Network operators who do not comply with corrections or warnings from authorities may face fines ranging from Rmb 10,000 to 100,000, while directly responsible managers may be fined between Rmb 5000 and 50,000. For Ciios, fines can go up to Rmb 1,000,000. Individuals who violate article 27 by harming cybersecurity or providing tools for such activities risk confiscation of illegal gains, up to 15 days of detention, and fines between Rmb 50,000 and 1,000,000. Operators who improperly collect user information without transparency can be fined up to Rmb 1,000,000, and directly responsible personnel may face fines between Rmb 10,000 and 100,000, along with potential operational suspensions or license revocations in serious cases.

5. The Cyberspace administration of China

In the previous paragraphs, we summarized what has been defined by Chinese president Xi Jinping as the «leadership for the management of the Internet» (Xi 2014), which, at the time, was regarded as «seriously flawed» according to China's paramount leader. Xi denounced the presence of multiple administrative bodies with overlapping functions and the consequent mismanagement of powers and responsibilities, which inevitably led to the «insufficient management» of the Internet. To tackle this issue, Xi urged Cpc officials and legislators to «adhere to the principles of proactive usage, well-planned development, management under the law and ensuring safety in strengthening management of the Internet in accordance with the law and accelerating the improvement of the leadership for the management of the internet» (Xi 2014).

Due to new technologies like cloud computing, wearable gadgets, and microblogging services, the Central people's government decided to reorganize its existing offices responsible for Internet-related matters. It created the

Cyberspace administration of China (*Guojia Hulianwang Xinxi Bangongshi* 国家互联网信息办公室, Cac) and the party-doublet Central leading group for cyberspace affairs (State council 2014; Miao and Lei 2016), which was transformed in March 2018 as the Central cyberspace affairs commission (Ccac) (Liang 2018). The head of this «one institution with two names» (*yige jigou liang kuai paizi* 一个机构两块牌子) is Zhuang Rongwen, who also served as the head of the Department for propaganda of the Central committee of the Cpc. Prior to Zhuang, former Vice-Mayor of Beijing Lu Wei served as the first director of the Cac. His role was highly controversial: while initially close to president Xi Jinping and placed in a top position as «China's Internet czar» or «the man who nailed Jello to the wall» (Allen-Ebrahimian 2016), he was later placed under investigation for corruption in November 2017, expelled from the Communist party in February 2018 for «arbitrary and tyrannical abuses of power» by Cpc's Central commission for discipline inspection, and sentenced to 14 years in prison by Ningbo intermediate people's court (Gao 2019).

On its official website, launched in December 2014 (English.gov.com 2014), Cac affirms that its main responsibilities include the «implementation of Internet information guidelines and policies, the establishment of a legal system for Internet information dissemination, guiding, coordinating, and urging relevant departments to strengthen Internet information content management, and being responsible for the examination and approval and daily supervision of Internet news services and other related businesses».

Moreover, Cac is also responsible for the planning and construction of key news websites, organizing and coordinating online publicity work, investigating and punishing illegal websites in accordance with the law, and guiding relevant departments to supervise and urge telecom operators, access service companies, domain name registration management and service organizations, etc. to do a good job in basic Internet management such as domain name registration, Internet address (Ip address) allocation, website registration and filing, and access.

These responsibilities, which mainly reflect the Cpc's desire to strengthen its control over the world's largest online population (Gan, 2018), culminated in the approval of the regulations on the ecological governance of network information content (Cac measures no. 5/2019), which came into effect on March 1, 2020 (Cac 2019). These rules must be interpreted in accordance with the national security law, the Csl, the Internet information service management measures, and any other applicable laws and administrative regulations (Cac 2019, art. 1).

According to art. 3 of Cac measures no. 5/2019, the Cac is responsible for the «overall coordination of the national cyber information content ecological governance and related supervision and management», in coordination with local cybersecurity and informatization departments and bureaus.

All individuals and entities, including government agencies, organizations, businesses, and netizens, are required to adhere to the principles of ecological governance on the Internet. This is done to cultivate and practice «socialist core values as the foundation [...] and establish and improve a comprehensive network governance system» (Cac, 2019, art. 2).

Network information content producers[12] shall «propagate Xi Jinping's thought [...] and fully, accurately, and vividly interpret the path, theory, system, and culture of Socialism with Chinese characteristics» (Cac 2019, art. 5(1)). They must also refrain from producing, copying, or publishing content that «opposes the basic principles established by the constitution» (Cac, 2019, art. 6(1)), or content that endangers national security, leaks state secrets, subverts state power, or undermines national unity.

Chapter III (artt. 8-17) imposes stricter rules on network information content service platforms[13] (Cac 2019, art. 11) with the aim of «strengthening page ecological management» (*jianqiang banmian yemian shengtai guanli* 加强版面页面生态管理) (Cac 2019, art. 11). These platforms are required to display on their homepages, blogs, microblogs, mobile application stores, and pop-up windows that adhere to the principles and values outlined in article 5. They must also take immediate legal measures, maintain relevant records, and report such content to the competent authority under artt. 6-7 (Cac 2019, art. 10). The provisions of the great firewall have been upgraded to not only detect words or phrases that could endanger national security and «social harmony» on the Internet (Hounsel *et al.* 2020) but also to identify technologies capable of circumventing the great firewall, such as Vpns.

If a network content producer or platform violates the provisions of artt. 6 or 10, relevant authorities shall take subsequent legal measures, including warning, rectification, restricting functions, suspending updates, or closing accounts (Cac 2019, artt. 34-35).

Cac Measures no. 5/2019 was followed by another set of «Provisions on the administration of Internet posting and commenting services» (Cac provisions 16 Nov 2022c). This batch of rules grants Cac the responsibility for supervising, managing, and enforcing laws regarding comment services in Chi-

[12] Article 41 defines network information content producers as «organizations or individuals that produce, copy, and publish network information content».

[13] Article 41 defines network information content platforms as «network information service providers that provide network information content dissemination services».

na (Cac 2022a, art. 3). These services encompass «Internet sites, applications, and other website platforms with public opinion attributes or social mobilization capabilities, which provide users with the means of posting texts, symbols, emojis, pictures, audio, videos, and other information services» (Cac 2022a, art. 1). Cac provisions 16 Nov 2022 posed additional burdens on Isps, first of all to authenticate users registered on their platforms based on the collection of «real identity information» such as «mobile phone number, Id card numbers or unified social credit codes (*tongyi shehui xinyong daima* 统一社会信用代码) » (Cac 2022a, art. 4(1)). While stating that Isps shall put in place a system for users' personal information protection, following principles of legality, legitimacy, necessity, and good faith as stated by both the Civil code and the Pipl (Cac 2022a, art. 4(2)), Isps are under the obligations to innovate, develop and improve «the ability to deal with illegal and bad information», establishing a «post review management» system, «real-time inspections, emergency response, and report acceptance» (Cac 2022a, art. 4(5)), and equipping a «review and editing team» in each service providers (Cac 2022a, art. 4(7)). Before entry into service, Isps shall pass security assessments following relevant laws and regulations (Cac 2022a, art. 5). Even users shall post comments that follow «laws and regulations, public order, and good customs» and «promote core socialist values» (Cac 2022a, art. 9).

Cac is also playing a leading role in advancing amendments to the aforementioned legislation. For example, on September 14, 2022, the Cac proposed amendments to the Csl for public comment. These amendments aim to enhance the legal liability system, protect the rights and interests of individuals and organizations in cyberspace, and safeguard national security and public interests (Cac 2022b).

The proposed amendments recalibrate fines for violations of the Csl. For general violations by network operators and Ciios under articles 59 to 62, companies failing to correct violations or those with serious infractions could face fines from Rmb 100,000 to Rmb 1 million. Severe violations could incur fines between Rmb 1 million and Rmb 5 million or 5 percent of the previous year's turnover, with responsible individuals fined between Rmb 100,000 and Rmb 1 million.

Article 70 addresses violations of obligations under article 12, imposing fines up to Rmb 1 million for undermining China's sovereignty and security, such as inciting subversion or terrorism. Responsible persons could be fined between Rmb 10,000 and Rmb 100,000. For serious violations, fines could range from Rmb 1 million to Rmb 50 million, or up to 5 percent of the previous year's turnover, with individuals fined between Rmb 100,000 and Rmb

1 million. These amendments emphasize China's stringent approach to cybersecurity and digital control.

6. Another two bricks in the great firewall: the promulgation of Pipl and Dsl

In 2021, the Chinese legislator adopted and enacted two additional laws that, combined with the Csl, form a triptych of laws. These laws, while securing the position of individuals against unlawful behaviors such as data breaches and personal information infringements, reinforce the authority of the Cac in the cybersphere.

As a «late entrant in the field of personal information protection and privacy laws» (Cui and Qi 2021), China has drawn inspiration from other legal systems, particularly the European Union (Eu), in safeguarding personal information. The Eu's intricate and multifaceted regulatory framework has served as a model for China in developing its own governance approach, tailored with distinct «Chinese characteristics» (European parliamentary research service 2022).

It can be observed that the combination of both Prc civil code (Prc 2020)[14] and the Personal information protection law (Prc 2021a, Pipl) has shifted China from the later-enforced monistic (or Us) system of privacy-personal information protection, to the dualistic/Eu system of protection of the private realm of individuals (Guo *et al.* 2024, 1-15). In the dualistic system, the right to privacy is considered a negative (*xiaoji* 消极) or a defensive (*fangyuxing* 防御性) right, where individuals can only exercise it in response to the event of infringement of their spirituality. On the other hand, the right to personal information protection is rather portrayed as a dynamic and active right, enabling individuals to proactively control their information, which may include elements of proprietary value (Wang 2013).

Under the civil code and Pipl, there is no denying the empowerment of citizens in asserting control over both their privacy and personal information in response to intrusions by individuals and, especially, large platforms. However, the Pil and its public-focused counterpart, the data security law (Prc

[14] Art. 111: «the personal information of a natural person shall be protected by law. Any organization or individual that needs to acquire the personal information of an individual shall obtain such information in accordance with law and guarantee the safety of such information. Any illegal collection, usage, processing, and transfer of the individual's personal information, or illegal trade, making available or disclosure of other's personal information is the violation of law».

2021b, Dsl), have introduced new tools that strengthen the authority of governmental agencies, with the Cac taking the lead.

Indeed, Pipl and Dsl delineate the often-conflated notions of personal information (*geren xinxi* 个人信息) and data (*shuju* 数据) by focusing on their functions, particularly in relation to the degree of state interest involved. When the interest at stake pertains to state security, including the protection of the «legitimate rights and interests of citizens and organizations» (Dsl, art. 21), state intervention under the Dsl and through the Cac is warrented. Conversely, when the issue pertains to the legitimate rights and interests of individuals, data appears to be reclassified as mere personal information, thereby falling within the scope of the Pipl. In this context, the Pipl governs the processing of personal information with an emphasis on safeguarding individual privacy and rights, rather than broader state interests. As a result, state intervention is less pronounced compared to the Dsl, focusing instead on protecting individuals from potential misuses of their personal data by private entities.

This legal foundation ultimately paved the way, beginning in October 2020, for what was referred to as China's «Red new deal» (Kuo *et al.* 2021)[15] or «the great rectification» (Creemers 2023): the Cyberspace administration of China has taken a leading role in tightly regulating, monitoring, and penalizing the private sector, particularly high-value-added technology industries. A prominent target of these measures was Didi global Co., Ltd. Outrageously, on July 21, 2022, the Cac announced sanctions against Didi for committing a total of sixteen illegal actions that occurred even before the implementation of Csl, Pipl, and Dsl, raising concerns about the principle of non-retroactivity of sanctions (Cac 2022c)[16].

Furthermore, on February 24, 2023, the Cac released its «Measures on the standard contract for outbound cross-border transfer of personal information» (Cac 2023). These measures were introduced in compliance with the personal information protection law and represent an additional step toward

[15] With this expression we want to underline the government's effort to «reduce inequality and make the lives of normal people better» through «actions that have an old-fashioned communist logic, but also because companies that hinder the government will lose blood».

[16] See also the official Q&A on the decision, where it was clearly stated that «in order to prevent national data security risks, safeguard national security, and protect the public interest, in accordance with the national security law and the cybersecurity law, the cybersecurity review office conducted a network security review of Didi in accordance with the cyber security review measures. [...] from the perspective of the duration of the illegal acts, Didi's related illegal acts began as early as June 2015 and have lasted for up to 7 years, continuously violating the cybersecurity law implemented in June 2017, the data security law implemented in September 2021, and the personal information protection law implemented in November 2021».

restricting data flow to the global community. They impose additional requirements on foreign personal information handlers, making it necessary for them to meet these requirements to lawfully establish standard contracts for the export of personal information to overseas recipients (Cac 2023, art. 2).

This development was a catalyst for further limitations on the well-known academic database China national knowledge infrastructure (Cnki), which restricted access to foreign researchers starting from April 1, 2023 (Park 2023). This action followed a penalty imposed by China's top anti-monopoly authority, the State administration of market regulation (Samr), on December 5, 2021. Cnki was accused of engaging in anticompetitive business practices and faced a fine of 5 percent of its 2021 revenue, totaling 1.75 billion yuan (Global Times 2022).

7. The impact of Chinese Internet restrictions on foreign companies

Since president Xi Jinping assumed office in 2013, European companies have lamented increasing «worrying trends» about increasing restrictive digital controls. These controls, which «can choke business growth and stifle investment in technology and R&D» (Wuttke 2012), are part of a strategy involving «incremental improvements to the regulatory environment [that] yet again failed to adequately counteract the challenges being faced» (European Chamber of commerce in China 2022, 2). In this way, the Csl was considered by European businesses as «omnibus, technology, and sector-neutral» (European union chamber of commerce in China 2021, 338), representing a significant milestone in the journey towards digital liability for Internet-related activities and operators, while also tightening the grip of the party-State over them.

In fact, the European Chamber of commerce in China's 2022 survey reveals that 12% of European firms in China struggle to attract talent due to these Internet restrictions. The Covid-19 pandemic exacerbated these issues, hindering remote work and access to official Vpns, with 48% of Hr departments noting adverse economic impacts, up from 41% in 2015. Additionally, 80% of companies report operational disruptions due to Internet instability and access restrictions.

Challenges in data exchange have affected 49% of European firms, and 70% report that Internet restrictions impact their annual revenue, with 21% experiencing a 6-10% revenue loss. Companies in R&D particularly criticize the limited Internet service access, reflecting broader concerns about the

operational environment in China. Despite these hurdles, Chinese firms have shown remarkable self-sufficiency and innovation, surpassing the Us in international patent filings in April 2020, which intimidates European businesses.

The concerns raised by European companies shed light on the regulatory framework and economic structure of China's cyberspace. China has maintained a strict protectionist policy in key sectors of the Internet, favoring an oligopolistic market where massive State-owned enterprises (Soes) wield significant control over digital facilities. Foreign firms operating in China inevitably encounter state-owned Internet service providers (Isps) that hold dominant positions in their respective markets. The increasing complexity of China's cyberspace regulatory environment is leading to administrative, operational, and cost challenges for organizations, except for state-owned enterprises and government agencies (European Union chamber of commerce in China, 2021, 338).

This stringent regulatory landscape not only hampers the operations of foreign entities but also strategically fosters the growth of domestic champions. China's desire to safeguard against Western influence in its growing and interconnected digital economy has led to the rise of independent Chinese Internet companies, with the most prominent being the «Batx» group, consisting of Baidu, Alibaba, Tencent, and Xiaomi. Partly due to the earlier closure of Western-based counterparts, even before a clear regulatory framework was established (Gao 2011), these companies «have gained almost unlimited and unopposed resources in the Chinese market, including the government's support» (Chandel *et al.*, 2019, 115). As a result, they have gained substantial resources and enjoyed unopposed access to the Chinese market, including government support. This dynamic has further fueled the growth of domestic enterprises that align with the government's interests.

8. Final remarks: towards a global convergence to the Beijing's digital model?

At first, the Prc prioritized sovereignty and security, particularly in relation to perceived ideological and existential threats from «foreign devils» (*yang guizi* 洋鬼子). However, its focus has since broadened to include promoting certain rights and interests of Chinese citizens. In the reorganization of party-State's activities, the cyberspace administration of China plays a pivotal role in regulating opaque practices by addressing the long-standing issue of the privatization of public policymaking and law, which is raging in liberal-democratic countries. Comprehensive regulations implemented by China ha-

ve effectively tackled this problem at its root, though resulting in significant restrictions on citizens' freedom of expression and corporate economic initiative. The instrumentalist characteristic of the Chinese legal tradition (Yu 1989; Wang 2022) has efficiently made the Cac an extension of the party-State, its administrative and regulatory facet on China's cyber realm, allowing it to monitor and scrutinize actions or omissions of private individuals and economic operators while wielding control and protection over sensitive aspects of people's digital lives.

The unique economic and political framework of China grants the cyberspace administration of China an unusual, yet successful centrality within the general and all-pervasive framework of China's cyberlaws and even in the global scenario. China's model of centralizing cyber-related powers and intervening in the digital realm is proliferating globally, influencing also liberal-democratic rule of law states in the West. This trend signals a worldwide move towards legal interventionism aimed at countering external threats and shaping individual behaviors (Hollis and Raustiala 2022; Creemers 2023, 16).

With its historically anti-regulatory stance, the Us has recently begun to grapple with the influence of private entities in shaping public and private regulations (Kello 2021, 11). These entities often use contracts and terms of use as regulatory tools, exploiting the absence of government oversight to advance their profit-driven agendas, frequently at the expense of individuals and citizens (Strange 1996; Rothkopf 2013; Pistor 2019; Ferrarese 2022). As long as rules are set by American companies adhering to Us national interests, the Us have been valuing the Internet as a space of freedom and minimal regulation under the cloak of freedom of expression guaranteed by the first amendment. Nowadays, under the menace of the Chinese adversary (Us 2021), restraints are surfacing precisely when challenges to the primacy of American social networks and data control come from platforms created in China that may still be under the Chinese government's influence (Zhang 2023).

The recent dispute between liberal-democratic systems (and Us above all) and the social creative content platform Tiktok is a demonstration of the legal shrinkage, at least teleologically, between the Beijing model and the Washington-led one (Bernot *et al.* 2024). Rather than passing legislation aimed at defining once and for all citizens' rights in cyberspace for every economic actor, liberal democracies are shifting toward nationalistic, protectionist rhetoric, weaponizing laws as instruments to cement national interests and, thus, moving closer to the way Beijing as historically handle its internal affairs.

Although it is unlikely that the Us and other Western jurisdictions will adopt a cybersecurity model akin to China's, where the party-State controls propaganda, rights, and data through a centralized political-regulatory insti-

tution, they may create institutions that regulate cyberspace while protecting citizens' freedoms and economic liberties and also implementing bodies of law that target foreign influences and competitors. Taking a closer look at our immediate context, the Eu finds itself in a delicate balancing act. Caught between the legal dominance of tech giants, predominantly American but also Chinese, the Eu is striving to strike a challenging equilibrium (Torino 2024). This involves ensuring these tech giants adhere to the rule of law while safeguarding the rights and interests of citizens.

References

Allen-Ebrahimian, B. (2016), "The Man Who Nailed Jello to the Wall", *Foreign Policy*, 29 June, https://foreignpolicy.com/2016/06/29/the-man-who-nailed-jello-to-the-wall-lu-wei-china-internet-czar-learns-how-to-tame-the-web/.

Baran, P. (1962), *On Distributed Communications Networks*, Santa Monica, Rand Corporation.

Bernot, A., Cooney-O'Donoghue D. and Mann, M. (2023), "Governing Chinese Technologies: TikTok, Foreign Interference, and Technological Sovereignty", *Internet Policy Review*, 13(1): 2-26.

Birch, K. and Wellen, R. (2023), *Global Economy and Capitalism*, in S. Scott, K. Birch and R. Wellen (eds.), *Business and Society: A Critical Introduction*, London, Bloomsbury.

Bird, R. (2020), "Am I critical (Information Infrastructure)?", *Freshfields Bruckhaus Deringer*. https://digital.freshfields.com/post/102g5zu/am-i-critical-information-infrastructure.

Bourgon, J. (2021), *Chinese Legal Thought: Overview*, in M. Sellers, S. Kirste (eds.), *Encyclopedia of the Philosophy of Law and Social Philosophy*, Dordrecht, Springer, 1-12.

C-Span (2000), "User Clip: Clinton on Firewall and Jello", *C-Span*, 9 March, https://www.c-span.org/video/?c4893404/user-clip-clinton-firewall-jello.

Cai, X. (2002), "New Fronts, New Challenges, New Countermeasures 新阵地, 新挑战, 新对策", Yunmeng Xuekan 云梦学刊, 2.

Castellucci, I. (2012), *Rule of Law and Legal Complexity in the People's Republic of China*, Trento, University of Trento.

Chandel, S., Jingji, Z., Yunnan, Y., Jingyao, S. and Zhipeng, Z. (2019), "The Golden Shield Project of China: A Decade Later. An In-Depth Study of the Great Firewall", in *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, IEEE, 111-119.

Chen, T. (2022), "Digital Wild West: Foreign Social Media Bans, Data Privacy, and Free Speech", *Hastings Communication & Entertainment Law Journal*, 44(2): 165-194.

Chinese Academy of Cyberspace Studies and Ping, P. (2020), *China Internet Development Report 2018: Blue Book of World Internet Conference*, Beijing, Springler and Publishing House of Electronics Industry.

Creemers, R. (2023), "The Great Rectification: A New Paradigm for China's Online Platform Economy". doi:10.2139/ssrn.4320952.

Cui, S. and Qi, P. (2021), "The Legal Construction of Personal Information Protection and Privacy Under the Chinese Civil Code", *Computer Law Security Review*, 41: 11.

Cyberspace Administration of China (2023), Order No. 17/2023. *Measures on the Standard Contract for Outbound Cross-Border Transfer of Personal Information* 国家互联网信息办公室令, 第13号 2023年2月22日 http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm. Last accessed 11 June 2024.

Cyberspace Administration of China (2019), Order No. 5/2019. *Regulations on the Ecological Governance of Network Information Content* 国家互联网信息办公室令 第5号 2019年12月15日 http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm. Last accessed 11 June 2024.

Cyberspace Administration of China (2020), Order No. 6/2020. *Measures for Cybersecurity Review* 网络安全审查办法.

Cyberspace Administration of China (2022a), *Provisions on the Administration of Internet Posting and Commenting Services*, 16 November http://www.cac.gov.cn/2022-11/16/c_1670253725725039.htm. Last accessed 11 June 2024.

Cyberspace Administration of China (2022b), *Notice on Public Solicitation of Opinions on the "Decision on Amending the Cybersecurity Law of the People's Republic of China (Draft for Comment)* 关于公开征求《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》意见的通知） http://www.cac.gov.cn/2022-09/14/c_1664781649609823.htm. Last accessed 11 June 2024.

Cyberspace Administration of China (2022c), *Decision of Administrative Penalties Related to Network Security Review Against Didi Global Co., Ltd., in accordance with the law.*

Dong, J. (2007), "Enterprises force Internet legislation, while government departments have different attitudes", *China Business News* 中国经营报, 3 September.

Duggal, P. (2020), *Cyberlaw, Cybercrime & Cybersecurity,* in *WSIS Forum 2020 Outcome Document: Fostering digital transformation and global partnerships. WSIS Action Lines for achieving SDGs*, International Telecommunication Union.

Ehrilich, E. (2014), *A Brief History of Internet Regulation*, Washington D.C., Progressive Policy Institute.

English.gov.com. (2014), "Cyberspace Administration of China Launches Official Website" http://english.www.gov.cn/news/top_news/2014/12/31/content_281475032291 728.htm.

Erie, M.S. and Streinz, T. (2021), "The Beijing Effect: China's Digital Silk Road as Transnational Data Governance", *New York University Journal of International Law and Politics*, 54(1): 3-92.

European Chamber of Commerce in China (2020), *European Business in China. Business Confidence Survey 2020. Navigating in the Dark.*

European Parliamentary Research Service (2022), *Governing Data and Artificial Intelligence for All. Models for Sustainable and just data governance,* Scientific Foresight Unit.

European Union Chamber of Commerce in China (2021), *European Business in China Position Paper 2020/2021*, Cybersecurity Sub-working Group.

Fabbri, D. (2018), "L'Impero informatico americano alla prova cinese", *Limes. Rivista italiana di geopolitica*, https://www.limesonline.com/rivista/l-impero-informatico-americano-alla-prova-cinese-14632003/.

Falk, R. (1995), *On Humane Governance: Toward a New Global Politics. The World Order Models Project of the Global Civilization Initiative*, Philadelphia, Pennsylvania State University Press.

Ferrarese, M.R. (2022), *Poteri nuovi*, Bologna, Il Mulino.

Gan, N. (2018), "Cyberspace Controls Set to Strengthen Under China's New Internet Boss", *South China Morning Post*, https://shorturl.at/HAqOe.

Gao, C. (2019), "Double-Faced Lu Wei Jailed for 14 Years for Bribery", *The Diplomat*, 27 March, https://thediplomat.com/2019/03/double-faced-lu-wei-jailed-for-14-years-for-bribery/.

Gao, H. (2004), "John P. Barlow: Declaration of Independence of Cyberspace" (约翰.P.巴洛:《网络空间独立宣言》), *Tsinghua Law Review* 清华法治论衡, 4: 509-511.

Gao, H.S. (2011), "Google's China Problem: a Case Study on Trade, Technology and Human Rights Under the GATS", *Asian Journal of WTO & International Health Law and Policy*, 6: 347-385.

Global Times (2022), "Chinese Online Academic Database CNKI Hit with Heavy Fine After Antitrust Probe", *Global Times*, 26 December, https://www.globaltimes.cn/page/202212/1282688.shtml.

Granet, M. (1934), *La pensée chinoise*, Paris, Albin Michel.

Guo, Z., Hao, J. and Kennedy, L. (2024), "Protection Path of Personal Data and Privacy in China: Moving From Monism to Dualism in Civil Law and the in Criminal Law", *Computer Law & Security Review*, 52: 1-15.

Hanna, N. and Zhen-Wei Qiang, C. (2010), "China's Emerging Informatization Strategy", *Journal of Knowledge Economy*, 1(2): 128-164.

Harvard Law Review (2023), "First Amendment – Regulation of Online Speech – Ninth Circuit Finds First Amendment Violation in School District Officials' Blocking of Parents on Social Media – Garnier v. O'Connor-Ratcliff, 41 F.4th 1158 9th Cir. 2022", *Harvard Law Review*, 136.

Hollis, D. and Raustiala, K. (2022), "The Global Governance of the Internet", *Temple University Legal Studies*, Research Paper No. 2022-17.

Hounsel, A. Mittal, P. and Feamster, N. (2020), "Automatically Generating a Large, Culture-Specific Blocklist for China", USENIX *Workshop on Free and Open Communications on the Internet*, arXiv:1806.03255.

Ikenberry, G.J. (2024), "Three Worlds: the West, East and South and the Competition to Shape Global Order", *International Affairs*, 100(1): 121-138.

Jiang, Z. (2012), *Speech on the Participation in the "Three Stresses" by the Standing Committee of the Central Committee's Political Bureau*, in J. Zemin (ed), *Selected Works of Jiang Zemin*, vol. II, Beijing, Foreign Languages Press.

Kastner, S.L. and Saunders, P.C. (2012), "Is China a Status Quo or Revisionist State? Leadership Travel as an Empirical Indicator of Foreign Policy Priorities", *International Study Quarterly*, 56(2): 163-177.

Kello, L. (2021), "Cyber Legalism: Why it Fails and What to Do About it", *Journal of Cybersecurity*, 7(1): 1-15.

Kettermann, M.C. (2020), *The Normative Order of the Internet: a Theory of Rule and Regulation Online*, Oxford, Oxford University Press.

Kuo, K. *et al.* (2021), "China's Red New Deal: Tracking all the Different Crackdowns on Companies Going on Right Now", The China Project, 9 September, https://thechinaproject.com/2021/09/09/chinas-red-new-deal-a-guide-to-all-the-different-crackdowns-on-companies-going-on-right-now/.

Larsson, T. (2001), *The Race to the Top: The Real Story of Globalization*, Washington D.C., Cato Institute.

Li, Y. (2021), "Cross-border Data Transfer Regulation in China", in S. Calzolaio (ed.), "Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati", *Rivista Italiana di Informatica del Diritto*, 1: 67-87.

Liang J. (2018), "CPC Releases Plan on Deepening Reform of Party and State Institutions", *Xinhua*, 22 March, http://en.people.cn/n3/2018/0322/c90000-9440252.html.

Litant, R.E. (2001), "Law and Policy in the Age of the Internet", *Duke Law Journa*l, 50(4): 1045-1085.

Lum, T. (2006), "Internet Development and Information Control in the People's Republic of China", *Congressional Research Service Reports*.

Mazzucato, M. (2015), *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*, London, Anthem Press.

McWhinney, E. (2000) (ed.), *The United Nations and the New World Order for a New Millennium: Self-Determination, State Succession, and Humanitarian Intervention*, The Hague, Netherlands, Kluwer Law International.

Meyer, N. (2012), *Public Intervention in Private Rule-Making: the Role of the European Commission in Industry Standardization*, Ph.D. Thesis, London School of Economics.

Miao, W. and Wei, L. (2016), "Policy Review: The Cyberspace Administration of China", *Global Media Communication*, 12(3): 337-340.

Milutinović, P. and Nikolić, G. (2023), "Can China Challenge the Technological Supremacy of the United States: Current Standpoint and Perspectives", *The Review of International Affairs*, 74(1187): 87-106.

Ministry of Industry and Information Technology. (2017), Notice No. 32/2017. *Notice of the Ministry of Industry and Information Technology on Cleaning and Regulating the Internet Network Access Service Market*.

Moccia, L. (2009) *Il diritto in Cina. Tra ritualismo e modernizzazione*, Torino, Bollati Boringhieri.

Morrison, F.L. (1998), "Sex, Lies, and Taxes: The American Law of the Internet", *German Yearbook of International Law*, 41: 84-100.

Ohlhausen, M.K. (2012), *The Open Internet: Regulating To Save The Unregulated Internet?*, Washington D.C., Federal Trade Commission.

Omae, K. (1995) (ed), *The Evolving Global Economy: Making Sense of the New World Order*, Harvard, Harvard Business School Press.

Palfrey, J. (2008), "The Public and the Private at the United States Border with Cyberspace", *Missouri Law Journal*, 78: 241-292.

Park, Y. (2023), "China to slash foreign researchers' access to academic database", *Financial Times*, 28 March, https://www.ft.com/content/93051bff-5af8-4841-8e1f-8c9ab0cbd3fe.

People's Republic of China (2020), *Civil Code of the People's Republic of China* 中华人民共和国民法典.

People's Republic of China (2021a), *Data Security Law of the People's Republic of China* 中华人民共和国数据安全法.

People's Republic of China (2021b), *Personal Information Protection Law of the People's Republic of China* 中华人民共和国个人信息保护法.

Perry Barlow, J. (1996), *A Declaration of the Independence of Cyberspace*, Davos, Switzerland, https://www.eff.org/it/cyberspace-independence.

Pistor, K. (2019), *The Code of Capital: How the Law Created Wealth and Inequality*, Princeton, Princeton University Press.

Qiu, J.L. (2003), "The Internet in China: Data and Issues", *Annenberg Research Seminar on International Communication*.

Rothkopf, D. (2013), *Power, Inc.: The Epic Rivarly Between Big Business and Government – and the Reckoning that Lies Ahead,* Farrar, Sraus and Giroux.

Ruo, Y. (2014), "What is Cyber Sovereignty? 什么是网络主权?", Red Flag Manuscripts 红旗文稿, 13.

Rupert, M. (2000), *Ideologies of Globalization: Contending Visions of a New World Order*, New York City, Routledge.

Ryan, J. (2010), *A History of The Internet and the Digital Future*, Chicago, University of Chicago Press.

Sales, N.A. (2003), "Regulating Cyber-Security", *Northwest University Law Review*, 107(4): 1503-1568.

Schmitt, C. (1950), *Der Nomos der Erde im Völkerrecht des Jus Publicum Europaeum*, Berlin, Duncker&Humblot.

Segura-Seranno, A. (2006), *Internet Regulation and the Role of International Law*, in A. von Bogdandy, R. Wolfrum and C.E. Philipp (eds), *Max Planck Yearbook of United Nations Law*, vol. 10, Koninklijke, N.V.

Shinal, J. (2005), "Netscape: the IPO that launched an era", *MarketWatch*, 5 August, https://www.marketwatch.com/story/netscape-ipo-ignited-the-boom-taught-some-hard-lessons-20058518550.

Standing Committee of the National People's Congress (2016), *Cybersecurity Law of the People's Republic of China* 中华人民共和国网络安全法.

State Council of the People's Republic of China (1996), Decree No. 195/1996. *Interim Provisions Governing the Management of the Computer Information Networks in the People's Republic of China Connecting to the International Network.*

State Council of the People's Republic of China (2000), Decree No. 292/2000. *Decree on Administrative Measures on Internet Information Services.*

State Council of the People's Republic of China (2008), Decree No. 11/2008. *Notice of the State Council on the establishment of institutions*.

State Council of the People's Republic of China (2014), Decree 33/2014. *Notice on authorizing the Cyberspace Administration of China*.

State Council of the People's Republic of China (2021), Decree No. 745/2021. *Critical Information Infrastructure Security Protection Regulations*.

Stockwell, J. (1990), *The Praetorian Guard: The U.S. Role in the New World Order*, Boston, South End Press.

Strange, S. (1996), *The Retreat of the State: The Diffusion of Power in the World Economy*, Cambridge, Cambridge University Press.

Supreme Court of the United States of America (1997). *Reno v. American Civil Liberties Union*, 521: 844-868.

Supreme Court of the United States of America (2017). *Packingham v. North Carolina*, 137 S. Ct. 1730.

Svensson, M. (2019), *Human rights and the Internet in China: New Frontiers and Challenges*, in S. Biddulph and J. Rosenzweig (eds.), *Handbook of Human Rights in China*, Northampton, Edward Elgar Publishing.

Tai, K. and Zhu, Y. Y. (2022). "A Historical Explanation of Chinese Cybersovereignty", *International Relations of Asia-Pacific*, 22: 469-499.

Time Magazine (1957), *The Nation: Red Moon Over the U.S.*, 14 October, New York City.

Torino, R. (2024), *Social Platforms and Protection of User Rights*, in R. Torino and S. Zorzetto (eds.), *La trasformazione digitale in Europa. Diritti e principi*, Torino, Giappichelli: 131-156.

Tosza, S. (2021), "Internet Service Providers as Law Enforcers and Adjudicators. A Public Role of Private Actors", *Computer Law Security Review*. doi:10.1016/j.clsr.2021.105614.

Tucker, R.W. and Hendrickson, D.C. (1992). *The Imperial Temptation: The New World Order and America's Purpose,* New York City, Council on Foreign Relations Press.

United States (1996), 47 U.S.C. § 151.

United States (1996), *Telecommunications Act of 1996*, 47 U.S.C. 609.

United States (2018), 6 U.S.C. § 651, Public Law 115-278.
United States (2021), Executive Order 14034, 9 June, *Protecting Americans' Sensitive Data From Foreign Adversaries*.
Von Bernstorff, J. (2003), "Democratic Global Internet Regulation? Governance Networks, International Law and the Shadow of Hegemony", *European Law Journal*, 9(3): 511-526.
Wang, L. (2013), "On the Legal Protection of Personal Information Rights 论个人信息权利的法律保护", *Xindai Faxue* 现代法学», 4.
Wang, S. (2022), "Authoritarian Legality and Legal Instrumentalism in China", *Chinese Journal of Comparative Law*, 10(1): 154-162.
Wang, X. (2007), "Cybersecurity Legislation Should no Longer Proceed at a Leisurely Pace 网络安全立法, 别再以散步的速度前行", *Legal Daily* 法制日报, 17 May.
Wang, Y. and Xin, Q. (2024), "Internet Sovereignty, an Inevitable Issue 互联网主权是一个不可避免的问题", *People's Daily* 人民日报, 23 April.
Werle, R. and Iversen, J. E. (2006), "Promoting Legitimacy in Technical Standardization", *Science Technology & Innovation Studies*, 2(1): 19-39.
Wuhan University *et al.* (2020). "Cyber Sovereignty: Theory and Practice (Version 2.0) 网络主权:理论与实践(2.0版)". *Cyberspace Administration of China*, 25 November, http://www.cac.gov.cn/2020-11/25/c_1607869924931855.htm.
Wuttke, J. (2012), "European Business Group Slams China's Internet Controls", *Reuters*, February 12, https://www.reuters.com/article/rbssITServicesConsulting/idUSL4N0VM2FH2015021.
Xi, J. (2014), Explanatory Notes to the "Decision of the Central Committee of the Communist Party of China on Some Mayor Issues Concerning Comprehensively Continuing the Reform, November 9, 2013, in J. Xi (ed.), The Governance of China, Vol. I, Beijing, Foreign Languages Press.
Xu, L. (2016), *Development, Security and Governance: An Agenda for China Cyberspace Governance*, in X. Jian (ed.), *Civilizational Revitalization and Remaking: Period of Strategic Opportunities in a Historical Perspective*, Beijing, People's Publishing House.
Yoo, C. (2010), "Innovations in the Internet's Architecture that Challenge the Status Quo", *Journal on Telecommunications and High Technology Law,* 8: 86-90.
Yu, X. (1989), "Legal Pragmatism in the People's Republic of China", Cornell Law Faculty Publications, 3(9): 29-51.
Zhang, B. (2019), "Collection of Personal Information: the Limits of Applying the Principle of Informed Consent", *Bijiaofa Yanjiu*比较法研究, 6.
Zhang, X. and Xu, K. (2016), "The Governance Model and Institutional Construction of Cyberspace Sovereignty 网络空间主权的治理模式及其制度构建", *Chinese Social Sciences* 中国社会科学, 8: 139-158.
Zhang, Z. (2023), "Paradigms for Foreign Tech-Platforms Regulation: U.S. Options after the TikTok Saga", *Washintong Journal Law of Tech & Arts*, 18(1): 3-28.
Zhi, Z. (2016), "Cyber Sovereignty Guides the New Pattern of International Governance", *People's Daily* 人民日报, 5 January.