Vanderbilt Journal of Transnational Law

Volume 55
Issue 3 *May 2022*

Article 2

5-2022

Comparative Cybersecurity Law in Socialist Asia

Ngoc S. Bui
University of Oxford

Jyh-An Lee
The Chinese University of Hong Kong

Comparative Cybersecurity Law in Socialist Asia

Ngoc Son Bui* & Jyh-An Lee**

ABSTRACT

This Article is a comparative study of the cybersecurity laws adopted in China and Vietnam in 2017 and 2018, respectively. The two laws both converge and diverge. Their convergences include the stringent regulation of banned acts, network operators, critical infrastructure, data localization, and personal data. These are all shaped by the immediate diffusion of China's Cybersecurity Law in Vietnam and broader structural factors: namely, the common features of the socialist state, socialist legality, and the statist approach to human rights. The foundational divergence is between the Chinese notion of cybersecurity sovereignty and the Vietnamese notion of national cyberspace, which is due to the global diffusion of cybersecurity law in Vietnam and the differences in technological infrastructure and developmental approaches—Chinese exceptionalism and Vietnamese universalism. This Article has implications for comparative law generally and comparative cybersecurity law particularly.

TABLE OF CONTENTS

I. INTRODUCTION 632
II. SOCIALIST REGULATION OF CYBERSECURITY 637
A. Background 637
1. China 637
2. Vietnam 640
B. National Cyberspace 643
1. China 643
2. Vietnam 645
C. Major Legal Issues 646
1. Prohibited Acts 646
2. Network Operators 649

---

* Associate Professor of Asian Laws, Faculty of Law, University of Oxford

** Professor and Director, Centre for Legal Innovation and Digital Society (CLINDS), Faculty of Law, The Chinese University of Hong Kong. The authors thank Sally Daultrey, Debrea Kennedy-Mayo, Mailyn Fidler, Charlotte Tschider and participants at the Cybersecurity Law and Policy Scholars Conference held by the University of Minnesota Law School for helpful comments. The authors are also grateful to Yangzi Li for her research assistance on Chinese Cybersecurity Law.

3. Critical Infrastructure 650
4. Data Localization 652
5. Security Evaluation, Assessment, Inspection, and Supervision 657
6. Personal Data Regime 660
D. Implementation 664
1. China 664
2. Vietnam 665
III. COMPARATIVE ANALYSIS 666
A. Convergences 666
1. Immediate Diffusion of Cybersecurity Law 667
2. The Socialist State: Cybersecurity as Regime Security 668
3. Socialist Legality and Cybersecurity 670
4. Statist Digital Rights 672
B. Divergences 674
1. Technological Architecture 675
2. Exceptionalism vs. Universalism 676
IV. CONCLUSION 678

I. INTRODUCTION

The socialist states of China and Vietnam have comprehensively regulated cybersecurity. China's Cybersecurity Law, which has been arguably one of the most massive regulatory concerns for foreign businesses,[1] came into effect on June 1, 2017.[2] One year after China, Vietnam adopted a similar Cybersecurity Law on June 12, 2018, which came into effect on January 1, 2019.[3]

China's Cybersecurity Law represents the country's determination to build robust digital infrastructure against cybersecurity threats. China has also actively established new cybersecurity institutions, laws, guidelines, and standards in the past

---

1. *See, e.g.*, Huifeng He, *Cybersecurity Law Causing 'Mass Concerns' Among Foreign Firms in China*, S. CHINA MORNING POST (Mar. 1, 2018), https://www.scmp.com/news/china/economy/article/2135338/cybersecurity-law-causing-mass-concerns-among-foreign-firms-china [https://perma.cc/Z577-X2YG] (archived Mar. 2, 2022).

2. Zhonghua Renmin Gongheguo Wanglao Anquan Fa (中华人民共和国网络安全法) [China's Cybersecurity Law] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017), art. 79, http://www.cac.gov.cn/2016-11/07/c_1119867116.htm [https://perma.cc/9MTQ-MTTR] (archived Mar. 2, 2022) [hereinafter China's Cybersecurity Law].

3. Law on Cybersecurity, 2018 (Act No. 24/2018/QH14) (Viet.), art. 43.

five years.[4] The promulgation of a series of cybersecurity laws and rules has echoed President Xi Jinping's pronouncement that "without cybersecurity there is no national security."[5] The enactment of the law drew intense criticism and opposition from foreign businesses, such as Amazon, IBM, Intel, and Microsoft.[6] Both the American Chamber of Commerce and European Chamber of Commerce cast serious doubt on the justification of this legislation.[7] Multinational bodies claimed that the law has possibly enabled more government censorship and surveillance, increased business operating costs and risk of intellectual property infringement, and reinforced the country's protectionism from global competition.[8] However, resistance against the law has gradually withered since the law came into effect in 2017.

The enactment of the Cybersecurity Law in Vietnam is a response to the booming internet in the country and potential threats to national security. Vietnam has over sixty-six million internet users among a population of over ninety-five million people.[9] The number of internet

---

4. *See, e.g.*, Adam Segal, Valeriy Akimenko, Keir Giles, Daniel A. Pinkston, James A. Lewis, Benjamin Bartlett, Hsini Huang, & Elina Noor, *China's Pursuit of Cyberpower*, 15 ASIA POL'Y, no. 2, 2020, at 60, 60.

5. *See, e.g.*, Meirong Guo, *China's Cybersecurity Legislation, Its Relevance to Critical Infrastructures and the Challenges It Faces*, 22 INT'L J. CRITICAL INFRASTRUCTURE PROT. 139, 140 (2018); Samm Sacks, *China's Cybersecurity Law Takes Effect: What to Expect*, LAWFARE (June 1, 2017, 10:56 AM), https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect [https://perma.cc/RK6A-MNFG] (archived Feb. 18, 2022).

6. *See, e.g.*, Jyh-An Lee, *Hacking into China's Cybersecurity Law*, 53 WAKE FOREST L. REV. 57, 61 (2018); Eva Dou, *Microsoft, Intel, IBM Push Back on China Cybersecurity Rules*, WALL ST. J. (Dec. 1, 2016, 5:19 AM), https://www.wsj.com/articles/microsoft-intel-ibm-push-back-on-china-cybersecurity-rules-1480587542 [https://perma.cc/BQF8-H9D5] (archived Feb. 18, 2022).

7. *See, e.g.*, Josh Horwitz, *A Key Question Is at the Heart of China's New Cybersecurity Law: Where Should Data Live?*, QUARTZ, (June 7, 2017), https://qz.com/999613/a-key-question-at-the-heart-of-chinas-cybersecurity-law-where-should-data-live/ [https://perma.cc/888K-U89Q] (archived Feb. 18, 2022); Sui-Lee Wee, *China's New Cybersecurity Law Leaves Foreign Firms Guessing*, N.Y. TIMES (May 31, 2017), https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html?mcubz=0 [https://perma.cc/C7M8-WSC9] (archived Feb. 18, 2022); Zhuang Pinhui & Reuters, *China Pushes Through Cybersecurity Law Despite Foreign Business Fears*, S. CHINA MORNING POST (Nov. 7, 2016), https://www.scmp.com/news/china/policies-politics/article/2043646/china-pushes-through-cybersecurity-legislation-heavily [https://perma.cc/2R4B-LJ28] (archived Feb. 18, 2022).

8. Lee, *supra* note 6, at 62–63, 77, 88; Jacob Quinn, Comment, *A Peek Over the Great Firewall: A Breakdown of China's New Cybersecurity Law*, 20 SMU SCI. & TECH. L. REV. 407, 432 (2017).

9. *Quyền con người trên không gian mạng ở Việt Nam luôn được đảm bảo* [*Human rights in Cyberspace in Vietnam are Always Guaranteed*], BÁO CÔNG AN NHÂN DÂN ĐIỆN TỬ [PUB. SEC. NEWS] (Aug. 9, 2020) (Viet.), http://cand.com.vn/Nhan-quyen/Quyen-con-nguoi-tren-khong-gian-mang-o-Viet-Nam-luon-duoc-dam-bao-610658/ [https://perma.cc/8S49-6EMA] (archived Feb. 18, 2022); *Vietnam: Total Population from 2016 to 2026*, STATISTICA (Nov. 23, 2021), https://www.statista.com/statistics/

users per one hundred people is 68.70; the number of households with an internet connection is 19,158,310; and the number of households with an internet connection per one hundred households is 71.30.[10] In April 2019, the 5G Base Transceiver station was deployed in the Hoan Kiem Lake area (Hanoi), making Vietnam one of the earliest 5G countries in the world. It has a connection speed of 600–700Mbps—equivalent to the service speed provided to customers of the Verizon 5G network in the United States.[11]

While the Vietnamese government claims that this law is necessary to protect "national security, social order and safety, or the lawful rights and interests of agencies, organizations and individuals,"[12] it has been met with vehement criticism from both local and international actors. Many critics believe that the Vietnamese Cybersecurity Law is a mere copy of China's Cybersecurity Law and that it undermines internet freedom and economic development.[13]

Domestic opposition to the law in Vietnam even led to legal mobilization. Two days before its adoption, on June 10, 2018, thousands of people in the capital of Hanoi, Ho Chi Minh City, and other provinces (Đà Nẵng, Nha Trang, Bình Thuận, Bình Dương, Đồng Nai, and Vũng Tàu) held peaceful protests against the Cybersecurity Bill, worrying that it would kill their constitutional rights to freedom of speech, freedom of information, and personal privacy.[14]

Vietnam's Cybersecurity Law was also subject to international criticism. Seventeen US lawmakers urged the CEOs of Facebook and Google to oppose it, believing that the law would "bolster the government's crackdown on online political activism."[15] Amnesty International also wrote a series of open letters to the executives of

---

444597/total-population-of-vietnam/ [https://perma.cc/P4GM-5CTR] (archived May 6, 2022).

10. *Id.*

11. *Id.*

12. Law on Cybersecurity, 2018 (No 24/2018/QH14) (Viet.), art. 2.

13. *Luật An ninh mạng, bước lùi lớn cho VN* [*Cybersecurity Law, Vietnam's Big Drawback*], BBC (June 12, 2018) (Viet.), https://www.bbc.com/vietnamese/vietnam-44449357 [https://perma.cc/5L4T-2Q6S] (archived Feb. 18, 2022) [hereinafter *Vietnam's Big Drawback*]; *Vietnam's Cybersecurity Law Sparks Concerns from Businesses*, NIKKEI Asia (June 12, 2018), https://asia.nikkei.com/Politics/Vietnam-s-cybersecurity-law-sparks-concerns-from-businesses [https://perma.cc/S96R-WLZB] (archived May 6, 2022).

14. *See* Trung Khang, *Một năm sau tổng biểu tình chống Luật Đặc khu và Luật An ninh mạng* [*One Year After the Protests against the Special Economic Zones Bill and Cybersecurity Bill*] , RADIO FREE ASIA (June 7, 2019) (Viet.), https://www.rfa.org/vietnamese/in_depth/one-year-after-the-protest-against-the-sez-bill-special-law-and-the-cyber-security-law-06072019142743.html [https://perma.cc/CP97-5TP9] (archived Feb. 18, 2022).

15. James Pearson & Mai Nguyen, *U.S. Lawmakers Urge Google, Facebook to Resist Vietnam Cybersecurity Law*, REUTERS (July 17, 2018), https://www.reuters.com/article/idUSL4N1UD28H [https://perma.cc/KM46-SGVE] (archived Feb. 18, 2022).

Apple, Facebook, Google, Microsoft, and Samsung, calling on these companies to "challenge" Vietnam's Cybersecurity Law on the grounds of fundamental human rights.[16]

Although one study has provided a thorough analysis of China's Cybersecurity Law,[17] so far, academic writings in English about Vietnam's Cybersecurity Law are largely absent, although it has been the subject of several popular policy commentaries.[18] This Article seeks to fill in this academic gap. From a comparative regulatory perspective, this Article seeks to understand the convergences and divergences between these two cybersecurity regimes in China and Vietnam.

Like China, Vietnam is a highly regulatory state. This characteristic is particularly prominent in the country's regulation of the internet. Therefore, it is appropriate to situate the legal framework for cybersecurity within regulatory scholarship.[19] In a recent study, Chritel Koop and Martin Lodge defined regulation as "intentional intervention in the activities of a target population, where the intervention is typically direct – involving binding standard-setting, monitoring, and sanctioning – and exercised by public-sector actors on the economic activities of private-sector actors."[20] Based on this pattern-based definition of regulation, this Article defines the regulation of cybersecurity as *the state's intervention into the activities of target agencies, organizations, and individuals for the purpose of protecting cybersecurity.*

Regulatory scholars have proposed several theories explaining the factors behind regulation: public interest theories, private interest theories, and institutional theories.[21] The interest-based theories (whether public or private) may be more relevant to explaining the regulation of economic activities. The institutional theories are more general, however, which can be useful in explaining the regulation of both economic and non-economic activities.[22] This Article therefore situates the cybersecurity regulation in China and Vietnam within the broader institutional context and argues about both convergences and

---

16. *Vietnam's Big Drawback*, *supra* note 13.

17. *See* Lee, *supra* note 6.

18. *See generally* Timothy McLaughlin, *Under Vietnam's New Cybersecurity Law, U.S. Tech Giants Face Stricter Censorship*, WASH. POST (Mar. 16, 2019), https://www.washingtonpost.com/world/asia_pacific/under-vietnams-new-cybersecurity-law-us-tech-giants-face-stricter-censorship/2019/03/16/8259cfae-3c24-11e9-a06c-3ec8ed509d15_story.html [https://perma.cc/P6GD-KKM6] (archived Feb. 18, 2022).

19. *See generally* A READER ON REGULATION (Robert Baldwin, Colin Scott, & Christopher Hood eds., 1998).

20. Christel Koop & Martin Lodge, *What is Regulation? An Interdisciplinary Concept Analysis*, 11 REGUL. & GOVERNANCE 95, 105 (2015).

21. BRONWEN MORGAN & KAREN YEUNG, AN INTRODUCTION TO LAW AND REGULATION 16 (2007).

22. *Id.* at 53.

divergences in the two countries' cybersecurity legal regimes. The convergence of the two laws is due in part to the immediate diffusion of China's Cybersecurity Law in Vietnam, but it is more deeply shaped by structural factors; namely, the ideational and institutional similarities between China and Vietnam. These structural factors include the socialist state, the principle of socialist legality, and the statist approach to human rights generally and digital rights particularly.

Despite these convergent features, there is a foundational divergence in the socialist cybersecurity regulatory regime between the Chinese notion of cybersecurity sovereignty and Vietnamese view of national cyberspace. The reasons for this divergence are both technological and political.

First, compared to China's counterpart, the cybersecurity regulatory regime in Vietnam tolerates greater citizen internet freedom for technological reasons. Without a Great Firewall or internet filtering, Vietnamese citizens can enjoy Google, Facebook, Twitter, and YouTube freely. In contrast, China has developed Chinese alternatives to these platforms (Baidu, WeChat, Weibo, and Youku, respectively).[23] The Vietnamese government does not have technological alternatives to control activities in cyberspace, so the Vietnamese cybersecurity regulatory framework must tolerate citizens' internet freedom to a certain extent.

Second, Chinese exceptionalism generates the concept of cybersecurity sovereignty as the basis of China's distinctive form of technological innovation and broader development according to socialism with Chinese characteristics. Conversely, Vietnamese universalism enables it to reference the global experience of cybersecurity law and regulate cyberspace while treating the internet as a global network beyond national sovereignty.

This Article contributes to the scholarship on comparative law. While both China and Vietnam are socialist countries with similar cybersecurity laws, the social reactions to and the actual implementations of the laws in the two countries differ significantly. Therefore, a careful examination of influencing factors, such as legal culture, political economy, and technological infrastructure, will provide a valuable lens for comparative law studies.

This Article is structured as follows. Part II descriptively explores the regulatory framework of cybersecurity in Vietnam compared to

---

23. *See, e.g.*, Jyh-An Lee, Ching-Yi Liu, & Weiping Li, *Searching for Internet Freedom in China: A Case Study on Google's China Experience*, 31 CARDOZO ARTS & ENT. L.J. 405, 424 n.126 (2013); Jyh-An Lee & Ching-Yi Liu, *Real-Name Registration Rules and the Fading Digital Anonymity in China*, 25 WASH. INT'L L.J. 1, 27 (2016) [hereinafter Lee & Liu, *Real-Name Registration Rules*]; Anqi Wang, *Cyber Sovereignty at Its Boldest: A Chinese Perspective*, 16 OHIO ST. TECH. L.J. 395, 409–10 (2020).

China, demonstrating how the two laws have institutionalized the two socialist states' longstanding assertions of internet sovereignty under the pretense of protecting cybersecurity and how the cybersecurity laws are designed to strengthen national security. This Part then explores major legal issues in the substance of the cybersecurity laws, which include the obligations of network operators, defense of critical infrastructure, data localization, security review, and protection of personal information. Part III comparatively analyzes the divergences and convergences in cybersecurity regulation in China and Vietnam, explaining the diffusion of China's Cybersecurity Law in Vietnam and the laws' convergent ideational and institutional factors, including the unique socialist approaches to cybersecurity, market intervention, legal ambiguity, and statist digital human rights. The underlying socialist value and ideology shared between China and Vietnam are significantly different from those in the Western world. This Part also explains divergences in cybersecurity regulation in the two countries. Finally, Part IV concludes.

II. SOCIALIST REGULATION OF CYBERSECURITY

Despite different approaches to the notion of cyberspace sovereignty and legal liabilities, the cybersecurity laws in China and Vietnam are similar in many ways. Both laws were enacted as national security legislation and include many similar provisions. This Part describes their background, the role of cyberspace sovereignty, the main legal issues, and the implementation of the cybersecurity laws in these two socialist states.

A. *Background*

1. China

Cybersecurity has been defined as a national security issue in China, and its Cybersecurity Law is unsurprisingly viewed as a legal tool to strengthen its national security.[24] Therefore, the Cybersecurity Law does not stand alone but should be understood alongside other legislative programs for national security promulgated in recent years,

24. Chieh Huang, *China's Take on National Security and Its Implications for the Evolution of International Economic Law*, 48 LEGAL ISSUES ECON. INTEGRATION 119, 127 (2021); Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?*, 8 PENN. ST. J.L. & INT'L AFF. 49, 109 (2020).

such as the National Security Law[25] and the Counterterrorism Law.[26] Furthermore, China's unique internet architecture—the so-called Great Firewall—also plays an important role in facilitating its control of online information flow and the implementation of its laws.[27]

On July 1, 2015, China passed its National Security Law,[28] Article 2 of which defines "national security" as "a status in which the regime, sovereignty, unity, territorial integrity, welfare of the people, sustainable economic and social development, and other major interests of the state are relatively not faced with any danger and not threatened internally or externally and the capability to maintain a sustained security status."[29] The purpose of the law is to protect "the regime of people's democratic dictatorship," "the socialist system with Chinese characteristics," and "the fundamental interest of the people" with a view to advance "reform, opening up, and socialist modernization."[30] The law broadly defines national security to include cybersecurity. In particular, Article 25 requires the government to "build a network and information security guarantee system," "improve network and information security protection capability," ensure "the controllable security of the core technologies and crucial infrastructure of network and information and the information systems and data in important fields," and "strengthen network management, prevent, frustrate, and . . . punish network attack, network invasion, network information theft, dissemination of illegal and harmful information, and other network-related infractions of law and crimes, and maintain the state's sovereignty, security, and development interests in the cyberspace."[31] Article 59 stipulates that the government should "conduct national security review" of "key technologies and network information technology products and

---

25. Zhonghua Renmin Gongheguo Guojia Anquan Fa (中华人民共和国国家安全法) [China's National Security Law] (promulgated by Standing Comm. Nat'l People's Cong., July 1, 2015, effective July 1, 2015) (translation available at https://chinacopyrightandmedia.wordpress.com/2015/07/01/national-security-law-of-the-peoples-republic-of-china/ [https://perma.cc/AP6V-VATN] (archived Feb. 18, 2022)).

26. Zhonghua Renmin Gongheguo Fan Kongbu Zhuyi Fa (中华人民共和国反恐怖主义法) [China's Counterterrorism Law] (promulgated by Standing Comm. Nat'l People's Cong., Dec. 27, 2015, effective Jan. 1, 2016) (translation available at https://www.uschina.org/china-hub/unofficial-translation-counter-terrorism-law-peoples-republic-china [https://perma.cc/G8MB-EFW2] (archived Feb. 18, 2022)).

27. *See, e.g.*, Jyh-An Lee & Ching-Yi Liu, *Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China*, 13 MINN. J. L. SCI. & TECH. 125, 129–35 (2012); Xiao Qiang, *The Road to Digital Unfreedom: President Xi's Surveillance State*, 30 J. DEMOCRACY 53, 55–56 (2019).

28. China's National Security Law.

29. *Id.* art. 2.

30. *Id.* art. 1.

31. *Id.* art. 25.

services that affect or may affect national security."[32] The broad scope covered by these cybersecurity-related provisions in the National Security Law informs the later enactment of the Cybersecurity Law.[33]

The main legislative purpose of China's Cybersecurity Law is to protect national security. Article 1 of the Cybersecurity Law makes this purpose quite explicit: "This Law is enacted for the purposes of guaranteeing cybersecurity, safeguarding cyberspace sovereignty, national security and public interest."[34] Article 12 stipulates that

> [a]ny individual or organization . . . shall not use the network to conduct any activity that endangers national security, honor and interest, incites to subvert the state power or overthrow the socialist system, incites to split the country or undermine national unity, advocates terrorism or extremism, [or] propagates ethnic hatred or discrimination.[35]

As part of the national security legislation, the Counterterrorism Law came into effect on January 1, 2016.[36] The Counterterrorism Law on the one hand obliges "telecommunications business operators and internet service providers to provide technical support and assistance—such as technical interface and decryption—to public security authorities and national security authorities to prevent and investigate terrorist activities"[37] and on the other hand provides competent authorities with the power to "order applicable entities to cease the transmission of and delete relevant information pertaining to any terrorist or extremist content or to order them to shut down the relevant websites and terminate the provision of the relevant services."[38] Competent telecommunications authorities must also "block terrorist or extremist content transmitted from abroad via the internet."[39] Overall, the Counterterrorism Law has facilitated government control of information via telecommunications and internet service providers in the name of security.[40]

---

32. *Id.* art. 59.
33. *See, e.g.*, Huang, *supra* note 24, at 126–27.
34. China's Cybersecurity Law, art. 1.
35. *Id.* art. 12.
36. Zhonghua Renmin Gongheguo Fan Kongbu Zhuyi Fa (中华人民共和国反恐怖主义法) [China's Counterterrorism Law] (promulgated by Standing Comm. Nat'l People's Cong., Dec. 27, 2015, effective Jan. 1, 2016), art. 97 ("This Law shall come into force on January 1, 2016.") (translation available at https://www.uschina.org/china-hub/unofficial-translation-counter-terrorism-law-peoples-republic-china [https://perma.cc/G8MB-EFW2] (archived Feb. 18, 2022)).
37. *Id.* art. 18.
38. *Id.* art. 19.
39. *Id.*
40. Emilio Iasiello, *China's Cyber Initiatives Counter International Pressure*, 10 J. STRATEGIC SEC. 1, 11 (2017).

2. Vietnam

In the same vein, Vietnam's Cybersecurity Law is a part of the government's larger legal framework for national security. Vietnam also has the National Security Law and the Counterterrorism Law. Apart from these two laws, various bureaucratic bodies issue numerous administrative measures to handle specific aspects of national security. On September 17, 2020, there were 691 reported legislative and administrative instruments on national security.[41] The Vietnamese state, therefore, has a solid regulatory framework for national security, part of which is the Cybersecurity Law.

Vietnam's National Security Law was adopted by the National Assembly on December 3, 2004.[42] The law defines "national security" as "the stability and sustainable development of the socialist regime and the State of the Socialist Republic of Vietnam, the inalienability of the independence, sovereignty, unity and territorial integrity of the Fatherland."[43] National security protection includes the protection of the socialist regime, national sovereignty, and territorial integrity. However, national security projection is broadly extended to the protection of "ideological and cultural security, the national unity bloc, the legitimate rights and interests of agencies, organizations and individuals," and "security in the economic, defense, external relation domains and other national interests."[44] These provisions give the government ample space to undertake measures to protect national security, including controlling the flow of information on the internet.

The Cybersecurity Law is, therefore, a tool of national security protection broadly conceived of by the National Security Law. Article 1 of the Cybersecurity Law defines its aims as protecting "national security and ensuring social order and safety in cyberspace; and the responsibilities of agencies, organizations and individuals involved."[45] The Cybersecurity Law aims to protect the security of not only cyberspace but also of the physical space of the socialist regime.

This aim differentiates the Cybersecurity Law from another related law, the Network Information Security Law, which was enacted by the Vietnamese National Assembly in 2015. The scope of this law includes "network information security activities, rights and duties of agencies, organizations and individuals in securing network

41. Văn bản Luật An ninh quốc gia [Legal Instruments on National Security], https://luatvietnam.vn/an-ninh-quoc-gia-46-f1.html (Viet.) [https://perma.cc/3XAM-A72P] (archived Feb. 18, 2022).

42. The Law of the National State of the Socialist Republic of Vietnam, 2004 (No. 32/2004/QH11) (Viet.).

43. *Id.* art. 3.

44. *Id.* art. 14.

45. Law on Cybersecurity, 2018 (No. 24/2018/QH14) (Viet.), art. 1.

information security; civil cryptography; technical standards and norms of network information security; business in information security; human development for network information security; [and] state management of network information security."[46] There were controversial debates on the overlap between the two laws.[47] One relevant authority has explained that the two laws are related, not overlapping.[48] To illustrate, Nguyễn Văn Thỉnh, Deputy Director of the Department of Cyber Security under the Ministry of Public Security and a member of the drafting committee of the Cyber Security Law, stated that

> the scope of Network Information Security Law focuses on the properties of network information with three characteristics: integrity, safety, and usefulness. Meanwhile, the Cybersecurity Law focuses on using cyberspace, without harming the objects, which is completely different from Network Information Security Law. The Cybersecurity Law focuses on protecting the regime and the Socialist State of Vietnam, on independence, sovereignty, territorial unification, national security, social order and safety, the rights and interests of legal organizations and individuals.[49]

This official statement suggest that the goal of the Network Information Security Law is technological while the goal of the Cybersecurity Law is political. However, the dichotomy between technology and politics is not always clear in the two laws. As indicated below, the Cybersecurity Law includes many technological provisions underpinned by political ideology and commitments to national security.

To better understand the link of Vietnam's Cybersecurity Law to broader national security, consider an article published in the *Communist Review* (*Tap chi Cong San*) on the Cybersecurity Law by Nguyễn Minh Chính, Chairman of the Department of Cyber Security and High-Tech Crime Prevention under the Ministry of Public Security of the Vietnamese government.[50] His article presents official concerns in promulgating the law, as it was authored by the head of the relevant

---

46. Law on Network Information Security, 2015 (No. 86/2015/QH13) (Viet.), art. 1.

47. Anh Lê, *Tranh luận về Dự thảo Luật An ninh mạng: Trùng lắp với các quy định pháp luật hiện hành?* [Debating the Draft Law on Cybersecurity: Overlapping with Current Legal Provisions?], VIETTIMES (Nov. 11, 2017), https://viettimes.vn/tranh-luan-ve-du-thao-luat-an-ninh-mang-trung-lap-voi-cac-quy-dinh-phap-luat-hien-hanh-post64469.html [https://perma.cc/CX9M-FA36] (archived Feb. 18, 2022).

48. *Id.*

49. *Id.*

50. Nguyễn Minh Chính, *Hoàn thiện pháp luật về an ninh mạng trong tình hình hiện nay* [*Completing the Law on Network Security in the Current Situation*], TAP CHI CONG SAN COMMUNIST REV. (Sept. 25, 2019) (Viet.), http://tapchicongsan.org.vn/an-ninh2/-/2018/812604/hoan-thien-phap-luat-ve-an-ninh-mang-trong-tinh-hinh-hien-nay.aspx [https://perma.cc/78Z8-A64R] (archived Feb. 18, 2022).

authority and published in the mainstream outlet of the Communist Party of Vietnam. The article provides the following justifications for the Cybersecurity Law:

First, "hostile reactionary forces" have increasingly used cyberspace to sabotage ideology, conduct internal sabotage, carry out "peaceful evolution," cause national conflicts, and incite demonstrations, violence, and chaos aimed at transforming political institutions in Vietnam.[51] Second, fake news, false information, and "poisonous news" (news harming the legitimate rights and interests of organizations and individuals) are increasingly serious.[52] Vietnam currently has 410 licensed social networking sites, and Facebook and YouTube are the two most influential foreign social networks, of which Facebook has more than sixty million users in Vietnam.[53] "However, these two social networks are also the places to spread [much] bad and poisonous information today, with a series of pages of reactionary, hostile, anti-dissident organizations. Some Facebook pages [with such information] have the number of followers up to hundreds of thousands."[54]

Third, Vietnam's network, like that in other countries, faces increasingly dangerous, large-scale cyberattacks.[55] Vietnam is ranked twentieth among the countries in the world whose network systems are attacked by malware and eighth of the top ten countries in the world for local malware infection.[56] Since the end of 2015, 12,360 news sites with the national domain name portal of Vietnam (.vn) have been attacked by hackers, including over four hundred websites and portals of state agencies; 9,763 websites have been attacked by foreign hackers; and 2,597 websites have been attacked by domestic hackers and groups.[57]

Fourth, information appropriation, disclosure of state secrets, and personal information disclosure of in-type users are worrying.[58] Fifth, criminal activities (e.g., fraud and online gambling organizations) using high technology have increased in number and sophistication, causing serious damage in many aspects and long-term consequences for society.[59] Particularly, Vietnam has about five hundred approved online games and more than thirty-three million players, with revenue reaching more than $380 million per year, as well as about forty large-

51. *Id.*
52. *Id.*
53. *Id.*
54. *Id.*
55. *Id.*
56. *Id.*
57. *Id.*
58. *Id.*
59. *Id.*

scale illegal online games. [60] Sixth, the state administration of cyberspace faces many challenges in the context of new online services (e.g., online payment, e-commerce, online games, virtual currency trading, and multi-level business). [61] Finally, the training of cybersecurity experts is limited and does not yet meet actual need.[62]

The official justifications for the Cybersecurity Law are not merely technological (e.g., preventing fake news and cyberattacks) but are also ideological and political. The law aims to prevent the use of the internet to disseminate information and ideas hostile to socialist ideology and to avoid the use of cyberspace to mobilize for regime change in Vietnam.

The Vietnamese government also promulgated the Counterterrorism Law on December 3, 2013. Terrorist activities include aspects relevant to the Cybersecurity Law—namely, "attacking, harming, obstructing, [and] disrupting the operation of computer networks, telecommunications networks, internet networks, [and the] digital equipment of agencies, organizations or individuals."[63] The law vests competent agencies and persons with the authority to detect and prevent publishing, posting, telecommunications, and other forms of information related to terrorist activities.[64]

B. *National Cyberspace*

1. China

China's Cybersecurity Law and other internet-related policies are premised on its distinctive philosophy known as "cyberspace sovereignty," which is sometimes referred to as "internet sovereignty," "network sovereignty," or "cyber sovereignty."[65] The law, as indicated in Article 1, aims to protect not only national security but also cyberspace sovereignty.[66] In other words, it views cybersecurity risks

---

60. *Id.*
61. *Id.*
62. *Id.*
63. Zhonghua Renmin Gongheguo Fan Kongbu Zhuyi Fa (中华人民共和国反恐怖主义法) [China's Counterterrorism Law] (promulgated by Standing Comm. Nat'l People's Cong., Dec. 27, 2015, effective Jan. 1, 2016), art. 3 ("This Law shall come into force on January 1, 2016.") (translated by authors) (translation available at https://www.uschina.org/china-hub/unofficial-translation-counter-terrorism-law-peoples-republic-china [https://perma.cc/G8MB-EFW2] (archived Feb. 18, 2022)).
64. China's Counterterrorism Law, art. 25.
65. Lee, *supra* note 6, at 67. *See generally* Yu Hong & G. Thomas Goodnight, *How to Think About Cyber Sovereignty: The Case of China*, 13 CHINESE J. COMM. 8 (2020).
66. China's Cybersecurity Law, art. 1.

as threats to both sovereignty and national security.[67] The country's National Security Law, the first national law codifying the concept of "cyberspace sovereignty,"[68] likewise emphasized that the state should "maintain cyberspace sovereignty" by "strengthening network management, preventing, stopping and lawfully punishing illegal and criminal internet activities, including cyberattacks, network hacking, cybertheft, and dissemination of unlawful and harmful information."[69]

The Chinese government has configured traditional concept sovereignty to the digitally networked environment by using the term "cyberspace sovereignty."[70] Cyberspace sovereignty represents nation-states' autonomy to regulate cyberspace on their territories.[71] Although conventional wisdom views cyberspace as a borderless place,[72] a nation-state can certainly claim sovereignty over its domestic network[73] and the information infrastructure within its borders.[74] This is indeed how the Chinese government puts the idea of cyberspace

---

67. Lee, *supra* note 6, at 67.

68. Guo, *supra* note 5, at 143; Scott J. Shackelford, Danuvasin Charoen, Tristen Waite, & Nancy Zhang, *Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking*, 41 U. PA. J. INT'L L. 377, 402 (2019).

69. Zhonghua Renmin Gongheguo Guojia Anquan Fa (中华人民共和国国家安全法) [China's National Security Law] (promulgated by Standing Comm. Nat'l People's Cong., July 1, 2015, effective July 1, 2015), art. 25 (translation available at https://chinacopyrightandmedia.wordpress.com/2015/07/01/national-security-law-of-the-peoples-republic-of-china/ [https://perma.cc/AP6V-VATN] (archived Feb. 18, 2022)).

70. *See, e.g.*, Hong & Goodnight, *supra* note 65, at 9–10.

71. *See, e.g.*, Zhixiong Huang & Kubo Mačák, *Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches*, 16 CHINESE J. INT'L L. 271, 292–96 (2017); Iasiello, *supra* note 40, at 1; Sarah McKune & Shazeda Ahmed, *The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda*, 12 INT'L J. COMM. 3835, 3837–38 (2018); Min Jiang, *Authoritarian Informationalism: China's Approach to Internet Sovereignty*, 30 SAIS REV. INT'L AFF. 71, 72–73 (2010); Shackelford, Charoen, Waite, & Zhang, *supra* note 68, at 401–05; Wang, *supra* note 23, at 397; *see also* Liudmyla Balke, Comment, *China's New Cybersecurity Law and U.S.-China Cybersecurity Issues*, 58 SANTA CLARA L. REV. 137, 141 (2018) (stating that "China wants to be completely independent from other countries, which largely prompted the idea of cyber sovereignty within the country"); Geoffrey Hoffman, *Cybersecurity Norm-Building and Signaling with China*, *in* GOVERNING CYBERSPACE: BEHAVIOR, POWER AND DIPLOMACY 187, 188 (Dennis Broeders & Bibi van den Berg eds., 2020) (stating that "China argues for its sovereign right to censor").

72. *See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 25–27 (2006); Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 409 (2007); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996).

73. *See, e.g.*, Scott J. Shackelford, Scott Russell, & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1, 11–12 (2016).

74. *See, e.g.*, GOLDSMITH & WU, *supra* note 72, at 68–74, 93–97; Oren Gross, *Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents*, 48 CORNELL INT'L L.J. 481, 499 (2015).

sovereignty into practice.[75] China's notion of cyberspace sovereignty is reaffirmed in its Cybersecurity Law, especially the provision requiring strict data localization.[76]

Moreover, the borderless cyberspace has been an illusion since China successfully implemented a massive internet-filtering system in its internet architecture, which is widely known as the "Great Firewall," that effectively blocks domestic net users from accessing undesirable foreign online content.[77] The Great Firewall, viewed as China's digital borders that define the scope of the country's cyberspace,[78] has functioned as essential infrastructure to facilitate government control of information flow.

2. Vietnam

Unlike China's cyber law, Vietnam's Cybersecurity Law does not accept the idea of cyberspace sovereignty. This idea, however, informed Vietnamese legislative discourse to some extent. For example, the idea of cyberspace sovereignty was included in the draft Law on National Defense[79] but was not adopted in the final text of the law enacted in 2018. However, it accepts the related notion of "national cyberspace," which it defines as the "cyberspace established, managed and

---

75. Lee, *supra* note 6, at 68; *see also* Sean Watts & Theodore Richard, *Baseline Territorial Sovereignty and Cyberspace*, 22 LEWIS & CLARK L. REV. 771, 775 (2018) ("[f]or China...the exercise of sovereignty in cyberspace involves not only efforts to secure the integrity of information and information systems but also to control the flow and character of content accessed on territorial cyber infrastructure.").

76. *See, e.g.*, Jinhe Liu, *China's Data Localization*, 13 CHINESE J. COMM. 84, 97–98 (2020); Pernot-Leplay, *supra* note 24, at 105–06; Shackelford, Russell, & Kuehn, *supra* note 73, at 31–32; Yang Feng, *The Future of China's Personal Data Protection Law: Challenges and Prospects*, 27 ASIA PAC. L. REV. 62, 72 (2019); *see infra* text accompanying notes 112–136; *see also* Sarah McKune & Shazeda Ahmed, *supra* note 71, at 3835 ("Internet sovereignty is defined by state participation or intrusion into wide swathes of online activity—for example, online censorship, penalization of online dissent, or data localization requirements for foreign companies."); Roxana Vatanparast, *Data Governance and the Elasticity of Sovereignty*, 46 BROOK. J. INT'L L. 1, 29 (2020) (describing data localization as the "starkest example" of cyber sovereignty).

77. *See, e.g.*, Jiang, *supra* note 71, at 75; Jyh-An Lee, *Great Firewall*, *in* THE SAGE ENCYCLOPEDIA OF THE INTERNET 406, 406–08 (Barney Warf ed., 2018); Lee & Liu, *supra* note 27, at 129–35; Lee, Lui & Li, *supra* note 23, 424–26.

78. *See, e.g.*, Bang Xiao, *The Complexities of Cyber Sovereignty in Chinese Airlines over Australian Skies*, ABC NEWS (Sept. 7, 2018), https://www.abc.net.au/news/2018-09-08/i-confronted-the-great-firewall-of-china-in-australian-airspace/10159900 [https://perma.cc/ELT3-795J] (archived Feb. 14, 2022).

79. *Khái Niệm "Chủ Quyền Quốc Gia Trên Không Gian Mạng" Và Ý Thức Hệ Của Dân Tộc* [The Concept Of "National Sovereignty On Cyberspace" And The Ideology Of The Nation], CAO ĐẲNG NGHỀ Số 1 BỘ QUỐC PHÒNG (Nov. 28, 2018) (Viet.), http://Truong1bqp.Edu.Vn/Khai-Niem-Chu-Quyen-Quoc-Gia-Tren-Khong-Gian-Mang-Va-Y-Thuc-He-Cua-Dan-Toc/ [https://perma.cc/KQ9P-PXNJ] (archived Feb. 16, 2022).

controlled by the Government."[80] The law further provides that "the State applies measures to protect national cyberspace." [81] The government's strict regulation of cyber activities within its territory and data-localization requirements (discussed below) exemplify the notion of national cyberspace. In practice, unlike China, Vietnam does not have an internet architecture that blocks foreign online content like the Great Firewall, nor does it have national alternatives to international platforms. Tech giants like Google, YouTube, and Facebook are popular in Vietnam. This indicates that the notion of national cyberspace may facilitate national regulation of the internet but does not assume that the internet is under the jurisdiction of Vietnamese sovereignty.

C. *Major Legal Issues*

1. Prohibited Acts

a. China

China's Cybersecurity Law forbids a long list of behaviors, that might endanger cybersecurity, such as "illegally intruding into any other person's network" and "interfering with the normal functions of any other person's network."[82] Moreover, whoever knows that another person is conducting an activity endangering cybersecurity is prohibited from "providing technical support, advertising promotion, payment and settlement services or any other assistance to such a person."[83] The law also forbids the provision of information or other support online of illegal or criminal activity.[84]

Foreign businesses have expressed significant concerns over the law's vague language. [85] In fact, the language used in Chinese legislation has largely been characterized as being general and ambiguous.[86] The justification of such a legislative approach is to

---

80. Law on Cybersecurity, 2018 (No. 24/2018/QH14) (Viet.), art. 2.
81. *Id.* art. 6.
82. China's Cybersecurity Law, art. 12.
83. *Id.* art. 27.
84. *Id.* art. 46.
85. *See, e.g.*, Lee, *supra* note 6, at 61–62; He, *supra* note 1; Lauren Maranto, *Who Benefits from China's Cybersecurity Laws?*, CTR. FOR STRATEGIC & INT'L STUD. (June 25, 2020), https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cyber security-laws [https://perma.cc/KVQ6-NHJ3] (archived Feb. 14, 2022).
86. *See, e.g.*, DEBORAH CAO, CHINESE LAW: A LANGUAGE PERSPECTIVE 94–96 (2016); RANDALL P. PEERENBOOM, CHINA'S LONG MARCH TOWARD RULE OF LAW 247, 251 (2002); Randall Peerenboom, *The X-Files: Past and Present Portrayals of China's Alien "Legal System,"* 2 WASH. U. GLOB. STUD. L. REV. 37, 81 (2003); Lindsay Wilson, Note,

intentionally provide flexibility with a view to respond to local conditions[87] or unexpected societal developments.[88] To implement the law, administrative authorities have to make more detailed administrative rules.[89] The Cybersecurity Law is no exception.[90] Nonetheless, like some other Chinese legislation, the law's ambiguity has created great uncertainty for the industry, which must worry that the law may be enforced in opaque, discriminatory ways.[91]

b. Vietnam

Like China's Cybersecurity Law, Vietnam's Cybersecurity Law provides a lavish list of prohibitions. It bans using cyberspace to conduct the following acts that cause harm to national security:

- organizing, activating, colluding, instigating, bribing, cheating or tricking, manipulating, training, or drilling people to oppose the State of the Socialist Republic of Vietnam;
- distorting history, denying revolutionary achievements, destroying the national solidarity block, conducting offenses against religion, gender discrimination, or racist acts;
- providing false information, causing confusion among the citizens, causing harm to socioeconomic activities, causing difficulties for the operation of state agencies or of people performing public duties, or infringing the lawful rights and interests of other agencies, organizations and individuals;
- activities such as prostitution, social evils, or human trafficking;
- publishing information which is lewd, depraved, or criminal;
- destroying the fine traditions and customs of the people, social ethics, or health of the community;
- and inciting, enticing, or activating other people to commit crime.[92]

Investors Beware: The WTO Will Not Cure All Ills with China, 2003 COLUM. BUS. L. REV. 1007, 1017 (2003).

87. *See, e.g.*, Perry Keller, *Sources of Order in Chinese Law*, 42 AM. J. COMP. L. 711, 749 (1994).

88. *See, e.g.*, Balke, *supra* note 71, at 153; Ruth Jebe, Don Mayer, & Yong-Shik Lee, *China's Export Restrictions of Raw Materials and Rare Earths: A New Balance Between Free Trade and Environmental Protection?*, 44 GEO. WASH. INT'L L. REV. 579, 630 (2012). *But see* Claudia Ross & Lester Ross, *Language and Law: Sources of Systemic Vagueness and Ambiguous Authority in Chinese Statutory Language*, 31 U. BRIT. COLUM. L. REV. 205, 209 (1997) (attributing the vagueness to the Chinese legislators' incapacity and inexperience in law drafting).

89. *See* Jebe, Mayer, & Lee, *supra* note 88, at 630.

90. Quinn, *supra* note 8, at 419.

91. Lee, *supra* note 6, at 61–62.

92. Law on Cybersecurity, 2018 (No. 24/2018/QH14) (Viet.), art. 8.

In addition, Vietnam's Cybersecurity Law prohibits acts causing harm to the information system critical for national security, including the following:

- conducting a cyberattack, cyberterrorism, cyberespionage, or cybercrime; causing a cybersecurity incident;
- attacking, infringing, or hijacking operational control of, or distorting, interrupting, stalling, paralyzing, or destroying an information system critical to national security;
- producing or putting into use tools, facilities, or software or otherwise committing an act to obstruct or disrupt the operation of a telecom network, the internet, computer network, information system, information processing and control system, or e-facility;
- distributing an informatics program that harms the operation of a telecom network, the internet, computer network, information system, information processing and control system, database, or e-facility;
- illegally accessing a telecom network, the internet, computer network, information system, information processing and control system, database, or e-facility of another person;
- opposing or obstructing the activities of a Cybersecurity Task Force;
- illegally attacking, neutralizing, disabling, or rendering ineffective any cybersecurity protective measures.[93]

The law employs ambiguous language (e.g., causing confusion among citizens, causing harm to socioeconomic activities, and destroying the fine traditions and customs of the people) to ban acts in cyberspace. The functions of this ambiguous language are twofold. First, it creates wide discretionary space for the authorities to enjoy the power to interpret vague clauses on banned acts. Second, the Delphic provisions on prohibited acts in cyberspace encourage self-censorship. As the language is ambiguous, netizens do not know the exact boundaries of permissible actions and lack a clear idea of when they will be punished. This uncertainty generated by the ambiguous language around banned acts may encourage Vietnamese netizens to self-censor for their safety.

93. *Id.*

2. Network Operators

a. China

Like those in many other jurisdictions, internet intermediaries have been the main targets of internet regulations in China. [94] Therefore, it is unsurprising that the country's Cybersecurity Law imposes significant obligations on network operators and network service and product providers.[95] Network operators' primary security obligations include:

- developing internal security management rules and operating procedures, determining the persons in charge of cybersecurity, and carrying out the responsibility for cybersecurity protection;
- taking technical measures to prevent computer viruses, network attack, network intrusion, and other acts endangering cybersecurity;
- taking technical measures to monitor and record the status of network operation and cybersecurity incidents, and preserving relevant weblogs for not less than six months as required;
- taking measures such as data categorization, and back-up and encryption of important data; and
- performing other obligations as prescribed by laws and administrative regulations.[96]

When discovering any risk, such as security defects and vulnerabilities in their network products and services, network providers are obliged to take immediate remedial measures, inform users in a timely manner, and report it to the competent department in accordance with relevant provisions.[97] Moreover, the law requires network operators to "develop emergency response plans to react to cybersecurity incidents," and "in the event of an incident," those operators must "promptly implement remediation measures and report incidents to the relevant authorities."[98]

---

94. *See, e.g.*, Lee & Liu, *supra* note 27, at 148–49.
95. Lee, *supra* note 6, at 70.
96. China's Cybersecurity Law, art. 21.
97. *Id.* art. 22.
98. *Id.* art. 25.

b. Vietnam

In the same vein, Vietnam's Cybersecurity Law requires service providers to:

- warn of the possibility of a loss of cybersecurity during the use of the services in cyberspace provided by such enterprises and to provide guidelines on preventive measures;
- formulate plans and solutions to quickly respond to cybersecurity incidents and immediately handle any security weaknesses or vulnerabilities, malicious codes, cyberattacks, cyber intrusions/infringements, and other security risks; and when a cybersecurity incident occurs, to immediately implement appropriate emergency plans and response measures and provide a report thereof to the Cybersecurity Task Force (CTF);
- apply technical solutions and other necessary measures to ensure security while collecting information and to prevent the risk of revelation, damage to, or loss of data; and in the case of occurrence or possible occurrence of the revelation, damage to, or loss of data about user information, to immediately provide response solutions, notify users, and report to the CTF; and
- coordinate with and facilitate CTFs to conduct their cybersecurity protective activities.[99]

3. Critical Infrastructure

a. China

The threat to critical infrastructure is a major cybersecurity concern in many countries.[100] The Chinese Cybersecurity Law defines "critical information infrastructure" as that which, "if destroyed, rendered dysfunctional, or leaked, might seriously endanger national security, national welfare and the people's livelihood, or the public interest."[101] Pursuant to the Cybersecurity Law, the State Council published the "Regulations on the Security Protection of Critical Information Infrastructure" (the CII Regulations) on August 17,

---

99. Law on Cybersecurity, 2018 (No. 24/2018/QH14) (Viet.), art. 41.

100. *See, e.g.*, John J. Chung, *Critical Infrastructure, Cybersecurity, and Market Failure*, 96 OR. L. REV. 441, 444–52 (2018); Kevin Quigley, Calvin Burns, & Kristen Stallard, *'Cyber Gurus': A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection*, 32 GOV'T INFO. Q. 108, 114–15 (2015).

101. China's Cybersecurity Law, art. 31.

2021.[102] While the Cybersecurity Law provides a non-exhaustive list of critical information infrastructure, including "public communication and information services, energy, transportation, water conservation, banking and finance, public services, and electronicgovernment,"[103] the CII Regulations add "national defense science, technology, and industry" as an additional type of critical information infrastructure.[104]

Other than a network operator's obligations, mentioned above, a critical information infrastructure operator is subject to additional obligations. The CII Regulations provide the general obligation of the critical information infrastructure operator is to "adopt technical protection measures and other necessary measures to respond to cybersecurity incidents and prevent cyber-attacks . . . and ensure the safe and stable operation of critical information infrastructure, and maintain the integrity, confidentiality and availability of data."[105] Both the Cybersecurity Law and the CII Regulations mandate that critical information infrastructure operators must "conduct a security background review on responsible personnel in key positions," "conduct cybersecurity education [and] technical training," and implement "disaster recovery backups."[106]

b. Vietnam

Similarly, the protection of "critical information systems" is an essential issue in the Vietnamese Cybersecurity Law, which defines "critical information systems" as information systems that, if subject to an incident, infiltration, hijacking of operational control, distortion, interruption, stoppage, paralysis, attack, or destruction, would seriously compromise network security. [107] The Vietnamese

---

102. Guanjian Xinxi Jichusheshi Anquanbaohu Tiaoli (关键信息基础设施安全保护条例) [Regulations on the Security Protection of Critical Information Infrastructure], (promulgated by the State Council, Apr. 27, 2021, effective on Sept. 1, 2021) [hereinafter CII Regulations].

103. China's Cybersecurity Law, art. 31.

104. CII Regulations, art. 2.

105. *Id.* art. 6.

106. China's Cybersecurity Law, art. 34 ("In addition to the provisions of Article 21 of this Law, the operators of key information infrastructures shall also fulfill the following security and protection obligations: (1) set up a special safety management agency and the person in charge of safety management, and conduct a security background review on responsible personnel in key positions; [(2)] [r]egularly conduct cybersecurity education, technical training and skills assessment for practitioners; (3) disaster recovery backup of important systems and databases; [(4)] develop [] contingency plans for network security incidents, and regular exercise; [(E)] [o]ther obligations as prescribed by laws and administrative regulations."); CII Regulations, art. 39 (stipulating the same obligations with accompanying liability for violation).

107. *See* Law on Cybersecurity, 2018 (No. 24/2018/QH14) (Viet.), art. 41.

Cybersecurity Law provides a broad list of critical information systems, including information systems in the areas of military, diplomacy, and cipher, state secrets, physical facilities relevant to national security, energy, finance, banking, telecommunications, transport, natural resources and the environment, chemicals, medical health, culture, and the press, among others.[108] The law authorizes the prime minister to issue, amend, and supplement a list of information systems critical to national security.[109]

The Vietnamese Cybersecurity Law has detailed provisions that allow various authorities (e.g., the Ministry of Public Security, the Ministry of National Defense, the Ministry of Information and Communications, and the Government Cipher Committee) to evaluate, inspect, supervise, and remedy incidents of information systems critical to national security under government coordination.[110] The law also imposes significant obligations on the operators of critical information systems: they must conduct cybersecurity inspections of the systems and provide written notices of their inspection results to the relevant authorities; formulate mechanisms for automatic warnings and receipt of such warnings of any cybersecurity threats, cybersecurity incidents, weaknesses or security vulnerabilities, and malicious codes or malicious hardware to provide plans on emergency response and remedy; and formulate a plan on responding to and remedying any cybersecurity incident in their systems. [111]

4. Data Localization

Data localization, which requires certain data to be stored and processed within the boundaries of the state, has been an important feature of the cybersecurity laws in both China and Vietnam.

a. China

Article 37, arguably "the most controversial provision" of China's Cybersecurity Law, [112] provides that "[c]ritical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China." [113] If a critical information infrastructure operator has a

108. *See id.*
109. *See id.*
110. *See generally id.* arts. 10–15.
111. *See id.* arts. 13–15.
112. Gabriela Kennedy & Xiaoyan Zhang, *China Passes Cybersecurity Law*, 29 INTELL. PROP. & TECH. L.J. 20, 20 (2017).
113. China's Cybersecurity Law, art. 37.

business need to transfer such information or data abroad, a security assessment and approval from the relevant government authority is compulsory.[114]

China's data localization policy is further advanced in the recently enacted Data Security Law and the Personal Information Protection Law (PIPL). The Data Security Law, governing the transfer of non-personal data, declares that relevant government authorities will release regulations governing cross-border transfers of data by data processors other than critical information infrastructure operators.[115] PIPL sets an even higher threshold for the transfer of personal information, obligating the data processor to comply with at least one of the below requirements:

- passing the security assessment organized by the state cyberspace administration;
- being certified by a specialized institute in accordance with the provisions of the State cyberspace administration in respect of the protection of personal information;
- concluding a contract with an overseas recipient according to the standard contract formulated by the state cyberspace administration, specifying the rights and obligations of both parties; or
- meeting other requirements prescribed by laws, administrative regulations, or the State cyberspace administration.[116]

The data localization requirement is unwelcome to most foreign businesses in China. [117] To comply with data localization rules, multinational enterprises have been forced to build local data centers

---

114. *See id.* art. 31.

115. *See* Zhonghua Renmin Gongheguo Shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law] (promulgated by Standing Comm. Nat'l People's Cong., Jun. 10, 2021, effective Sept. 1, 2020), art. 31, http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml [https://perma.cc/YSJ9-G59S] (archived Feb. 11, 2022).

116. Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law] [hereinafter "PIPL"] (promulgated by Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) art. 38(1)–(4), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml [https://perma.cc/MM5B-ZRKE] (archived Feb. 11, 2022).

117. *See, e.g.*, Wang, *supra* note 23, at 408 (stating that "many foreign companies left China due to strict data localization regulations").

in China or store their data in other local data centers.[118] The restructuring or reconfiguration of their information technology infrastructure certainly leads to hefty costs.[119] Moreover, while the purpose of data localization is to enhance the level of cybersecurity,[120] its outcome is an ironically higher risk of data leaks and government censorship and surveillance.[121] From a technological perspective, storing data in data centers in multiple jurisdictions might be a cybersecurity strategy for businesses.[122]

To address these concerns, the Chinese government has elucidated that data localization is compatible with its globalization strategy under the One Belt One Road initiative,[123] aiming to make China a leading power through the economic integration of its

---

118. *See, e.g.*, Keeton Christian, Note, *The Fortification of the Great Firewall and Its Effect on E-Discovery Disputes in U.S. Courts*, 82 U. PITT. L. REV. 173, 197 (2020); Jie (Jeanne) Huang, *Personal Jurisdiction Based on the Location of a Server: Chinese Territorialism in the Internet Era?*, 36 WIS. INT'L L.J. 87, 111 (2018); *see also* Wentong Zheng, *The Digital Challenge to International Trade Law*, 52 N.Y.U. J. INT'L L. & POL. 539, 552 (2020) (claiming that "data localization measures dramatically alter the fundamental architecture of the Internet by forcing businesses to make data decisions based not on efficiency, but on territorial boundaries").

119. *See, e.g.*, Alexander Savelyev, *Russia's New Personal Data Localization Regulations: A Step Forward or A Self-Imposed Sanction?*, 32 COMPUTER L. & SEC. REV. 128, 141 (2016); *see also* Shelli Gimelstein, *A Location-Based Test for Jurisdiction Over Data: The Consequences for Global Online Privacy*, U. ILL. J.L. TECH. & POL'Y 1, 28 (2018) ("data localization laws . . . force ISPs to build costly data storage centers and maintain in-country copies of user data, making it far more expensive and inefficient to operate abroad. Smaller companies may be unable to bear such costs and will either increase prices for their services or exit these markets, denying consumers access to innovative services. Companies may avoid selling their products in countries with data localization laws—even in large countries with a huge consumer base.").

120. *See, e.g.*, Vatanparast, *supra* note 76, at 17.

121. *See, e.g.*, OFFICE OF THE U.S. TRADE REPRESENTATIVE, FINDINGS OF THE INVESTIGATION INTO CHINA'S ACTS, POLICIES AND PRACTICES RELATED TO TECHNOLOGY TRANSFER, INTELLECTUAL PROPERTY, AND INNOVATION UNDER SECTION 301 OF THE TRADE ACT OF 1974 at 178 (Mar. 22, 2018), https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF [https://perma.cc/LFH5-EYW6] (archived Feb. 11, 2022); Yu-Jie Chen, Ching-Fu Lin, & Han-Wei Liu, *"Rule of Trust": The Power and Perils of China's Social Credit Megaproject*, 32 COLUM. J. ASIAN L. 1, 26–27 (2018); Jordan A. Klumpp, *International Impact of the Clarifying Lawful Overseas Use of Data (CLOUD) Act and Suggested Amendments to Improve Foreign Relations*, 48 GA. J. INT'L & COMP. L. 613, 628 (2020); Gimelstein, *supra* note 119, at 29.

122. *See, e.g.*, Jennifer Daskal, Paul Ohm, & Pierre de Vries, *Debate: We Need to Protect Strong National Borders on the Internet*, 17 COLO. TECH. L.J. 13, 27 (2018); Huang, *supra* note 118, at 111; *see also* Kimberly A. Houser & Anjanette H. Raymond, *It Is Time to Move Beyond the 'AI Race' Narrative: Why Investment and International Cooperation Must Win the Day*, 18 NW. J. TECH. & INTELL. PROP. 129, 144 (2021) (indicating that "China's data localization requirement...does have the effect of making Chinese data more secure vis-a-vis foreign bad actors").

123. *See* Sacks, *supra* note 5.

continental and maritime regions.[124] Moreover, although economic studies indicated that data localization policies are harmful to the overall economy,[125] some believe that data localization policy can benefit local data industry and therefore promote economic development.[126] China's data center industry has indeed grown significantly in recent years.[127]

b. Vietnam

A controversial provision in Vietnam's Cybersecurity Law is clause 3 of Article 26, which requires that foreign service providers in Vietnam store local personal data on users in Vietnam for a specified period to be provided by the government and must have branches or representative offices in the country.[128] During the law-making process, this provision was subject to contentious debates among Vietnamese legislators.[129] Supporters of the provision believed that it was necessary to protect national sovereignty.[130] Its opponents, however, questioned the provision's enforceability. For example, deputy of the National Assembly Cao Đình Thưởng wondered, "When we have made this regulation, but foreign businesses, such as Google or Facebook, do not implement, what is our solution here? Whether to stop providing services in the territory of Vietnam? Therefore, it is necessary to have regulations in accordance with Vietnam's reality and current relationships as well as Vietnam's commitments to foreign countries and international law."[131] Another deputy of the National Assembly, Phạm Thị Thanh Thủy, had a similar concern: "If foreign businesses do not comply with this regulation, they may not be allowed to provide services in Vietnam, and this will greatly affect the people's access to information and service use, especially in the context that our

124. *See, e.g.*, Jyh-An Lee, *The New Silk Road to Global IP Landscape*, *in* LEGAL DIMENSIONS OF CHINA'S BELT AND ROAD INITIATIVE 417, 417 (Lutz-Christian Wolff & Chao Xi eds., 2016).

125. *See, e.g.*, Huang, *supra* note 118, at 111.

126. *See, e.g.*, Wang, *supra* note 23, at 411–12; *see also* Pernot-Leplay, *supra* note 24, at 105 (explaining that one of the rationales in legislating data localization requirement is to advance China's economic development).

127. *See, e.g.*, Liu, *supra* note 76, at 91.

128. *See* Law on Cybersecurity, 2018 (No. 24/2018/QH14) (Viet.), art. 26.

129. *See* Tranh cãi về quy định Facebook, Google phải đặt văn phòng tại Việt Nam [Controversy over regulations that Facebook and Google must set up offices in Vietnam], VIETNAMBIZ (May 30, 2018), https://vietnambiz.vn/tranh-cai-ve-quy-dinh-facebook-google-phai-dat-van-phong-tai-viet-nam-55204.htm [https://perma.cc/UV69-KTRQ] (archived Feb. 8, 2022).

130. *See id.*

131. *Id.*

country does not have any brand name to meet the needs of people to access information and use services."[132]

Domestic critics believed that the requirement of data localization would impede economic development in Vietnam. For example, prior to the law's enactment, the Vietnam Digital Communications Association sent a letter to the relevant authority warning that the requirement of data localization would reduce gross domestic product growth by 1.7 percent and reduce foreign investment in Vietnam by 3.1 percent.[133] The letter suggested that the clauses on data localization should be abolished because they "will negatively impact economic development through limiting international data exchange, increasing costs and reducing the ability to take advantage of domestic enterprises' technological development. Although the direct costs to enforce this regulation may fall into the group of foreign firms, the indirect costs will be distributed over the entire business and economy of Vietnam. Moreover, this [requirement of data localization] has the potential to affect the business investment environment, reduce the investment attraction for foreign enterprises in Vietnam, and potentially violate international commitments [of which] Vietnam is a member."[134]

In response, the Ministry of Public Security, which was the relevant authority responsible for proposing the law, provided four justifications for the data localization requirement in Vietnam's Cybersecurity Law.[135] First, the ministry argued that it was consistent with international practices, citing the same requirements in more than eighteen countries, including the United States, Canada, the Russian Federation, Germany, China, Indonesia, Greece, Bulgaria, Denmark, Finland, Sweden, Turkey, Venezuela, Colombia, Argentina, and Brazil.[136]

Second, the ministry claimed that it was practicably possible for foreign enterprises to comply with the clause on data localization in

---

132. *Id.*

133. *See* Hội Truyền thông số Việt Nam gửi kiến nghị 4 điểm về dự thảo Luật An ninh mạng [The Vietnam Digital Media Association Sends a 4-Point Recommendation on the Draft Law on Cyber Security], VIET. DIGIT. MEDIA ASS'N (June 19, 2018), http://vdca.org.vn/tin-tuc/t273/hoi-truyen-thong-so-viet-nam-gui-kien-nghi-4-diem-ve-du-thao-luat-an-ninh-mang.html [https://perma.cc/F53G-R3HG] (archived Feb. 8, 2022).

134. *Id.*

135. *See* Bộ Công an nêu 4 lý do về quy định lưu trữ dữ liệu, đặt chi nhánh tại Việt Nam trong Luật An ninh mạng là phù hợp [The Ministry of Public Security Stated 4 Reasons That Regulations on Data Storage and Branching in Vietnam in the Law on Cyber Security Are Appropriate], TO QUOC (Nov. 3, 2018), http://toquoc.vn/bo-cong-an-neu-4-ly-do-ve-quy-dinh-luu-tru-du-lieu-dat-chi-nhanh-tai-viet-nam-trong-luat-an-ninh-mang-la-phu-hop-20181103202709478.htm [https://perma.cc/RB5Q-RVPV] (archived Feb. 8, 2022).

136. *See id.*

Vietnam because they did the same elsewhere.[137] Google has about seventy representative offices and Facebook about eighty representative offices in countries around the world.[138] In Southeast Asia, Google and Facebook have opened representative offices in Singapore, Malaysia, and Indonesia.[139]

Third, the clause was consistent with Vietnamese domestic laws, including the 2005 Commercial Law and the 2017 Foreign Trade Management Law, which require foreign trade promotion organizations to establish representative offices in Vietnam.[140] Cross-border service providers, such as Facebook and Google, have profitable business activities in Vietnam and therefore must be under the scope of these domestic laws.[141]

Fourth, the clauses were not contrary to international commitments, including related treaties that Vietnam had signed.[142] Vietnamese legal authority attached to international and comparative law and practices to legitimize the Cybersecurity Law's requirement of data localization. The adherence to international and foreign sources of law is also to counter international and local criticism and seek wider support for the law, which was necessary for its implementation.

5. Security Evaluation, Assessment, Inspection, and Supervision

a. China

The Chinese Cybersecurity Law provides detailed rules governing security certification, inspection, and review. Article 23 requires that "critical network equipment and specialized network security products shall follow national standards and mandatory requirements," with security levels "certified by a qualified institute or confirmed by security inspection."[143] The same article stipulates that the "state's network information departments, together with the relevant departments of the State Council, shall formulate and release a catalog of critical network equipment and specialized network security products as well as promote the reciprocal recognition of security certifications and security inspection results to avoid duplicate certifications and inspections."[144]

---

137. *See id.*
138. *See id.*
139. *See id.*
140. *See id.*
141. *See id.*
142. *See id.*
143. China's Cybersecurity Law, art. 23.
144. *Id.*

Under Article 35, "the network products and services purchased by critical information infrastructure operators that might affect national security are required to undergo a national security review by the State Cyberspace Administration departments and other relevant departments of the State Council."[145] To implement Article 35, the Chinese government released the Cybersecurity Review Measures on April 13, 2020, which came into effect on June 1, 2020.[146] These measures provide that when purchasing network products or services, a critical information operator shall assess the potential national security risks resulting from the use of such products or services.[147] The critical information operator is obliged to report to the Cybersecurity Review Office for cybersecurity reviews if the use of such products or services may lead to any national security risk.[148] During the cybersecurity review, the Cybersecurity Review Office will primarily consider:

- the risk of critical information infrastructure being illegally controlled, interfered with, or destroyed after that the product or service is put into use, as well as the risk of important data being stolen, leaked, or harmed;
- the threat to the continuity of critical information infrastructure from interruptions in the supply of the products or services;
- the products' or services' security, openness, transparency, and diversity of sources, as the reliability of supply channels and the risk of supply interruptions due [to] political, diplomatic, or trade factors, and so forth;
- the supplier of the product or services' compliance with Chinese law, administrative regulations, and departmental rules; and
- other factors that might endanger critical information infrastructure security and national security.[149]

The main criticism of Articles 23, 35, and related regulations is that they may be used as political tools to prevent companies that are defined as critical infrastructure from fairly competing with others favored by the government.[150] Foreign business also worried that they will be forced to disclose their trade secrets in the cybersecurity review

145. *Id.* art. 35.

146. *See generally* Cybersecurity Review Measures [网络安全审查办法], (promulgated by Cyberspace Administration of China (CAC) and other relevant authorities) (April 13, 2020).

147. *See id.* art. 5.

148. *See id.*

149. *Id.* art. 9.

150. *See* Lee, *supra* note 6, at 85.

and inspection process.[151] Moreover, these regulations may be part of the government intervention to develop a domestic cybersecurity industry and protect it from international competition.[152]

b. Vietnam

In the same vein, Vietnam's Cybersecurity Law imposes a complicated regime of security evaluation, assessment, inspection, and supervision.

Under Article 11, evaluation items include compliance with regulations and conditions for cybersecurity and conformity with plans for protection from, response to, and remedying of any incident as well as the deployment of human resources to protect cybersecurity.[153] According to Article 12, information systems critical to national security must satisfy the following conditions:

- regulations, procedures, and plans on ensuring cybersecurity;
- personnel operating and administering the system;
- ensuring cybersecurity of equipment, hardware, and software system components;
- technical measures for supervising and protecting cybersecurity;
- protective measures for automatic control and monitoring systems, the internet of things, complex virtual reality systems, cloud computing, large data systems, fast data systems, and artificial intelligence systems;
- and measures ensuring physical security comprising special isolation, data leakage prevention, prevention of information collection, and access control.[154]

Article 13 provides that a cybersecurity inspection shall be conducted when introducing e-facilities and network information security services for use in an information system and when there is a change in the current status of an information system. Article 13 also provides for regular, annual inspections and one-off inspections in response to cybersecurity breakdowns or infringements of network security.[155] Items to be inspected include hardware and software

151. *See* OFFICE OF THE U.S. TRADE REPRESENTATIVE, *supra* note 121, at 43; *see also* OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2021 SPECIAL 301 REPORT (April 2021) 48, https://ustr.gov/sites/default/files/files/reports/2021/2021%20Special%20301%20Report%20(final).pdf [https://perma.cc/L97E-BJJV] (archived Feb. 8, 2022) (claiming that Cybersecurity and other relevant regulations have been used to force foreign businesses to "disclose sensitive IP to the government, transfer it to a Chinese entity, or restrict market access").

152. *See* Lee, *supra* note 6, at 86.

153. *See* Law on Cybersecurity, 2018 (No. 24/2018/QH14) (Viet.), art. 11.

154. *Id.* art. 12(2).

155. *Id.* art. 13(2).

systems and digital devices used in an information system; regulations and measures on protecting network security; information stored, processed, and transmitted on an information system; plans of a system administrator to respond to and remedy any cybersecurity incident; measures for protecting state secrets and for preventing revelation or loss of state secrets via technical channels; and cybersecurity protective human resources.[156]

Article 14 defines cybersecurity supervision to include "activities of collecting and analyzing the current status to identify cybersecurity threats, cybersecurity incidents, any weaknesses or security vulnerabilities, malicious codes and malicious hardware in order to provide warnings thereof and remedy and deal with [such issues]."[157]

The law empowers the CTF under the Ministry of Public Security to evaluate, inspect, and supervise the cybersecurity of information systems critical to national security, except for military information systems managed by the Ministry of National Defense and for cipher information systems under the Government Cipher Committee.[158] The CTF "shall supervise cybersecurity of information systems critical for national security within its managerial scope; and shall provide warnings and coordinate with the system administrator to remedy and deal with any cybersecurity threat, cybersecurity incident, weakness or security vulnerability, malicious code or malicious hardware in respect of the information system critical for national security."[159]

6. Personal Data Regime

a. China

The Cybersecurity Law sets the basic regulatory framework for privacy protection in China.[160] While China passed the PIPL in 2021 to provide more detailed rules in personal data protection,[161] the 2021 law basically follows the general principles set forth in the Cybersecurity Law. The Cybersecurity Law defines "personal

156. *Id.* art. 13(3).

157. *Id.* art. 14(1).

158. *See generally id.* arts. 11–13.

159. *Id.* art. 14(3).

160. *See* Lee, *supra* note 6, at 87; *see also* Fan Yang & Jian Xu, *Privacy Concerns in China's Smart City Campaign: The Deficit of China's Cybersecurity Law*, 5 ASIA PAC. POL'Y STUD. 533, 539 (2018) ("Cybersecurity Law expands the scope of personal information protection from 'users' to 'individuals', illustrating the extensiveness of Cybersecurity Law"); Pernot-Leplay, *supra* note 24, at 73 (describing Cybersecurity Law as the "most important milestone in China's data protection legal landscape").

161. *See generally* Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law] (promulgated by Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021).

information" as "information that can be used on its own or in conjunction with other information to determine the identity of a natural person, including but not limited to a person's name, birthday, identity card number, biological identification information, address, and telephone number."[162] Based on this definition, the PIPL similarly defines "personal information" as "information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously."[163]

The Cybersecurity Law imposes many privacy obligations on network operators. Network operators' collection and use of personal information must be legal, proper, and necessary.[164] This basic principle is reiterated in the PIPL.[165] Moreover, the Cybersecurity Law states that network operators must also "disclose the purpose, methods, and scope of their data collection and obtain the consent of the persons whose information is collected."[166] This principle of disclosure and consent is further expanded as the data processor's obligation in the PIPL.[167] The Cybersecurity Law provides data subjects the right to request network operators to modify and delete their personal information if they "discover that network operators have violated laws, administrative regulations, or agreements between the parties to gather or use their personal information."[168] The PIPL further provides that data subjects have such a right as to all data processors and the circumstances under which data processors should proactively delete personal information.[169] In the event of a data breach or potential data breach, the Cybersecurity Law obliges network operators to "take remedial action, promptly inform users, and report to the competent authorities."[170] Based on this principle, the PIPL provides more detailed remedial procedures for data processors to follow when "personal information has been or may be leaked, falsified, or lost."[171]

The Cybersecurity Law represents a puzzle for privacy protection in China. On the one hand, it provides citizens with unprecedented protection of their data privacy. On the other hand, it generates significant privacy risks by legalizing the government's access to personal information held by network operators without much

162. China's Cybersecurity Law, art. 76(5).
163. PIPL, art. 4(1).
164. *See* China's Cybersecurity Law, art. 41.
165. PIPL, art. 5.
166. China's Cybersecurity Law, art. 42.
167. *See generally* PIPL, arts. 13–14.
168. China's Cybersecurity Law, art. 43.
169. *See* PIPL, arts. 46–47.
170. China's Cybersecurity Law, art. 42.
171. PIPL, art. 57.

restriction.[172] For example, the law demands network operators "to provide technical support and assistance to public security authorities and state security authorities for the purposes of lawfully upholding national security and investigating crimes."[173] In addition, the law introduces real-name registration policies,[174] mandating network operators to require users to disclose their true identity information.[175] Although the government explained that the real-name registration rule is designed to ensure cybersecurity and a healthier internet,[176] some commentators have expressed concerns that such a rule may be used to eliminate online speech against the government or its officials.[177] Furthermore, the implementation of real-name registration rules may lead to a higher level of privacy risk because the more personal data that is collected by network operators, the more likely these operators will become the targets of hackers interested in misappropriating personal data.[178] Nevertheless, it is noteworthy that the PIPL has imposed limited restrictions on the government's ability to process personal information.[179] Although these restrictions do not affect the possible surveillance and censorship entailed by the Cybersecurity Law, the PIPL has signaled the government's minimum duty of care in handling personal data.

b. Vietnam

Similarly, Vietnam issued several legal rules for personal data protection before the enactment of the Cybersecurity Law. The 2013 Constitution includes a new provision on privacy protection that states: "Everyone is entitled to the inviolability of personal privacy, personal secrecy and familial secrecy and has the right to protect his or her honor and prestige. Information regarding personal privacy, personal secrecy and familial secrecy is safely protected by the law."[180]

The constitutional right to privacy has been the basis of subsequent laws. The Network Information Security Law, for instance, bans the "illegal collection, use, dissemination of or trading in personal

---

172. *See, e.g.*, Pernot-Leplay, *supra* note 24, at 106; *see also* Qiang, *supra* note 27, at 55, 60.

173. China's Cybersecurity Law, art. 28.

174. *See* Lee & Liu, *supra* note 23, at 11–15.

175. *See* China's Cybersecurity Law, art. 24.

176. *See* Lee & Liu, *supra* note 23, at 15–16

177. *See id.* at 16.

178. *Id.* at 18–19; *see also* Quinn, *supra* note 8, at 430.

179. *See* Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law], arts. 33–35, (promulgated by Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021).

180. CONSTITUTION OF VIETNAM art. 21.

information of others; [and the] exploitation of a weakness point of an information system to collect and exploit personal information."[181]

According to the Cybersecurity Law, acts infringing on personal secrets, family secrets, or private life in cyberspace include the following:

- appropriating, buying, selling, seizing, and/or intentionally disclosing information classified as personal secrets, family secrets, or private life;
- deliberately deleting, damaging, misplacing, and/or changing information classified as personal secrets, family secrets, or private life;
- deliberately altering, cancelling, or invalidating technical measures that have been constructed and/or applied to protect information classified as personal secrets, family secrets, or private life;
- putting in cyberspace information classified as personal secrets, family secrets, or private life; and
- deliberately listening to or recording in sound or images conversations contrary to law.[182]

The Cybersecurity Law requires information system owners to apply managerial and technical measures to prevent, detect, and block any acts infringing on personal secrets, family secrets, or private life on the information system, promptly remove any information related to such conduct, and coordinate with and implement requests made by the CTF regarding the protection of information classified as personal secrets, family secrets, or private life on the information system.[183]

The Cybersecurity Law also imposes legal obligations on network operators, which are instrumental to personal data protection. However, if the relevant authority has the power to request network operators grant access to personal information for national security protection, this may be a risk to personal data.[184]

But, unlike the Chinese Cybersecurity Law, its Vietnamese counterpart does not require network operators to disclose their real names or personal identities, giving Vietnamese netizens more internet freedom.

---

181. Law on Network Information Security, 2015 (No. 86/2015/QH13) (Viet.), art. 7.

182. Socialist Republic of Viet. Law on Cybersecurity, art. 17(1) (2018).

183. *See id.*

184. For discussion on the same issue in the China's Cybersecurity Law, see Lee, *supra* note 6, at 88.

D. *Implementation*

1. China

China's Cybersecurity Law came into effect on June 1, 2017. It provides comprehensive administrative liabilities for the violation of each provision. For example, if a network operator fails to fulfill its responsibility for cybersecurity protection, or to promptly implement remediation measures and report the incident to the relevant authorities in the event of an incident, and refuses to correct the errors after receiving a warning from the government, it will be subject to "a fine ranging from RMB 10,000 to RMB 100,000, and its directly responsible person in charge will be subject to a fine ranging from RMB 5,000 to RMB 50,000."[185] If a critical information infrastructure operator fails to conduct security background checks on responsible personnel in critical positions, implement disaster recovery backups, or conduct inspections of its network security at least annually and refuses to correct errors after receiving a warning from the government, it will "be subject a fine ranging from RMB 100,000 to RMB 1,000,000, and its directly responsible person in charge will be subject to a fine ranging from RMB 10,000 to RMB 100,000."[186]

The Chinese government has actively enforced the Cybersecurity Law since it came into effect in June 2017. Numerous cases implicating the Cybersecurity Law have been reported, including those pertaining to personal information protection,[187] cybercrimes, [188] spreading information jeopardizing national security,[189] and configuring websites to advocate for secession.[190] The Cyberspace Administration of China (CAC) has issued several rules to implement the Cybersecurity Law.[191]

---

185. China's Cybersecurity Law, art. 59. A fine ranging from "RMB 10,000 to RMB 100,000" is approximately USD 1,580 to USD 158,000. A fine ranging from "RMB 5,000 to RMB 50,000" is approximately USD 790 to USD 7,900.

186. *Id*; Guanjian Xinxi Jichusheshi Anquanbaohu Tiaoli (关键信息基础设施安全保护条例) [Regulations on the Security Protection of Critical Information Infrastructure], art. 39, (promulgated by the State Council, Apr. 27, 2021, effective on Sept. 1, 2021).

187. *See, e.g.*, JONES DAY, *China Cybersecurity Law Continues to Bring Enforcement Crackdown*, LEXOLOGY, (Nov. 9, 2019) https://www.lexology.com/library/detail.aspx?g=5fd25c1e-2108-4bea-a473-90be786be21d [https://perma.cc/J4MF-7KWS] (archived Mar. 16, 2022).

188. *Id.*

189. *See* Lee, *supra* note 6, at 92.

190. *See id.* at 92–93.

191. *See, e.g.*, Provisions on the Administration of Microblog Information Services (微博客信息服务管理规定), (promulgated by Cyberspace Administration of China (CAC), Feb. 2, 2018); Provisions on the Administration of Blockchain Information Services (区块链信息服务管理规定), (promulgated by Cyberspace Administration of China (CAC), Jan. 10, 2019); Provisions on the Protection of Children's online Personal Information (儿童个人信息网络保护规定), (promulgated by Cyberspace Administration of China

However, although the government has issued several consultation drafts concerning data localization,[192] it has not yet finalized the most controversial rules concerning the cross-border transfer of personal data and important information.

2. Vietnam

Vietnam's Cybersecurity Law took effect on January 1, 2019. It requires the administrators of information systems critical to national security to ensure the satisfaction of all the law's conditions within twelve months of the effective date of the law, and the law provides that the CTF shall assess compliance.[193]

The Cybersecurity Law itself does not provide sanctions for violations of its requirements. Rather, the applicable sanctions are found in Vietnam's Criminal Code (the last version of which was published in 2015) and administrative regulations. Chapter XIII of the Criminal Code includes thirteen articles on offenses against national security. In particular, those who violate the prohibitions provided in the Cybersecurity Law can be punished according to Article 117 of the Criminal Code, which provides that any person who makes, stores, or spreads information, materials, or items for the purpose of opposing the state shall face a penalty of one to five years' imprisonment.[194]

Apart from criminal sanctions, in February 2020 the government issued a regulation on administrative punishments for cyber activities.[195] The main forms of sanctions include warnings and fines, while supplementary forms include revocation of the right to use licenses for a period of one to twenty-four months, confiscation of the property used for administrative violations, suspending operations for a period of one to twenty-four months, and deportation.[196]

(CAC), Aug. 22, 2019); Provisions on Governance of Network Information Content Ecology (网络信息内容生态治理规定), (promulgated by Cyberspace Administration of China (CAC), Dec. 15, 2019).

192. Guidelines for Security Assessment of Cross-Border Transfer of Personal Information and Important Data (Consultation Draft) (个人信息和重要数据出境安全评估办法(征求意见稿)), (promulgated by Cyberspace Administration of China ("CAC"), Apr. 11, 2017); Guidelines for Data Cross-Border Transfer Security Assessment (Consultation Draft) (信息安全技术数据出境安全评估指南(征求意见稿)) (promulgated by National Information Security Standardization Technical Committee, Aug. 31, 2017); Guidelines for Security Assessment of Cross-Border Transfer of Personal Information (Consultation Draft) (个人信息出境安全评估办法(征求意见稿)), (promulgated by Cyberspace Administration of China ("CAC"), June 13, 2019).

193. *See* Socialist Republic of Viet. Law on Cybersecurity, art. 43 (2018).

194. Socialist Republic of Viet Criminal Code, art. 117 (2015).

195. *See* Socialist Republic of Viet. Decree on Penalties For Administrative Violations In Posts, Telecommunications, Radio Frequency, Information Technology And Electronic Transactions, No. 15/2020/NĐ-CP (Feb. 3, 2020).

196. *Id.* art. 3.

Particularly, the Cybersecurity Law and administrative measures were used to deal with information regarding the COVID-19 pandemic. According to the relevant authority, the police force has handled more than thirty cases regarding the spread of "false information" about the pandemic.[197] In the province of Nghe An, the authorities have started seven cases against those spreading false information on social networks.[198] In Ho Chi Minh City, artists were fined for posting "false information" about the pandemic on social networks.[199]

III. COMPARATIVE ANALYSIS

Comparative law scholarship explores the convergences and divergences of legal systems and their contributing factors.[200] This Part probes the convergences and divergences of the cybersecurity laws in China and Vietnam. The findings contribute to both comparative socialist law and comparative cybersecurity law scholarship.

A. *Convergences*

The Chinese and Vietnamese Cybersecurity Laws have many convergent points in major legal issues pertaining to banned acts, network operators, critical infrastructure, data localization, and personal data protection. There are two types of factors explaining their convergences: immediate and structural. First, their convergences are due to the immediate diffusion of the Chinese Cybersecurity Law into Vietnam. At a deeper level, their convergences are shaped by broader structural factors; namely, the countries' ideational and institutional similarities, including the socialist state, socialist legality, and statist rights. The immediate and structural factors are interrelated because these shared ideational and institutional features facilitate immediate learning. However, the structural factors have independent explanatory values. The two

---

197. *Ngọc Anh, Hiệu quả của Luật An ninh mạng sau hơn 1 năm đi vào cuộc sống*, BÁO ĐIỆN TỬ CONG NGHE AN (Feb. 18, 2020), https://congannghean.vn/phap-luat/202002/hieu-qua-cua-luat-an-ninh-mang-sau-hon-1-nam-di-vao-cuoc-song-892362/ [https://perma.cc/KW5S-98UN] (archived May 8, 2022).

198. *Id.*

199. *Id.*

200. *See, e.g.*, Oliver Brand, *Conceptual Comparisons: Toward a Coherent Methodology of Comparative Legal Studies*, 32 BROOK. J. INT'L L. 405, 423 (2007); Sagit Leviner, *The Intricacies of Tax and Globalization*, 5 COLUM. J. TAX L. 207, 223–26 (2014); Anthony Ogus, *Competition Between National Legal Systems: A Contribution of Economic Analysis to* Comparative Law, 48 INT'L & COMP. L.Q. 405, 405–06 (1999); Mathias Reimann, *The Progress and Failure of Comparative Law in the Second Half of the Twentieth Century*, 50 AM. J. COMP. L. 671, 678–79 (2002).

cybersecurity laws may share common features, as they are both shaped by deep socialist commitments.

1. Immediate Diffusion of Cybersecurity Law

The immediate factor is the diffusion of the Chinese Cybersecurity Law into Vietnam through a learning mechanism. Comparative law scholarship explores legal diffusion or "transplants"—the movement of laws from one country to another country—as a tool of legal change.[201] In the last few decades, the diffusion of legal models, ideas, and institutions from different countries, including China, has been a familiar form of legal reform in Vietnam.[202]

The diffusion of Chinese law into Vietnamese law can be traced back to pre-modern times. For example, the Hong Duc Code of the Le Dynasty and the Gia Long Code of the Nguyen Dynasty were modeled after the Ming Code and Qing Code in China, respectively.[203]

In modern times, John Gillespie demonstrated that during the early period of the Renovation (initiated in 1986), "Vietnamese lawmakers turned initially to China for legal inspiration."[204] However, Gillespie argued that Chinese influence on Vietnamese legal development was limited due to several factors: China and Vietnam had a border war in 1979; Vietnamese lawmakers knew more about Soviet and East German law than Chinese legal and economic development and the Chinese language; and in the late 1980s, "the Chinese legal model had not yet proved its capacity to generate sustained economic growth."[205]

Despite these limiting factors, the diffusion of the Chinese Cybersecurity Law into Vietnam is evident. The Vietnamese translation of the Chinese Cybersecurity Law was attached to the draft

---

201. *See* William Twining, *Social Science and Diffusion of Law*, 32 J.L. & SOC'Y 203 (2005). *See generally* ALAN WATSON, LEGAL TRANSPLANTS: AN APPROACH TO COMPARATIVE LAW (1974).

202. *See* John Gillespie, *Transplanted Company Law: An Ideological and Cultural Analysis of Market-Entry in Vietnam*, 51 INT'L & COMPAR. L.Q. 641–72 (2002); Matthew Steven Erie & Do Ha Hai, *Law and Development Minus Legal Transplants: The Example of China in Vietnam*, ASIAN J.L. & SOC'Y, (forthcoming), https://ssrn.com/abstract=3581475 [https://perma.cc/K9LH-UQZ3] (archived Mar. 16, 2022).

203. *See generally* TA VAN TAI, NGUYEN NGOC HUY, & TRAN VAN LIEM, THE LE CODE: LAW IN TRADITIONAL VIETNAM, A COMPARATIVE SINO-VIETNAMESE LEGAL STUDY WITH HISTORICAL-JURIDICAL ANALYSIS AND ANNOTATIONS (1987); Nguyễn Thị Thu Thủy, *Về Mối Quan Hệ Giữa "Hoàng Việt Luật Lệ" Và "Đại Thanh Luật Lệ"* [*On The Relationship Between The "Hoàng Việt Luật Lệ" And the Great Qing Code*], 418 TẠP CHÍ NGHIÊN CỨU LỊCH SỬ, 19, 19 (2011).

204. John Gillespie, *The Juridification of State Regulation in Vietnam*, *in* LEGAL REFORMS IN CHINA AND VIETNAM: A COMPARISON OF ASIAN COMMUNIST REGIMES 78, 92 (John Gillespie & Albert H.Y. Chen eds., 2010).

205. *Id.*

of Vietnamese Cybersecurity Law submitted to the Vietnamese legislature in October 2017.[206] Timing is also a relevant factor: the Vietnamese draft of the cybersecurity law was submitted to the National Assembly shortly after the same law was adopted in China in the same year, implying Vietnamese lawmakers' intentions to learn from the Chinese experience in drafting their cybersecurity law. Therefore, it is unsurprising that the two laws share similar points on major legal issues.

The diffusion of the Chinese Cybersecurity Law into Vietnam can be explained by the logic of learning models. The learning models posit that "individuals copy the actions or strategies that are most prevalent or that are performing above average."[207] This logic can also be applied to institutions such as states. China's success in the supervision of citizens' activities in cyberspace being most prevalent and its performance in this area being above average[208] gave Vietnam the impetus to turn to Chinese lessons in drafting its own Cybersecurity Law. Geographic proximity may also have facilitated the immediate diffusion of the Chinese Cybersecurity Law into Vietnam. Furthermore, an immediate turn to the Chinese Cybersecurity Law likely reduced the cost of time, institutional resources, human resources, and the like in drafting the Vietnamese Cybersecurity Law.

However, immediate diffusion is not the only factor explaining the convergence of the cybersecurity laws in China and Vietnam. At a deeper level, the convergence is shaped by structural factors.

2. The Socialist State: Cybersecurity as Regime Security

One important structural factor is the socialist state. Both China and Vietnam are socialist states characterized by the leadership of a communist party over the state and society, Marxism-Leninism as the guiding ideology of the party and the state, and a centralized

---

206. The Vietnamese translation of the Chinese Cybersecurity Law is available at the website of the Vietnamese National Assembly at: http://duthaoonline.quochoi.vn/Pages/dsduthao/chitietduthao.aspx?id=1382

207. SCOTT E. PAGE, THE MODEL THINKER: WHAT YOU NEED TO KNOW TO MAKE DATA WORK FOR YOU 306 (2018).

208. *See, e.g.*, ANUPAM CHANDER, THE ELECTRONIC SILK ROAD: HOW THE WEB BINDS THE WORLD TOGETHER IN COMMERCE 193–201 (2013); REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM 32–40 (2012); Lee, Liu, & Li, *supra* note 23, at 419–26; Hoffman, *supra* note 71, at 188; *see also* Jean-Christophe Plantin & Gabriele de Seta, *WeChat As Infrastructure: The Techno-Nationalist Shaping of Chinese Digital Platforms*, 12 CHINESE J. COMMC'N 257, 259, 268–70 (2019) (describing how China enables more government control over internet activities through the social media platform WeChat); Mikkaela A. Salamatin, Note, *China's Belt and Road Initiative is Reshaping Human Rights Norms*, 53 VAND. J. TRANSNAT'L L. 1427, 1440–41 (2020) (revealing that more and more countries are learning digital surveillance systems from China).

institutional structure shaped by the Leninist principle of "democratic centralism" as an antithesis of Montesquieu's theory of separation of powers.[209]

The socialist state is the institutional source of law. Consequently, law is enacted to protect the socialist state. Cybersecurity laws are no exception. Their main function in China and Vietnam is to protect not only cybersecurity but also regime security. Therefore, unlike the Western approach to cybersecurity, which focuses on technological threats, the socialist approach to cybersecurity emphasizes political and ideological threats[210] to the stability of the socialist state, the hegemony of the communist party, and the legitimacy of Marxist-Leninist ideology.

The political and ideological threats are real. In China, the 2009 Xingiang riot caused the shutdown of the internet in the entire region.[211] A few years later, the enactment of the Cybersecurity Law was partly driven by the incident of Edward J. Snowden, a former Central Intelligence Agency employee and contractor in the United States, who revealed that the US government had been spying on foreign governments through hacking operations, including in China.[212] Moreover, activists and other people deployed cyber platforms to challenge the socialist regime.[213] Activists criticizing the government or mobilizing citizens via the internet in China have been arrested and subject to criminal liabilities.[214] In the case of Vietnam, various activists and their organizations (e.g., the Bloc 8406, the Committee for Democracy and Human Rights, and the periodical *Free Speech*) used the internet to advocate for liberal democratization,[215] which posed a threat to the socialist state. Understandably, a main function of the cybersecurity laws in socialist states is to prevent online activism to protect the security of the socialist regime. In addition, the

---

209. For more details, see BUI NGOC SON, CONSTITUTIONAL CHANGE IN THE CONTEMPORARY SOCIALIST WORLD 79–81 (2020).

210. Lee, *supra* note 6, at 90; *see also* Rogier Creemers, *Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century*, 26 J. CONTEMP. CHINA 85, 95 (2017) (arguing that China's internet governance as designed to maintain the stability of the regime); Hoffman, *supra* note 71, at 189 (describing how China uses censorship for its unique cybersecurity purpose).

211. Creemers, *supra* note 210, at 86.

212. *See, e.g.*, Mirren Gidda, *China's New Cybersecurity Law Could Cost Foreign Companies Their Ideas*, NEWSWEEK (May 31, 2017), http://www.newsweek.com/china-cybersecurity-hacking-intellectual-property-multinationals-618345 [https://perma.cc/62C2-FMWA] (archived Feb. 10, 2022); Wee, *supra* note 7.

213. For China, see generally JING WANG, THE OTHER DIGITAL CHINA: NONCONFRONTATIONAL ACTIVISM ON THE SOCIAL WEB (2019). For Vietnam, see BENEDICT J. TRIA KERKVLIET, SPEAKING OUT IN VIETNAM: PUBLIC POLITICAL CRITICISM IN A COMMUNIST PARTY–RULED NATION 87–114 (2019).

214. *See, e.g.*, Creemers, *supra* note 210, at 92.

215. KERKVLIET, *supra* note 213, at 102–03.

spread of alternative ideas (e.g., liberal and universal ideas) about a legitimate governance structure in cyberspace may challenge the legitimacy of socialist ideology. This explains why the cybersecurity laws (e.g., through the entrenchment of prohibited acts) attempt to limit ideational diffusion for ideological security.

3. Socialist Legality and Cybersecurity

Another structural factor is the principle of socialist legality. Both China and Vietnam adopted this principle from Soviet law.[216] Socialist legality requires that the state's statutes, regulations, and decrees be observed by social organs and citizens in the strictest fashion.[217] This principle shapes the following common features of the cybersecurity legal framework in China and Vietnam.

First, socialist legality defines the *regulatory* nature of the cybersecurity legal framework. Cybersecurity laws facilitate state interventional control of socioeconomic organs and citizens' activities in cyberspace by, for example, entrenching banned activities, imposing duties on network operators, requiring data localization, and enabling authorities' access to personal data.

Second, socialist legality facilitates a *formal* framework for cybersecurity regulation. This framework involves the formal enactment of cybersecurity laws that comprehensively regulate organizations' and citizens' activities in cyberspace. However, the formal framework is not limited to statutes but broadly includes numerous regulations and decrees issued by different administrative agencies to detail and interpret the provisions in the laws. Consequently, cybersecurity laws in the socialist countries of China and Vietnam are not principally the legalistic law of lawyers to be used in courts. Rather, they are political-administrative laws formally enacted and interpreted by political and governmental bodies. Take China, for example: dozens of cases concerning violations of the Cybersecurity Law have been reported since it came into effect on June 1, 2017, and all ended with administrative penalties imposed by

---

216. For China, see Fu Hualing, John Gillespie, Pip Nicholson, & William Parlett, *Socialist Law in Socialist East Asia*, *in* SOCIALIST LAW IN SOCIALIST EAST ASIA 3, 10 (Hualing Fu, John Gillespie, Pip Nicholson, & William Partlett eds., 2018). For Vietnam, see Pham Duy Nghia & Do Hai Ha, *The Soviet Legacy and Its Impact on Contemporary Vietnam*, *in* SOCIALIST LAW IN SOCIALIST EAST ASIA 97, 104 (Hualing Fu, John Gillespie, Pip Nicholson, & William Partlett eds., 2018).

217. Imre Szabó, *III. The Socialist Conception of Law*, *in* INTERNATIONAL ENCYCLOPEDIA OF COMPARATIVE LAW ONLINE (U. Drobnig et al. eds., 2018), http://dx.doi.org/10.1163/2589-4021_IECO_COM_020103 (last visited Jan. 4, 2021) [https://perma.cc/U9P2-ASD5] (archived Feb. 12, 2022).

relevant authorities on violating parties.[218] Although the authors' search in the Peking University (PKU) Law Database revealed that the cybersecurity law was cited in 118 court decisions in China, no party was held liable under the Cybersecurity Law in these cases. The law was often cited to define legal concepts, such as "personal information," but not as a legal basis for liability.[219]

Third, socialist legality shapes the *institutional* features of the cybersecurity regulatory framework. Structural institutions of the framework include general state institutions and specific institutions created to facilitate the stringent observation of the laws. In China, while the primary government authority in charge of implementing the

---

218. Cybersecurity Law Research Center at the Third Research Institute of the Ministry of Public Security of the People's Republic of China, *A Comprehensive Collection of Cases Regarding the Enforcement of Cybersecurity Law Issue II* (《网络安全法》执法案例汇总第二期) (Oct. 16, 2017) http://www.djbh.net/webdev/web/HomeWebAction.do?p=getZxdt&id=8a8182565deefd0d015f22b943710128&xx=a57ea59e9f6cf27b129f9bf21f7111ee [https://perma.cc/A48Y-6TNC] (archived Feb. 12, 2022); Zhong Lun Law Firm, 2019 Annual Report on Cybersecurity and Data Protection (2019年网络安全河数据保护年度报告), Annex 1 Cases of Cybersecurity Law Enforcement (附件一：《网络安全法》行政执法相关处罚案例一览) (2019) http://f.wkinfo.com.cn/law/附件一.pdf (last visited Jan 25, 2021) [https://perma.cc/6X9J-5LAN] (archived Feb. 12, 2022).

219. *See, e.g.*, Cheng Weihong v. Zhao Chunfei (程卫红与赵春飞合同纠纷案), [2020] Su 0281 Min Chu No.7297 (People's Ct. of Jiangyin District of Jiangsu Province Mar. 21, 2021) (citing Article 76 (5) of the Cybersecurity Law to define the scope of "personal information"); Liu Ruibo v. Beijing Happy Elements Tech. Co. (刘瑞博与乐元素科技（北京）股份有限公司隐私权纠纷案), [2020] Jin 01 Min Zhong No. 8911 (Beijing 1st Interm. People's Ct. Dec. 28, 2020) (citing Article 76 (5) to clarify the definition of "personal information"); Ling v. Beijing Weibo Shijie Tech. Co. (Douyin)(凌某某诉北京微播视界科技有限公司隐私权、个人信息权益网络侵权责任纠纷案), [2019] Jin 0491Min Chu No. 6694 (Beijing Internet Ct. Jul. 30, 2020) (referring to 76(5) of the Cybersecurity Law regarding the definition of "personal information" and to Articles 41 regarding the principle of managing personal information); Huang v. Shenzhen Tencent Tech. Co. (黄某诉腾讯科技(深圳)有限公司等隐私权、个人信息权益网络侵权责任纠纷案), [2019] Jin 0491Min Chu No.16142 (Beijing Internet Ct. Jul. 30, 2020) (citing Article 76(5) to distinguish "personal information" from "privacy"); Hu Yongming v. Xiang Songbai (胡永明、向松柏名誉权纠纷案), [2019] Chuan 1602 Min Chu No.7224 (Guangan District Ct. of Sichuan Province Jun. 22, 2020) (citing Article 76 (5) to define the scope of "personal information"); Deng Lirong v. Beijing S.F. Holding Co., Ltd. (邓立容与北京顺丰速运有限公司侵权责任纠纷上诉案), [2020] Jing 03 Min Zhong No.2049 (Beijing 3rd Interm. People's Ct. Mar. 26, 2020) (citing Article 76 (5) to define the scope of "personal information"); Fu Quangui v. Beijing Sankuai Information & Technology Co. (Meituan)(付全贵与北京三快信息科技有限公司等网络侵权责任纠纷案) [2018] Jin 0491 Min Chu No.1905 (Beijing Internet Ct. May 27, 2019) (citing Articles 21, 41, 42(2), and 76 to specify the obligations of network operators and to define the scope of "personal information"); China Taobao Software Co. v. Anhui Meijing Information & Technology Co. (淘宝（中国）软件有限公司与安徽美景信息科技有限公司不正当竞争纠纷案), [2018] Zhe 01 Min Zhong No.7312 (Hangzhou Interm. People's Ct. Dece. 22, 2018) (citing Article 76(5) to identify "personal information" from general user information). The search was conducted by the authors in the PKU Law Database (https://www.pkulaw.cn/) as of October 15, 2021.

Cybersecurity Law is the CAC, other government agencies, such as the telecommunications department of the State Council and public security departments on national and local levels, are also responsible for cybersecurity protection, supervision, and administration within the scope of their respective functions.[220] In the case of Vietnam, the general institutions include the government, the Ministry of Public Security, the Ministry of National Defense, the Ministry of Information and Communications, and the Government Cipher Committee, and the specific institutions include CTFs under ministerial institutions.

Fourth, socialist legality determines the *procedural* features of the cybersecurity regulatory framework. Cybersecurity laws include multiple procedures to review, assess, inspect, and supervise cybersecurity. These heavy procedures are not merely technological but facilitate the state's detailed control of citizens' activities in cyberspace to ensure their strict observation of the legal requirements regarding cybersecurity and, sometimes, to foster the development of the local cybersecurity industry.

4. Statist Digital Rights

Last but not least, the convergences in the cybersecurity laws in China and Vietnam are shaped by their similar statist approaches to human rights. Their constitutions include the notion of human rights and provide a long list of fundamental rights, including rights related to cybersecurity, such as freedom of speech, freedom of expression, and the right to personal privacy.[221] However, the socialist approach to rights is fundamentally different from the Western liberal or universalist approaches.[222] Socialist rights are not liberal rights; that is, they are not legal limits on state power,[223] nor are they conceived as universal rights inherent to human beings. Rather, rights in the socialist states are statist rights; that is, they are granted to citizens by the state.[224] Consequently, their meaning and scope are determined by the state. In addition, as rights are granted to citizens by the state, the state can withdraw them when it considers it necessary to do so. Moreover, rights are given to citizens in exchange for their duty to the

220. China's Cybersecurity Law, art. 8; *see also* Wang, *supra* note 23, at 401 (describing how China's authorities regulate the physical layer, logical layer, and content layers of the Internet).

221. XIANFA arts. 33, 35, 40 (2018) (China); THE CONSTITUTION OF THE SOCIALIST REPUBLIC OF VIETNAM arts. 14, 21, 25 (2013).

222. *See* Lee, *supra* note 6, at 100 (distinguishing between Chinese human rights and Western human rights).

223. *See id.*; Frédéric Krumbein, *The Human Rights Gap in the Taiwan Strait: How China Pushes Taiwan Towards the US*, PAC. REV. 8–9 (2020).

224. Lee, *supra* note 6, at 100 ("Therefore, human rights are never considered to represent an individual's rights over the Chinese state.").

state. Therefore, fundamental rights are not separated from fundamental duties.[225]

China explained the concept of "human rights with Chinese characteristics" in its 2018 Universal Periodic Review submitted to the United Nations Human Rights Council:

> As an important element in the economic and social development of each country, the cause of human rights must be promoted on the basis of the national conditions and the needs of the people of that country, and cannot be defined on the basis of a single authority . . . As it upholds the principle of the people's primacy, China is enhancing the people's well-being and promoting the comprehensive development and common prosperity of the people as a whole . . . [China] attaches increasing importance to the economic, social and cultural rights and the right to development that are of concern to developing countries, and promotes the comprehensive development of human rights of all kinds.[226]

China intentionally distinguishes its understanding of human rights from Western values by emphasizing the "common prosperity of the people as a whole."[227] To illustrate the case of Vietnam, consider the approach to human rights expressed in the country's White Paper on Human Rights:

> Vietnam is also of the view that there should be a comprehensive approach to human rights, comprised of civil, political, economic, social and cultural rights and all categories of rights should be treated on the same footing. At the same time, the rights and freedom of each individual can only be protected and promoted on the basis of respect for the common rights and interests of the nation and community, and one's rights must be accompanied by his/her obligations to the society.
>
> The Vietnamese Government holds the view that protecting and promoting human rights are primarily the responsibility of the State . . . Given differences

225. For more details on statist approach to rights in the socialist states, see BUI, *supra* note 209, at 81–82; *see also* Yu-Jie Chen, *China's Challenge to the International Human Rights Regime*, 51 N.Y.U. J. INT'L L. & Pol. 1179, 1211 (2019) ("[H]uman rights should be conditioned on the performance of duties by the individual."); Randall Peerenboom, *Assessing Human Rights in China: Why the Double Standard?*, 38 CORNELL INT'L L.J. 71, 81 (2005) ("Moreover, the emphasis on [human] rights [in China] should not obscure the importance of duties and the responsibilities of individuals toward others.").

226. Human Rights Council, Working Group on the Universal Periodic Review, National Report Submitted in Accordance with Paragraph 5 of the Annex to Human Rights. Council Resolution 16/21, China, U.N. Doc. A/HRC/WG.6/31/CHN/1, at 2–4 (Aug. 20, 2018).

227. *Id.*

> in political regime, development level, cultural value and historical background, approaches to human rights might vary from country to country.[228]

Thus, Vietnam has its own statist approach to human rights, as the protection and promotion of rights depend on the state, and rights go hand in hand with obligations to the state and society.

Rights statism is embodied in the two cybersecurity laws in China and Vietnam. Citizens may enjoy digital rights to the extent that they do not pose threats to the socialist state, as defined by the state. This statist approach to rights is particularly expressed in the two cybersecurity laws' similar provisions on banned acts, obligations of network operators, and the state's possible access to personal data. In addition, statist rights are not juridical rights to be claimed in courts, so unlike the institutional protection of rights through judicial checks on governmental power in Western democracies, courts in China and Vietnam play no role in interpreting the meaning of digital rights.[229] Rather, the interpretation of digital rights rests on administrative authorities, and the courts do not constrain governmental discretion in restricting digital rights for the sake of cybersecurity and national security.[230]

B. *Divergences*

Despite being set within similar socialist regimes, divergences in Chinese and Vietnamese political and legal developments have been documented.[231] In cybersecurity law, the foundational divergence is between the Chinese notion of cybersecurity sovereignty and the Vietnamese notion of national cyberspace. The former suggests that the internet is under national sovereignty, while the latter facilitates the national regulation of the internet but treats it as a global network that transcends national sovereignty. This divergence is foundational because it results in other differences in the two laws: for example, Vietnam's Cybersecurity Law does not require real-name registration

---

228. VIET NAM'S ACHIEVEMENTS IN THE PROTECTION AND PROMOTION OF HUMAN RIGHTS, 4 (Hanoi, 2005).

229. In China and Vietnam, courts are not constitutionally vested with the power to interpret the law. Rather, this power belongs to the standing committee of the legislature. *See* XIANFA, *supra* note 221, art. 67; CONSTITUTION OF VIETNAM, *supra* note 180, art. 74.

230. *See* Lee, *supra* note 6, at 102 (discussing the the lack of oversight that Chinese courts have over administrative entities' interpretation of rights).

231. *See* Fu Hualing & Jason Buhi, *Diverging Trends in the Socialist Constitutionalism of the People's Republic of China and the Socialist Republic of Vietnam*, *in* SOCIALIST LAW IN SOCIALIST EAST ASIA 135, 135–163 (Hualing Fu et al. eds., 2018); Edmund Malesky, Regina Abrami, & Yu Zheng, *Institutions and Inequality in Single-Party Regimes: A Comparative Analysis of Vietnam and China*, 43 COMPAR. POL. 401, 401–19 (2011).

as China's does. In addition, this central divergence may differentiate the implementation of similar cybersecurity legal provisions in the two countries.

1. Technological Architecture

The reasons for the divergences between the Chinese and Vietnamese cybersecurity laws are both technological and political. To begin, a difference in technological infrastructure accounts for one divergence. Lawrence Lessig has notably argued that code—software or hardware—can perform regulatory functions and can have the same effects as legal regulations.[232] The architecture of the internet has determined how information flows on it and how people perceive it.[233] Therefore, from a comparative law perspective, different internet architectures will likely result in different regulatory effects.[234]

The Chinese notion of cybersecurity sovereignty is underpinned by its technological infrastructure. Particularly, the Great Firewall in China is instrumental in ensuring its national sovereignty in cyberspace. The Great Firewall refers to the massive, sophisticated internet-filtering system used in China to block the populace from viewing online content hosted in other countries that government censors deem harmful to the nation.[235] It has played an important role in China to facilitate government control and censorship of online information flow.[236] While the content filtering enabled by the Great Firewall is not perfect and savvy users can always circumvent it via virtual private networks,[237] the Great Firewall, together with other censorship mechanisms, has successfully shaped internet user behavior in the country.[238] Empirical evidence reveals that most citizens in China use the internet for entertainment instead of political discussions.[239]

---

232. *See* LAWRENCE LESSIG, CODE VERSION 2.0, 5 (2006).

233. *See id.* at 6.

234. *See* Carla L. Reyes, *Cryptolaw for Distributed Ledger Technologies: A Jurisprudential Framework*, 58 JURIMETRICS 283, 290 (2018).

235. *See, e.g.*, Lee & Liu, *supra* note 27, at 129–35.

236. *See generally id.* at 137–45 (discussing the invisibility and pervasiveness of China's Great Firewall as compared to other countries' internet-filtering systems).

237. Lee, *supra* note 77, at 408.

238. *See* Lee & Liu, *supra* note 27, at 145–48; *see also* Creemers, *supra* note 210, at 86 ("Countering keyword-based censorship, netizens turned to puns and satire."); Jyh-An Lee, *Regulating Blogging and Microblogging in China*, 91 OR. L. REV. 609, 613–14 ("Owing to the government's strict control of online political speech, Chinese bloggers have learned to avoid publishing politically sensitive content or to publish it in disguised or indirect way.").

239. Lee & Liu, *supra* note 27, at 146.

From a regulatory perspective, the Great Firewall has facilitated the implementation of important internet laws and policies in China that might not be feasible in other countries. For example, South Korea abandoned its real-name registration rules partly because it lacked a Great Firewall to prevent users from accessing foreign websites that did not follow its rules.[240] Moreover, because of the Great Firewall, multinational internet companies cannot serve Chinese consumers with servers located outside Chinese territory.[241] If they plan to enter the Chinese internet market, they must subject themselves to Chinese sovereignty by setting up servers in the country.[242]

The Chinese government has been weaving its national ideology into its internet architecture since the internet architecture's inception in the mid-1990s.[243] Unlike the decentralized architecture in other countries, the internet architecture in China is designed with centralized points of control, where filtering technology can be installed.[244] This is why not every country can build a Great Firewall as effective as that in China today. For example, Australia once considered building a filtering system but was unable to do so because with a decentralized internet architecture, the Australian government failed to find control points to deploy the filtering system effectively.[245]

Internet censorship has been conducted in Vietnam as well, but Vietnam also lacks a Great Firewall, so it lacks the technological condition to claim cybersecurity sovereignty. What it can do is use regulatory instruments (e.g., the Cybersecurity Law and relevant administrative regulations) to control the flow of information on the internet.

2. Exceptionalism vs. Universalism

Political reasons also explain the divergences between Chinese exceptionalism and Vietnamese universalism.[246] Given its achievements in economic development and its prominent role in the international order, China is confident to articulate its distinctive developmental model as "socialism with Chinese characteristics."[247] Chinese exceptionalism is also embodied in the technological arena:

---

240. *Id.*, at 26–27.

241. *See* Lee, Liu & Li, *supra* note 23, at 424–28.

242. *See generally id.* at 413–17 (describing the Google's attempts to enter the Chinese market).

243. Lee & Liu, *supra* note 27, at 142.

244. *See id.*

245. *Id.* at 143.

246. For Chinese exceptionalism and Vietnamese universalism in the area of constitutional law, see BUI, *supra* note 209, at 63–64.

247. XIANFA, *supra* note 221, at pmbl.

China can develop technological alternatives to Western tech giants.[248] Based on its unique internet architecture, sizable market for electronic commerce, and fast technological development, China has developed its own regulatory model for the internet,[249] actively diffused its digital authoritarian practices,[250] and argued that its approach is more suitable to developing countries than that promoted by the "cyber hegemon" in the Western world.[251] This Chinese approach to the internet has become a model for governments particularly keen to exert more control over online activities.[252]

The concept of cybersecurity sovereignty is also an expression of Chinese technological exceptionalism. The aspiration to place the internet under national sovereignty is not merely to ensure cybersecurity but also to create the basis of China's distinctive form of technological innovation and broader development according to "socialism with Chinese characteristics."

Unlike China, Vietnam does not aspire to develop "socialism with Vietnamese characteristics." In terms of geography and population, Vietnam is smaller than China. Its development depends on the support of both its citizens and the broader international community. Therefore, Vietnam's developmental model tends to adhere to global norms and models with the necessary localization.[253] Vietnamese universalism is also embodied in the technological field.

Vietnam's Cybersecurity Law is influenced by the global diffusion of cybersecurity law generally, not merely the diffusion of Chinese laws. Along with the Vietnamese translation of China's Cybersecurity Law, a Vietnamese translation of Japan's Basic Act on Cybersecurity was attached to the draft of Vietnam's Cybersecurity Law submitted to

---

248. *See supra* text accompanying note 23.

249. *See, e.g.*, Lee & Liu, *supra* note 27, at 151 (claiming that "[t]he unusual history of the Chinese Internet has made it unique and effective in filtering online information"); Hong Shen, *China and Global Internet Governance: Toward an Alternative Analytical Framework*, 9 CHINESE J. COMM. 304, 305 (2016) (describing China's state-centric regulatory model based on the claim of Internet sovereignty in contrast with the American private multi-stakeholder model based on the idea of internet freedom); *see also* Jyh-An Lee, *The Red Storm in Uncharted Waters: China and International Cyber Security*, 82 UMKC L. REV. 951, 960–64 (elaborating different approaches to international cybersecurity by China and the United States); Wang, *supra* note 23, at 407–08 (describing China's resistance to the "ideological and infrastructural American hegemony" of the Internet).

250. McKune & Ahmed, *supra* note 71, at 3845–46; *see also* Wang, *supra* note 23, at 412–18 (describing how China promotes the concept of Internet sovereignty internationally).

251. McKune & Ahmed, *supra* note 71, at 3840–41.

252. *See, e.g.*, *id.* at 3846; Lee, Liu, & Li, *supra* note 23, 425–26; Salamatin, *supra* note 208, at 1440–41.

253. *See generally* John Gillespie, *Localized Global Competition Law in Vietnam: A Bottom-Up Perspective*, 64 INT'L COMP. L. Q. (2015).

the National Assembly in October 2017.[254] In addition, a report on cybersecurity law in various countries, including China, India, Russia, South Africa, the United States, and the United Kingdom, was submitted to the National Assembly together with the proposal to make Vietnam's Cybersecurity Law.[255] While the reference to Chinese experience was prominent, Vietnamese lawmakers studied global experiences in cybersecurity law. This indicates their universalist approach in making the Cybersecurity Law in Vietnam. The global reference may be the reason for the divergence between Chinese and Vietnamese cybersecurity law at a foundational level; the latter does not adopt the notion of cybersecurity sovereignty, which is not a prevailing concept in the global experience of cybersecurity law.

In addition to global diffusion, Vietnamese universalism is also embodied in technological infrastructure. The popular use in Vietnam of global platforms, such as Google, Facebook, and YouTube, expresses Vietnamese technological universalism. For cybersecurity and regime-security reasons, Vietnam regulates the internet under the notion of national cyberspace. However, for global integration, the country must treat the internet as a global network rather than attempt to place it under national sovereignty.

IV. CONCLUSION

This Article presents a Sino-Vietnamese comparative study of cybersecurity law. It argues that due to immediate diffusion and ideational and institutional similarities, the cybersecurity laws in the two socialist countries have important convergences. However, these convergences should not blind observers to the foundational divergence animated by the global diffusion of cybersecurity law in Vietnam and the differences in technological infrastructure and developmental approaches in China and Vietnam. This Article concludes with further reflections on implications for comparative law generally and comparative cybersecurity law particularly.

First, on comparative law, this Article suggests that legacies of socialist law should be taken seriously. The collapse of the Soviet Union does not entail the collapse of the entire socialist legal tradition. The legacies of socialist law remain prominent on a structural level in contemporary socialist countries, such as China and Vietnam. These legacies continue to shape lawmaking and legal change in these

254. The Vietnamese translation of the Japan's Basic Act on Cybersecurity is available at the website of the Vietnamese National Assembly at http://duthaoonline.quochoi.vn/Pages/dsduthao/chitietduthao.aspx?id=1382

255. The Ministry of Public Security of Vietnam Government, Báo Cáo Tham Khảo Kinh Nghiệm Pháp Luật Nước Ngoài Về Bảo Đảm An Ninh Mạng [The Report Experiencing Foreign Laws On Cyber Security] (2017).

countries, even in areas that seem largely technological, such as the internet. Another point in comparative law is that socialist legal legacies do not always lead to legal convergence, even within socialist countries. Due to their different physical sizes, populations, and international roles, socialist countries have different ways to acclimate their socialist legal systems to the global international environment, leading to many legal divergences. The divergent points in cybersecurity law in China and Vietnam exemplify this.

Second, this Article has specific implications for comparative cybersecurity law. While cybersecurity law has become a trendy subject encompassing many issues, such as national security, privacy, data security, trade secrets, online speech, and cybercrime, its substance differs from jurisdiction to jurisdiction. While the concept of cybersecurity in the Western world originates from technical threats, the socialist view of cybersecurity emphasizes the ideological threats to the stability of the regime and the society. This fundamental difference has resulted in dissimilar designs of enforcement agencies, procedures, and human rights protections in cybersecurity laws. Moreover, based on Lawrence Lessig's code-is-law theory, this Article argues that a country's internet architecture is its de facto internet law and that China's Great Firewall system has effectively facilitated the enforcement of its Cybersecurity Law and other internet regulations. Therefore, the Chinese model of internet regulation cannot be easily transplanted to other countries lacking a similar internet architecture.

***