June 16, 17, 2022

THE ROLE AND LIMITATION OF LAW AND TECHNOLOGY IN DIGITAL AUTHORITARIANISM

A STUDY OF CHINA UNDER COVID-19

Jiaxin Zhao

Shibolet & Co.

Tel Aviv - Shanghai

Abstract

Online speeches in China since the outbreak of Covid-19 have experienced crackdown of an unprecedented level of magnitude and efficiency. Like its digital surveillance system, which is expansively employed to fight the pandemic crisis, China's full-scale control of its cyberspace is the result of a decade-long practice in technological and legislative fields that gradually matured. The role of technology in building and reinforcing digital authoritarianism is broken down into three simultaneously functioning phases, namely blocking, filtering and manipulating information. Under a legal framework that aims to regulate all aspects of the cyberspace, as well as the advocacy of cyber sovereignty, technology companies become the complicit actor in facilitating to realise the State's vision. Netizens' resistance using technological and other tools has intensified since Covid-19, reflecting a shift of attitude from the governed regarding the deprivation of freedom. However, more profound issues are being discovered tardively. The interaction between law and technology in China reveals problems of the cyber sovereignty argument and legislation by convenience while departing further away from the rule of law.

I. Introduction

Chinese citizens had experienced an unprecedented free flow of information and liberty to discuss publicly their opinions since the popularisation of the internet - while it lasted. The number of internet users in China surpassed that of the United States in 2008,[1] not long before the country departed to become the largest and most sophisticated censorship in the world. The period of rapid development of China's information technology had also nurtured global tech giants which later came to be known as Alibaba, Huawei, Tencent, etc. The prosperous digital economy was accompanied by a relatively free internet which offered unparalleled access to information and freedom of expression to the governed.

Yet what makes it marvellous is exactly what makes it dangerous. As we enter more profoundly into the digital age, authoritarian governments are sensitive to an ideological subversion that is made more easily by availability of unchained information. Harari observes that while a political shift has complex reasons, those reasons "appear to be intertwined with current technological developments."[2] The critical roles of technology and law, as well as their interplay, call for an examination on how the State's goal for more control over its citizens has been gradually realised through the rapid development of technology intertwined with legal instruments, and whether the latter provide a solid legal basis, particularly against the background of Covid-19.

Therefore, the paper attempts to answer the following question: What are the limitations of law in China's growing digital authoritarianism and has their implication on the social order shifted since Covid-19?

---

1 *China surpasses US in number of internet users,* THE NEW YORK TIMES, July. 26, 2008, https://www.nytimes.com/2008/07/26/business/worldbusiness/26internet.html.

2 Yuval Noah Harari, *Why technology favor tyranny,* THE ATLANTIC, Oct. 2018, https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330/.

The question will be addressed in three parts. Section II of the paper will seek possible justifications elaborated by the legal framework in order to explain whether and how such practice may find its basis in law; Section III will identify major technological mechanisms to achieve digital censorship as well as the important market players making it possible; Section IV will build on aforementioned analysis to discuss the implications of this structure, notably limitations of cyber sovereignty and legislative reliance, as well as its impact on the social order. Throughout the paper, online censorship and big data surveillance, as two most pertinent cyber practices to Covid-19, will be examined.

II. The Legal Framework[3]

The first laws criminalising illegal online posting were enacted back in 1997,[4] following the "Year of the Internet" when around 150,000 Chinese citizens had access to it.[5] It was a time when neither information technology nor law was advanced in China. In 2013, the priority to develop a comprehensive legal framework as a response to challenges of progressive information technology started to implement itself under President Xi. This section will explain the relevant legal instruments and their real-life application scenarios.

2.1 The Constitution

Constitutional rights relevant to the scope of this paper are those concerning freedom of expression and right to privacy. Article 35 of the Constitution provides for freedom of speech and of the press, among others[6]. Although there is no single provision in the Constitution articulating the right to privacy, legal scholars argue that a constitutional basis to protect the right to privacy[7] is provided in Articles 38 and 39 declaring the inviolability of personal dignity[8] and private homes,[9] as well as to guarantee free and private correspondences between citizens as provided in Article 40.[10]

---

[3] China's immense administration bodies dwarf its judicial system. Therefore, in practice, it is necessary to also follow closely components other than the Constitution and the laws, such as regulations, measures, guidelines, answers from the administration, etc., in order to fully understand China's regulatory framework. Such piecemeal components will not be elaborated in this paper which will focus on key legislations of China's cyberspace governance system.

[4] Computer Information Network and Internet Security, Protection and Management Regulations, Nov.30, 1997, http://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/computer-information-network-and-internet-security-protection-and-management-regulations-1997.html.

[5] *China to boost internet access,* UNITED PRESS INTERNATIONAL, Jan.6, 1997, https://www.upi.com/Archives/1997/01/06/China-to-boost-internet-access/7863852526800/.

[6] PRC Const. art. 35.

[7] Jingchun Cao, *Protecting the right to privacy in China,* VUWLR. 36, no.3 (2005), 645, 660-61, https://doi.org/10.26686/vuwlr.v36i3.5610.

[8] *Supra* note 6, art. 38.

[9] *Id.* art. 39.

[10] *Id.* art. 40.

However, there are primarily two factors that call for seeking further beyond the Constitution. First of all, the Constitution is inadequate, if not entirely useless, in Chinese legal practice to invoke the Constitution in court or under other judicial circumstances.[11] Therefore, substantive provisions from relevant laws which often find its leading principles in the Constitution ought to be reviewed as elaborated in Section 2.2 below.

In addition, the nature of China's Constitution determines the overriding principles of the Communist Party's (Party) rule and emphasises on the foremost and irreplaceable role of the Party in the operation of the State, including in the administration of the rule of law. This idea was further asserted by President Xi Jinping that the Party leads everything, including law[12]. It is defined in the preamble of the Constitution that the basic task of the nation is to "concentrate its effort on socialist modernisation […] under the leadership of the Communist Party of China."[13] It is also immediately stipulated in Article 1 of the Constitution that "sabotage of the socialist system by any organisation or individual is prohibited.[14] Moreover, Article 53 requires citizens to simultaneously respect the Constitution and state secrets.[15]

2.2 The Laws

Compromises on freedom of expression and privacy often find their legal basis in issues regarding national security and public policy. This section will first examine some most important legislations in the field of security, namely cybersecurity and national security (including state secrets, national security provisions which extended to Hong Kong, and counter-terrorism). Then it will proceed to explain the new data security laws enacted last

---

[11] Daniel Sprick, *Judicialization of the Chinese Constitution Revisited: Empirical Evidence from Court Data*, CHINA REVIEW 19, no.2 (2019), 41-68, https://ssrn.com/abstract=3333958.

[12] Xi Jinping, *Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era,* 18, Oct. 2017, https://www.mfa.gov.cn/ce/ceil/eng/zt/19thCPCNationalCongress/W020171120127269060039.pdf.

[13] *S*upra note 6, preamble, para. 3.

[14] *Id.* art. 1.

[15] *Id.* art. 53.

year to understand the uniqueness of China's approach to the cyberspace. These laws combined, old and latest, reflect China's desire to cover broadly its legislative framework to catch up with its effort in building a cyber-governance regime.

2.2.1 Security Laws

A. State Secrets Law

Article 53 of the Constitutiton requires state secrets to be simultaneously respected as the Constitution itself. State secrets are defined as "matters which relate to the national security and interests as determined under statutory procedures and to which access is vested in a limited scope of persons […]".[16] Categories of state secrets are further defined in the subsequent provisions with a catch-all paragraph containing "other classified matters as determined by the State Secrecy Administrative Department"[17].

Vague yet comprehensive, it is reasonable to speculate that many deleted online speech had belonged to this catch-all category, given that expression of dissatisfaction with the government does not fit into the other categories mentioned in the same provision, except for being remotely relatable to that of national security, if wording one's discontent may be construed as some sort of plot to threaten national security.

B. National Security Laws – from Mainland China to Hong Kong

There are two versions of National Security Law, one enacted in July 2015 for the Chinese Mainland, i.e., the National Security Law (NSL); the other enacted in June 2020 for Hong Kong, i.e., the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (HKNSL). While the NSL focuses primarily on national security in a conventional (and broad) sense, the HKNSL addresses directly freedom of expression matters.

---

16 Law of the People's Republic of China on Guarding State Secrets of 1988 (2010 revision), art. 2.

17 *Id.* art. 9.

The HKNSL specifically offers protection for basic human rights such as freedom of speech and its adherence to the International Covenant on Civil and Political Rights (ICCPR) – a provision[18] nowhere to be found in its Mainland counterpart legislation. Nonetheless, a series of unheard cases and denied bails[19] on the ground of the HKNSL have obscured the understanding of how those basic rights are being safeguarded.

Besides individual cases, the Hong Kong Bar Association was labelled by Beijing as being "political"[20] which is paradoxical in at least two ways. First, the so-called political comments[21] by the Bar Association were about the rule of law and second, if Hong Kong Bar Association were to be treated in a similar manner as its Mainland counterparts, i.e., bar associations across all Chinese cities, then it would in fact be expected to be "political", in a sense that it would centre itself around the Party rule rather than the rule of law. Accompanying Hong Kong crackdown on defenders of the law is an even more outreaching approach in bar associations in several Mainland cities, where registered lawyers are required to submit a form listing all their social network accounts.

The HKNSL stirred considerable controversy and is seen as Beijing's war of authoritarian control over Hong Kong.[22] It is alarming because firstly, Hong Kong shall enjoy a high level of autonomy by maintaining a separate economic, judicial and political system. It is a special status under the Sino-British Joint Declaration[23], the so-called "One country, two

---

18 Law of the People's Republic of China on Safeguarding National Security of in the Hong Kong Special Administrative Region, 2020, art. 4

19 *Prosecution of the Hong Kong 47: Rule of law on trial*, HRIC, Apr.22, 2022, https://www.hrichina.org/en/press-work/hric-bulletin/prosecution-hong-kong-47-rule-law-trial.

20 *Ex-chief of Hong Kong Bar Assoc. reportedly meets with national security police,* HRIC, Mar.1, 2022, https://hongkongfp.com/2022/03/01/hong-kong-bar-assoc-ex-chief-paul-harris-receives-warning-for-allegedly-breaching-national-security-law/.

21 *Ongoing concerns on the situation in Hong Kong and the independence of the Bar Association,* LAWYERS FOR LAWYERS, Apr. 4, 2022, https://lawyersforlawyers.org/en/ongoing-concerns-on-the-situation-in-hong-kong-and-the-independence-of-the-bar-association/.

22 *Supra* note 19.

23 Joint Declaration of the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the People's Republic of China on the Question of Hong Kong, Dec. 19, 1984, art. 3.

systems" arrangement. The implementation of the HKNSL could serve as a preview of what spreading authoritarian regimes beyond borders might look like.

Secondly, as specified in the Declaration, Hong Kong's governing autonomy ends at diplomatic and defence matters which fall into the scope of national security, offering justification for HKNSL which ends up involving and compromising many essential human rights such as freedom of expression. It demonstrates a vulnerability where matters not conventionally considered to be related to national security could nonetheless be framed to be so.

Consequently, national security laws in both Hong Kong and Mainland China have succeeded in putting as many elements as possible under the "national security umbrella". The vague yet comprehensive provisions raise alarming concerns on rule of law status, as well as China's international obligations. While national security consideration is present in many jurisdictions, principles of legality, proportionality and necessity must be observed under international standards.[24]

C. Counter-terrorism Law

The enactment of the Counter-terrorism Law 2016 is a legislative continuum of the "Strike Hard against Violent Extremism" campaign 2014.[25] The campaign mainly aimed at a series of deadly terrorist events carried out by citizens of Uyghur ethnicity and was scheduled for one year.[26] The Counter-terrorism Law draws some light on how its provisions might have enabled, from both legal and technical perspectives, access to private communications

---

[24] *Supra* note 19.

[25] *The Ministry of Public Security launched a special campaign to crack down on violent terrorist activities*, XINHUA NEWS, May.25, 2015, http://www.gov.cn/xinwen/2014-05/25/content_2686705.htm.

[26] Including two terrorist attacks shortly preceding the "Strike Hard" campaign, killing 39 and injuring 94 in Urumqi, capital city of Xinjiang Province, *See* Urumqi attack kills 31 in China's Xinjiang region, BBC NEWS, May.23, 2014, https://www.bbc.com/news/world-asia-china-27502652; Train station mass knife attack in Kunming, capial city of Yunan Province, killing 31 and injuring 141, *See Scores dead in mass knife attack at Chinese train station*, FRANCE 24, Mar.1, 2014, https://www.france24.com/en/20140301-china-knife-attack-train-station-kunming.

which became exceedingly disproportional in just a few years' time, as well as an increasingly empowered algorithm backed by the development of big data and artificial intelligence.

The Law requires[27] providers of internet and telecommunications services to fully cooperate with the government in monitoring information passing through their networks, and handling over access or interface information and decryption keys[28]. Non-compliance would result in punishment including fines and detention of companies' employees[29]. The Implementation Methods of the Law further requires a real-name registration system enforced on delivery, telecommunications, internet, finance, hotel, long-distance bus, and rental car companies.[30] This legal obligation, especially that on internet companies, predates the Cybersecurity Law. May one assume that, similar to the algorithm and big data technologies developed following the Counter-terrorism Law, Xinjiang (even incidentally) served a testing field for the legislative measures for a real-name registration system across the whole country?

Nonetheless, the idea of a real-name registration requirement online had been advocated in as early as 2002 by a professor at Tsinghua University and was subsequently abandoned amid wide criticisms from the netizens[31], as well as the professor's own admission that such a requirement would be unrealistic through both law and technology.[32] This last concern is no longer true today.

---

[27] The final version does not contain "installing security backdoors" which was proposed in the drafts.

[28] Counter-Terrorism Law of the People's Republic of China, 2016, art. 18, 19.

[29] *Id.* art. 84.

[30] Xinjiang Implementation Methods of the Counter-Terrorism Law, 2016, art. 19, 20.

[31] Apart from netizens' reproaches, prominent professors such as Prof. Guoji Jiao from Peking University criticised such pre-assumption that online commentators were immoral liars; Prof. Xiaozheng Zhou from Renmin University said the history was reversing Prof. Gangjian Du of National Academy of Governance considered that an internet real-name requirement lacked basic legal common sense and violated Constitutional rights such as free speech, *See The truth behind Li Guangxi Incident,* SINA NEWS, June 6, 2003, http://tech.sina.com.cn/me/2003-06-06/0007195125.shtml.

[32] *Who gave Shenzhen the right to enforce real-name registration?* SOUTHERN METROPOLIS DAILY, July 28, 2005, https://m.aisixiang.com/data/7789.html.

Although with the knowledge of today, all these measures fall into the State's overall endeavour to build its techno-censorship base. Yet it was unclear and little contested among citizens. With the benefit of hindsight, such obligations imposed on service providers may at first seem to solely serve the purpose of fighting terrorism, yet as we later became aware of, this invasive technology practice backed by legal instruments has given the State growing surveillance capabilities to extensively monitor and suppress ordinary communications between and among Chinese citizens, "terrorist" or not.

D. Cybersecurity Law

Effective as of June 2017, the Cybersecurity Law (CSL) is the cornerstone codifying existing rules imposed on the Chinese internet and displays China's ambition to regulate its cyberspace full-scale, particularly the online content. Under the CSL, internet service providers (ISP) are required not only to strictly monitor content posted on their platforms by removing the "illegal content", but also to report users who published such content to the government as well as to provide technical support to the latter in investigating such "illegal activities".[33]

The element of anonymity is a unique quality of the cyberspace and used to be a safe net to express dissent opinions in authoritarian states. This element has been eliminated by the CSL that obliges ISPs to register users under their real identity as a condition to continue providing network service[34]. The mechanism can effectively make netizens self-censor each time before they speak and is seen to have little connection with cybersecurity.[35] The "real name provision" is further elaborated by follow-on regulations on online forums.[36]

---

[33] Cybersecurity Law of the People's Republic of China, 2017, art. 48, 28.

[34] *Id.* art. 24.

[35] *A closer look at China's cybersecurity law - cybersecurity, or something else?* ACCESS NOW, https://www.accessnow.org/closer-look-chinas-cybersecurity-law-cybersecurity-something-else/.

[36] Provisions on the Administration of Internet Forum Community Services, 2017, http://www.cac.gov.cn/2017-08/25/c_1121541921.htm.

Freedom of expression is intertwined with the right to be informed. Without access to information from a variety of sources, there is little opinions to be formed and expressed. As a vivid example of codification to support the Great Firewall, the CSL stipulates that access to information outside Mainland China that is "inconsistent" with Chinese laws shall be denied. The authorities are also entitled to disrupt network communications should the latter be deemed to unsettle national security or social order.[37]

The CSL grants the Cybersecurity Administration of China (CAC) extensive authority. In an interview, the CAC answered journalist's questions regarding what constituted illegal content.[38] The enforcement was significant – just the summer following CSL's entry into effect, the CAC revoked over 3,918 licenses to operate websites for not fulfilling their censorship duties.[39] Even internet giants such as Tencent, Sina and Baidu[40] also went under investigations by the CAC that same summer.[41] Moreover, CAC issued subsequent rules to restrict production and distribution of online news and orders all platforms to be supervised by party-sanctioned employees.[42] One year later, in 2018, the same authority introduced additional rules to punish both the platforms and the individuals for "falsifying history of the Communist Party".[43] Most recently, the CAC initiated an action called "Clear 2022 Comprehensive Governance of Algorithms" for the purpose of censoring

---

37 *Id.* 58.

38 However, the forbidden items are so broad and vague that any criticism of the government could fall into one of the categories. *See* interview scripts in Chinese: http://www.cac.gov.cn/2017-08/25/c_1121541845.htm.

39 Adam Pan, *China's Cybersecurity Administration cracks down on free speech,* MEDIA FREEDOM & INFORMATION ACCESS CLINIC, Oct. 19, 2017, https://law.yale.edu/mfia/case-disclosed/chinas-cybersecurity-administration-cracks-down-free-speech.

40 Tencent operates WeChat, the biggest Chinese language messaging application; Sina operates Weibo, a twitter-like online forum; Baidu operates Tieba, China's biggest BBS-like communication platform.

41 Charlotte Gao, China Accuses Its Top 3 Internet Giants of Potentially Violating Cybersecurity Law, Aug.12, 2017, https://thediplomat.com/2017/08/china-accuses-its-top-3-internet-giants-of-potentially-violating-cybersecurity-law/.

42 *China tightens rules on online news, network providers,* REUTERS, May. 2, 2017, https://www.reuters.com/article/us-china-internet-censorship-security-idUSKBN17Y0Y6.

43 Cate Cadell, *China robot censors crank up as Tiananmen anniversary nears*, REUTERS, May 26, 2019, https://www.reuters.com/article/us-china-tiananmen-censorship/chinas-robot-censors-crank-up-as-tiananmen-anniversary-nears-idUSKCN1SW03Y.

online platforms with significant capacities in mobilisation or changing public opinions, as well as pushing internet companies to transmit "positive energy" and censor illegal content using algorithms.[44]

There is a curious chain of regulatory pressure to be observed in this instance. Shortly before the crackdown, the CAC was publicly criticised by the Party for failure in safeguarding political stability. Subsequently, the CAC imposed harsh measures on any internet companies that managed online content. Finally, Chinese netizens were the ones to endure the outcome of an online environment with disproportional and hypersensitive censorship.

2.2.2 New Data Security Laws

The most recent legislative development in the Chinese cyberspace is the enactment of the Data Security Law 2021 (DSL) and the Personal Information Protection Law 2021 (PIPL). In the midst of global legislative waves in data protection, both laws put forward more detailed responsibilities on business parties in terms of processing users' data and restrict free flow of data in extraterritorial scenarios.

Nonetheless, PIPL is worth a closer inspection as it sets out specific provisions regulating the government's treatment of data, rather than solely that of the companies. Section III of the PIPL provides for rules of conduct imposed on State organs in handling personal information, such as the requirement of "necessity for the scope of statutory duties and responsibilities of the State organs" for the extent of handling personal information.[45] Prior notification duties are also stipulated in processing personal data, although the said duties may be easily waived if the notification itself would "impede State organs' fulfilment

---

[44] Notice on Launching the Clear 2022 Special Action on the Comprehensive Governance of Alg orithms, Apr. 8, 2022, https://www.chinalawtranslate.com/en/special-action-on-algorithms/.

[45] Personal Information Protection Law of the People's Republic of China, 2021, art. 34.

of their statutory duties and responsibilities",[46] or when confidentiality or emergency is in question. Or simply, when laws or administrative regulations provide that notification is not necessary[47].

Innovative and perhaps even revolutionary in its legislative attempt to regulate the State which is usually a silent party, PIPL is still limited in its capacity to clarify the State's power and its relation with citizens in the latter's privacy rights. The duties imposed on the State organs are concentrated on the handling of personal information already acquired, such as prohibition of unlawfully selling it to third parties or disclosing it without due process, but not on the grounds of the collection of such information. Moreover, PIPL contains rather vague languages in restricting the State organs which will not only render enforcement difficult, but also raise questions to the existence of any cause of action given the broad array of exceptions in Articles 18 and 35. Therefore, one may speculate that PIPL, as a legislation in the field of privacy, would form part of a larger regulatory framework which constrains the State on the one hand and empowers it on the other hand.[48]

A review of laws related to the paper's subject has illustrated legal and policy grounds devised to support the Chinese government's vision of what its cyberspace should resemble. Vast legislative moves also suggest the government's appreciation in the legitimating power of law.[49] The State allows zero compromise in matters pertaining to national security and delegates substantial responsibilities to ISPs to closely manage online speech, even when the majority of censored content had little to do with national security.

---

46 *Id.* art. 35.

47 *Id.* art. 18.

48 Jamie P. Horsley, *How will China's privacy law apply to the Chinese state?* NEW AMERICA, Jan. 26, 2021, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/how-will-chinas-privacy-law-apply-to-the-chinese-state/.

49 Jamie P. Horsley, *Party leadership and rule of law in the Xi Jinping era,* GLOBAL CHINA, Sept. 2019, https://law.yale.edu/sites/default/files/area/center/china/document/horsley_china_party-_legal_development.pdf.

This limitation of legal tools is rather recurrent[50] in the Chinese context where legislation is made to justify certain State's behaviours, while such legislation is exceedingly unspecific and disrupts the balance between the so-called national security and basic human rights to a point that benefits do not outweigh harm.

[50] *See* e.g. Donald Clarke, *No, New Xinjiang Legislation does not legalize detention centers*, LAWFARE, https://www.lawfareblog.com/no-new-xinjiang-legislation-does-not-legalize-detention-centers.

III. The Role of Technology

With a legal framework designed to support the digital censorship regime, this section will elaborate on the evolving technologies that make techno-authoritarianism efficient. The following will address specific mechanisms to the effect of limiting online speech, private actors making such limitation successful, and the situation of netizens' resistance using technology in return.

3.1 A Three-Step Mechanism

Online censorship to limit free speech is achieved by employing technologies aimed at three cumulative effects. First, it uses blocking mechanisms to deter access to outside information which is considered as contradictory to the government's narrative; Second, it employs filtering tools to monitor and delete content posted on the Chinese internet, notably social network; Third, it retains services to manipulate comments online to guide public opinion.

A. The Evolution of the Great Firewall and Similar Tools

While the Great Wall of China was built by slave labour more than 2000 years ago to deter Eurasian nomads, the Great Firewall[51] has been construed by today's computer engineers at government requests to deter their fellow citizens. Unintended as it might be, the very first email sent in China in 1987 was titled "Across the Great Wall we can reach every corner in the world."[52] Being one of the most notorious censorship tools, the Great Firewall is a diverse arrangement of legislative and technological endeavour to block access to a wide selection of foreign websites.

---

[51] The first printed use of the term "Great Firewall of China" dates back to a 1997 article, *See* S ang Ye and Geremie R. Barmé, *The Great Firewall of China*, WIRED, June 1, 1997, https://www.wired.com/1997/06/china-3/.

[52] Jaime A. FlorCruz & Lucrezia Seu, *From snail mail to 4G, China celebrates 20 years of Internet connectivity*, CNN, Apr. 24, 2014, https://www.cnn.com/2014/04/23/world/asia/china-internet-20th-anniversary/index.html.

Fang Bingxin, the notorious "father" and architect of the Great Firewall, defended the mechanism by arguing that "invisible enemies abroad sit comfortably at home, thinking only of how, through their fingertips on a keyboard, they can bring chaos to China."[53] Arguments as such continue to focus on national security concerns which are deemed by policy makers and their collaborators to outweigh the right to information. This argument was further advanced by poorly regulated international cybersecurity environment such as cyberattacks initiated by private parties and/or foreign governments. An example would be the security exposure to the United States, when its National Security Agency's (NSA) former contractor Edward Snowden revealed that the U.S. hacked Chinese mobile phones and universities.[54]

Another tool called the "Great Cannon"[55] was introduced in 2015 to disrupt and deluge foreign websites in order to take them offline by manipulating traffic. This technique is also able to redirect and replace specific content not favoured by the government. The coding and software development site GitHub underwent a distributed denial-of-service attack powered by the Great Cannon which caused the site to take down the Chinese version of The New York Times and GreatFire.org.[56]

The most well-known corporate victims of these blocking technologies include Facebook and its subsidiaries, Twitter, YouTube, Google and its associated services[57], Wikipedia and

---

[53] Evan Osnos, *Why China let Snowden go*, THE NEW YORKER, June. 23, 2013, https://www.newyorker.com/news/evan-osnos/why-china-let-snowden-go.

[54] Kenneth Rapoza, *U.S. hacked Chinese universities, mobile phones, Snowden tells China press*, FORBES, June. 22, 2013, https://www.forbes.com/sites/kenrapoza/2013/06/22/u-s-hacked-china-universities-mobile-phones-snowden-tells-china-press/.

[55] The term "Great Cannon" was coined by the University of Toronto's Citizen Lab, which produced a detailed report explaining the new tool, *See* https://citizenlab.ca/2015/04/chinas-great-cannon/.

[56] Sebastian Anthony, *GitHub battles "largest DDoS" in site's history, targeted at anti-censorship tools*, ARSTECHNICA, Mar. 30, 2015, https://arstechnica.com/information-technology/2015/03/github-battles-largest-ddos-in-sites-history-targeted-at-anti-censorship-tools/.

[57] It should be clarified that Google, like LinkedIn, decided to exit China market instead of being blocked behind the Great Firewall, as a result of no longer being able to observe the tightening local laws. For a

approximately all major foreign press, which are all platforms that constitute an important part of daily life in the digital age. Although this situation seems to have been there since the introduction of internet to China, it was not the case a little more than a decade ago. The mainstream websites listed above only started to be inaccessible starting 2009, before which Chinese netizens enjoyed an unprecedented freedom of information.[58] The situation escalated from 2012.

As of October 2021, LinkedIn, the last major U.S. social network then still operating in China, announced its decision to shut down its platform in the country, pushing China-based professionals and academics further away from being connected to international opportunities and exchanges. The decision followed CAC's request earlier in March to moderate its social networking content within 30 days.[59]

B. A Multi-billion RMB Industry of Filtering

If one considers blocking foreign websites as the cover page of the handbook for digital authoritarianism, then the complex filtering mechanisms would be its substantive chapters. From *ex ante* to *ex post* removal of publications, from human censors to AI censors, targeting from keywords to visual content, the technologies backed by their enabling factors[60] have essentially construed a formidable instrument that stymies freedom of expression.

As stipulated in Cybersecurity Law 2017, ISPs have legal obligations to censor content published on their platforms. Over the years, companies have developed advanced

---

review of LinkedIn's series of attempt in abiding by various censorship requirements, *See* https://mindmatters.ai/2021/10/linkedin-says-goodbye-to-china/.

[58] Li Yuan, *A Generation Grows Up in China Without Google, Facebook or Twitter*, THE NEW YORK TIMES, Aug. 6, 2018, https://www.nytimes.com/2018/08/06/technology/china-generation-blocked-internet.html.

[59] Liza Lin, *Microsoft folds LinkedIn social media service in China*, THE WALLSTREET JOURNAL, Oct. 14, 2021, https://www.wsj.com/articles/microsoft-abandons-linkedin-in-china-citing-challenging-operating-environment-11634220026?mod=djemalertNEWS.

[60] Namely rules and policies as discussed in Section II, as well as the indispensable "little" elves also known as tech companies explained in "Actors" below.

algorithms to analyse and remove content. Despite swift development in artificial intelligence and big data technologies, online filtering remains an important industry employing over two million people known as "internet public opinion analyst" as of 2013 and the talent market was said to be growing by 50% annually.[61] In 2018, the industry was said to worth tens of billions of RMB according to People's Daily. These opinion analysts are employed to manually monitor content published online and send questionable ones to the decisionmakers for possible removal. As a result, countless posts and original articles disappeared from the Chinese internet on the grounds of fraud, spam, pornography and politically sensitive subjects. Since the Covid-19 outbreak, there has also been an abusively increasing portion of content takedowns framed as disinformation, even though they very often end up being the truth.[62]

WeChat censors not only content published in Moments,[63] but also messages in private conversations between users. Regarding the latter, all messages are first sent to WeChat's server, where they undergo a review procedure, then are either sent to the recipient or intercepted depending on whether any specific message contains blacklisted keywords. If a message fails to deliver, neither the sender nor the recipient will see a notification to this effect. This mechanism to silence the speaker who does not even know to have been silenced significantly hinders the quality of a conversation and demonstrates how technology is being used so accurately to control not just what *cannot* be said, but to such an extreme so as to dictate what *will not* be said.[64]

---

[61] Michelle Fong & Jennifer Cheung, *If you like killing time on social networks, China has a job for you,* THE WORLD, July 31, 2014, https://theworld.org/stories/2014-07-31/if-you-killing-time-social-networks-china-has-job-you.

[62] AFP, *Shanghai social media unpicks China's virus lockdown story,* FRANCE 24, Apr. 7, 2022, https://www.france24.com/en/live-news/20220407-shanghai-social-media-unpicks-china-s-virus-lockdown-story; Nectar Gan, *Shanghai declares zero-Covid milestone but residents cast doubt on reopening*, CNN, May. 17, 2022, https://www.cnn.com/2022/05/17/china/china-covid-shanghai-reopening-intl-hnk/index.html.

[63] The social networking function of WeChat can be roughly seen as the equivalent of Facebook feed where one shares content such as texts, photos and articles with people of the friends list.

[64] Miles Kenyon, *WeChat surveillance explained,* THE CITIZEN LAB, May. 7, 2020, https://citizenlab.ca/2020/05/wechat-surveillance-explained/.

The same absence of notification also occurs in original publications, i.e., texts and images, in Moments. On the posting user's side, the post is successfully published and shows in the feed, but it is invisible to other users. WeChat's AI capacity to analyse images is remarkable as it recognises not only texts containing blacklisted words, but also photos indicating a historical event. As such, a photo of the Tiananmen square will likely be censored if it was posted near June 4.[65]

Human interference can no longer satisfy this magnitude of censorship. To be equipped with such broad yet precise analytical capacity, WeChat uses monitored content to train its censorship algorithm. One method being used is to flag a file's MD5 hash, which is a digital fingerprint, and future content similar to the flagged ones will be censored as well.[66] In addition, WeChat surveillance system is also the only system that monitors content sent by one set of users to enhance censorship on another set of users.[67]

C. Manipulation of Information

The censorship mechanisms developed by ISPs stop *speeches* from being made via removal of sensitive speeches *ex ante* or *ex post*. A step further into the grand design of restricting free speech is to stop "incorrect" *opinions* from being formed, hence eradicating expressions thereof by the roots. Like censorship, manipulation of information online is also achieved by joint effort between humans and robots.

The chosen narrative of events, historical or current, is central to understanding one's situation and forming opinions. For future historians, online content is history books in the process of being written. So how it unfolds and affects its audience are important for the ruling class. As soon as the power of online discussion was understood, a new job

---

65 *Supra* note 43.

66 *Supra* note 64.

67 Jeffrey Knockel et al., *We chat, they watch, how international users unwittingly build up WeChat's Chinese censorship apparatus,* THE CITIZEN LAB, May. 7, 2020, https://citizenlab.ca/2020/05/we-chat-they-watch/.

position was created which entails commenting and guiding online discussions in politically appropriate directions. In 2004, universities were called upon to hire students to identify political dissenting content and comment on them with Party-friendly views.[68] Those commentators later became known as the 50 Cent Army, as they were paid little to be engaged in this job. This Army quickly expanded to employees outside the universities.

The technology to automatically manipulate content online, or an AI opinion leader,[69] is relatively immature compared to that of censors. A recent incident on Baidu Tieba shows that a certain swearword (which had previously been banned) will be automatically modified and another word will appear in the publication.[70] It could be understood as autocorrect occurring in the air. The change is done at the server's level and not the user's end. This new development is regarded by some to be more frightening than simply censoring sensitive words as now one's speech online can be altered by someone (or somebot) other than the speaker himself.[71] Similarly, users have discovered that their Sina Weibo account had been sharing pro-Party posts after not logging in for a certain period of time.

3.2 Private Actors Powered by Technology

Although the government as lawmaker and executor is the main actor for controversial practices such as surveillance and restriction of online speech, two other important actors, namely technology companies and their users, also play a nonnegligible role in this calculation.

---

[68] *As Chinese students go online, little sister is watching,* THE NEW YORK TIMES, May. 9, 2006, https://www.nytimes.com/2006/05/09/world/asia/09internet.html?_r=2&pagewanted=all.

[69] Stephen Chen, *China's internet police losing man-versus-machine duel on social media,* SOUTH CHINA MORNING POST, Nov. 14, 2021, https://www.scmp.com/news/china/science/article/3155920/chinas-internet-police-losing-man-versus-machine-duel-social.

[70] So far, the feature is only updated to the app and not the web version. *See* https://posts.careerengine.us/p/61456619c24cd9749661ea3f.

[71] *See* https://www.zhihu.com/question/486851069/answer/2495021292.

A. Tech Companies – The Complicit Geniuses[72]

Curiously, the manner being used to describe domestic and foreign internet players in China are very different. While both cooperate with the government to limit free speech, the Chinese platforms are usually depicted as "the target of official scrutiny", while the foreign platforms are denoted as "complicit to suppress fundamental values". This differentiation is possibly due to these articles being generally written by western media who believe that non-Chinese internet companies have a choice and that they have chosen profits over values.

In October 2017, the U.S. Senate questioned Apple regarding the latter's censorship practice in China,[73] to which Apple replied that it had been practicing censorship because it must comply with local regulations, and that it was in the interest of a U.S. corporation to open up China.[74] The tech giant constantly removes apps related to sensitive matters or encrypted messaging from its China App Store.[75] It also admitted to have removed from its App Store 674 VPN apps in 2017 alone.[76] The company further compromised Chinese users' privacy rights by playing along with China's request to store Apple's Chinese iCloud decryption keys in a government-owned data centre, under the pretext of the Cryptography Law 2020. This makes Apple's pledge of safeguarding users' privacy and

---

[72] This subsection will focus on the role of international tech companies in China while analysis of the role played by domestic tech companies is elaborated in section 3.1 above.

[73] *See* Letter from the U.S. Senate to Tim Cook, Oct. 17, 2017, https://www.cruz.senate.gov/files/documents/Letters_/20171017_tim_cook_letter.pdf.

[74] *See* Letter from Cynthia C. Hogan, vice president for public policy for Apple Americas, to Senator Ted Cruz and Patrick Leahy, dated Nov. 21, 2017, https://www.leahy.senate.gov/imo/media/doc/Apple%2011212017.pdf.

[75] Felicia Hou, *Apple removes popular religious apps in China,* FORTUNE, Oct. 16, 2021, https://fortune.com/2021/10/15/apple-china-censorship-religious-apps-quran-bible/; *Apple censoring its app store in China,* TECH TRANSPARENCY PROJECT, Dec. 23, 2020, https://www.techtransparencyproject.org/articles/apple-censoring-its-app-store-china.

[76] Saheli Roy Choudhury, *Apple removes VPN apps in China as Beijing doubles down on censorship*, CNBC, Aug. 1, 2017, https://www.cnbc.com/2017/07/31/apple-removes-vpn-apps-in-china-app-store.html.

freedom of expression a hypocritic statement as it has practically given the Chinese government access to its users' data.[77]

Apple is hardly a pioneer in complying with the Chinese law at the expense of the rights of its customers to access the lucrative market where it earns a fifth of its global revenue. Google entered the Chinese market in 2006 with a censored version of its search engine. When the U.S. argued in 2010 that China's internet censorship was a violation of human rights, Microsoft sided with China when Bill Gates said "You've got to decide: do you want to obey the laws of the countries you're in or not? If not, you may not end up doing business there".[78] In that same year, China published a white paper titled "The Internet in China"[79] to defend its internet practices by stating that foreign companies must follow Chinese laws to do business in the country and that what was best for Chinese people was China's concern.[80] In hindsight, the second part was the prologue of China's initial claim of cyber sovereignty, a concept frequently appearing in international political and academic debates.

At the same time, it is alarming that some companies which previously exited China, have made attempts to return by developing specific projects that comply with Chinese censorship rules. Google had been developing its controversial Dragonfly Project, a search engine catering to censorship requirement specifically designated to the China market, up until its termination in 2019.[81] Facebook had been contemplating to re-enter the market

---

[77] Michael Caster, *Apple cares about your privacy unless you're in China,* ARTICLE 19, July 14, 2021, https://www.article19.org/resources/apple-cares-about-digital-rights-unless-youre-in-china/.

[78] *Bill Gates bats for China,* GLOBAL TIMES, Jan.27, 2010, https://www.mfa.gov.cn/ce/ceus/eng/xw/t654165.htm.

[79] *The internet in China,* June 8, 2010, http://www.china.org.cn/government/whitepaper/node_7093508.htm.

[80] Geoffrey Hoffman, *Cybersecurity norm-building and signaling with China* , IN GOVERNING CYBER SPACE, BEHAVIOR, POWER AND DIPLOMACY, 198, 187-204 (Dennis Broeders & Bibi van den Berg ed., 2020).

[81] *See* report series ranging from 2018 – 2019 by Ryan Gallagher, *Google Dragonfly,* https://theintercept.com/collections/google-dragonfly-china/. Rachel Kraus, *Facebook chooses values over profits in staying out of China*, MASCHABLE, Nov. 14, 2018, *see* https://www.mashable.com/article/facebook-no-china-service.amp.

through a deal of developing a censorship tool for the social network to operate in China.[82] However, its intention to establish a subsidiary in Hangzhou was rejected by the CAC in 2018, a few months before the company told the U.S. Congress that it would not provide service to China unless censorship is no longer on the table.[83] Would the story unfold differently had Beijing been a bit more friendly to Facebook? Would the company stay open for alternatives to enter the Chinese market like Google did?[84]

Global tech companies' complicity in strengthening a digital authoritarian regime sees its decadence in three phases. The most coherent attitude in returning to fundamental values such as freedom of expression is to exit the Chinese market as abiding by local laws would contradict its values; The less admired but reasonable approach is to operate under local laws to the minimum extent required in order to have access to the market; The unacceptable way is to proactively develop a censorship system that arguably goes beyond what is required by Chinese law to please the State, such as what Apple does with its App Store[85] and engraving services[86]. This proactive complicity is atrocious because tech giants are aware of the power they possess to help build a digital authoritarianism whose defeat is practically unimaginable as we enter deeper into the digital age.

B. Netizens – The Unfortunate Collaborators

One frightful effect of censorship is that it concentrates all information and power to the State and individuals lose trust between each other. The take-down practice is conducted

---

82 Mike Issac, *Facebook Said to Create Censorship Tool to Get Back Into China*, THE NEW YORK TIMES, Nov. 22, 2016, http://www.nytimes.com/2016/11/22/technology/facebook-censorship-tool-china.html.

83 Rachel Kraus, *Facebook chooses values over profits in staying out of China*, MASCHABLE, Nov. 14, 2018, https://www.mashable.com/article/facebook-no-china-service.amp.

84 Jeb Su, *Confirmed: Google terminated project butterfly, its censored Chinese search engine,* FORBES, July 19, 2019, https://www.forbes.com/sites/jeanbaptiste/2019/07/19/confirmed-google-terminated-project-dragonfly-its-censored-chinese-search-engine/?sh=4e8c72327e84.

85 *GreatFire asks apple about app stores management in China (Open Letter),* APPLE CENSORSHIP, May. 25, 2021, https://applecensorship.com/greatfire-asks-apple-about-app-stores-management-in-china-open-letter/.

86 Jeffrey Knockel & Lotus Ruan, *Engrave danger, an analysis of apple engraving censorship across six regions,* THE CITIZEN LAB, Aug. 18, 2021, https://citizenlab.ca/2021/08/engrave-danger-an-analysis-of-apple-engraving-censorship-across-six-regions/.

by human employees and AI, but the users feature to report violation helped perfectionate censorship. Members of the 50-cent-party regularly report online comments that violate the law. Private citizens are also encouraged to report content which they suspect to have violated some rules. Statistics show that the CAC accepted more than 166 million reports for illegal content in 2021.[87] As a result, one can often see a notice stating "you cannot review this content as it has been reported by multiple users" when trying to open an article. After a while, many people have developed a certain sensitivity of knowing whether an article will be censored just by reading its title or first lines and hence opt to race against the censorship.[88]

3.3 Resistance by Technology

A. The Crackdown of VPN and Exonerated Cases

Despite the Great Firewall and similar blocking tools, the internet remains the most essential channel for ordinary Chinese citizens to acquire information. Many use circumvention tools such as virtual private networks (VPN) to visit blocked websites and educate themselves, a practice rather unhindered till 2017 when massive waves of crackdown of VPNs took place as part of an ongoing campaign aimed at cleaning the internet.[89] As a result, the majority of websites of VPN subscription were blocked and VPN apps were removed from app stores.

Prior to the crackdown, it was uncomplicated to use VPN uninterrupted and for free. Nowadays one must pay for the limited options available. Therefore, apart from technological difficulties, it is also economically more burdensome for China-based netizens to use the internet. Ordinary people, among them academics and scientific researchers, were furious. Students threw eggs and shoes at the architect of the Great

---

87 CAC received nation-wise a total of 166 million reports on illegal and bad information in 2021. *See* http://www.cac.gov.cn/2022-01/29/c_1645059191950185.htm.

88 *See* Section 3.3 C.

89 Sherisse Pham, *China fortifies Great Firewall with crackdown on VPNs*, CNN, Jan. 24, 2017, https://money.cnn.com/2017/01/23/technology/china-vpn-illegal-great-firewall/index.html?iid=EL.

Firewall Fang when the latter gave a speech at Wuhan University in 2011.[90] Foreign companies, however, were exonerated from the VPN crackdown. The reason is quite straightforward as globalised corporate entities will not be able to operate without connection to the outside world.

B. Blockchain and NFTs

The rapid development of blockchain technology is challenging the censorship agenda as data sent via the blockchain network is encrypted and hence cannot be deleted or modified by censors. The decentralised database conserves information to be consulted on the blockchain, offering a counterweight to centralised power.

Since March 2022, China has been experiencing its worst Covid outbreak with Shanghai as the epicentre. As the first outbreak two years ago starting from Wuhan, massive censorship is being deployed to control information online such as criticism of the government, revelation of corruption and fake news, inhuman treatment of citizens, etc. So people use blockchain to preserve the part of history that they have experienced but is being erased on the internet. For instance, screenshots of a video[91] documenting people's sufferings under Shanghai's brutal lockdown measures were uploaded to the blockchain and then casted into non fungible tokens (NFTs).[92] A legal scholar's analysis of the legal and humanitarian disaster caused by the lockdown has also been permanently engraved into the blockchain, before it was removed by censors.[93]

C. Evade Censors – High Tech and Low Tech Methods

---

[90] Joshua Keating, *Great Firewall architect gets shoe'd and egg'd,* FOREIGN POLICY, May. 19, 2011, https://foreignpolicy.com/2011/05/19/great-firewall-architect-gets-shoed-and-eggd/.

[91] The video titled "The Voice of April" is available at: https://www.youtube.com/watch?v=oiiyll1i7zc.

[92] Eleanor Olcott, *Defiant Chinese netizens skirt lockdown censorship using blockchain,* FINANCIAL TIMES, May. 18, 2022, https://www.ft.com/content/3bbb2af3-e934-4603-8aae-26b758140c65.

[93] The original article is also available in overseas Chinese language website. https://yibaochina.com/?p=246371.

Additional techniques used by Chinese netizens include manipulating the appearance of information to evade censors, and this is truly a cat-and-mouse chasing game. It started with texts being presented as a screenshot to avoid keywords detection. Then censors gradually developed themselves to identify sensitive words in images as well. So now people would flip the screenshot upside down, or doodle on the image to confuse the algorithmic inspection, or both.

The above methods are employed when a certain topic has become the absolute priority and target of censorship under updating directives, usually for a specific period. In the ordinary course of web surfing, the more conventional way is to stick with posting the text but use another word with similar pronunciation in place of the blacklisted sensitive words.

Netizens have also used robots to fight their freedom of expression. Social media bots that imitate human behaviours often work in groups to generate and spread information online.[94] This "defeat magic by magic" approach[95] signifies increasing pressure on the censorship regime to upgrade its artificial intelligence as its target is turning from human beings to machines.

A more "crude" approach recently used during the 2022 Shanghai lockdown is to spell terrifying curses, in the comment section, on the human public opinion analysts who are censoring and deleting vital information. Such a comment always receives the highest number of "likes" by readers and is placed on the top of the comment section. Interestingly, as observed by netizens as well as the author, these articles stay online much longer than they are supposed to under the increased rigidity of censorship during this period.

---

[94] *Supra* note 69.

[95] It has been suggested by the Centre for Information Resilience that bot-like accounts have been created, primarily over western social media platforms, that post or share pro-China content. *See* https://www.bbc.com/news/world-asia-china-57780023 and https://www.nytimes.com/2022/02/18/technology/china-olympics-propaganda.html.

In the end, those attempts did not manage to entirely prevent censorship, which quickly caught up from behind. But this resistance did manage to safeguard the right to information of their fellow citizens for a little longer. Especially during China's second wave of Covid crisis, people have become more awaken at the value of right to information and freedom of expression. It causes censorship to operate less smoothly than it used to because even though information is short-lived and that it is a cat-and-mouse game, the number of cats is considerably outnumbered by the number of mice.

IV. LIMITATIONS AND CONSEQUENCES

Building on a review of the interaction between law and technology which render China's online surveillance, particularly in the field of freedom of expression, not only possible but also efficient, Section IV will analyse the adequacy of the legal framework by inspecting the Chinese government's reliance on cyber sovereignty and legislative works, inspected against the background of the current and arguably more disastrous Covid wave in the country, as well as additional risks for the development of human society.

4.1 The Question of Cyber Sovereignty

The concept of cyber sovereignty was brought forward by China in 2010 and has since then become a key response to growing criticism by foreign interested parties who were disappointed at the absence of political liberalisation and commercial openness which were expected to be brought by China's focus on developing information technologies[96].

Indeed, China took an opposite stance of what was proposed by John Barlow's 1996 Declaration of the Independence of Cyberspace,[97] where he claimed that the government should leave cyberspace alone over which it had no sovereignty. Out of instrumental distrust of the government, Barlow considered Cyberspace as the new home of Mind. The Party's understanding of cyberspace is also deviating from Kevin Kelly's Technium and the 7th Kingdom of Life, [98]where the chief effect of technology is that it produces more possibilities and more freedom, although the role of technology remains to be truly discovered.

---

[96] Rogier Creemers, *China's Conception of Cyber Sovereignty: Rhetoric and Realization*, IN GOVERNING CYBER SPACE, BEHAVIOR, POWER AND DIPLOMACY, 107-142 (Dennis Broeders & Bibi van den Berg ed., 2020).

[97] John Perry Barlow, *A declaration of the independence of Cyberspace,* 24 HOURS IN CYBERSPACE, Feb. 8, 1996, https://www.eff.org/cyberspace-independence.

[98] Kevin Kelly, *The Technium and the 7th kingdom of life,* EDGE, July 18, 2007, https://www.edge.org/conversation/the-technium-and-the-7th-kingdom-of-life.

The proposal of cyber sovereignty consists of non-interference by other states of one state's treatment of law and technology in its cyberspace. In the case of China, it largely refers to its regulatory regime of online behaviours, especially practices of surveillance and censorship, within its jurisdiction. Assuming such, issues of such practices will be reviewed from the perspective that a government should run the country with its own values and traditions without being constantly compared to the West.

A. Open Surveillance, Open Censorship

Perhaps the only certainty in all the opaque legal languages is that China is not vague in its resolve of censorship and surveillance. China does not hide the fact that it is monitoring its citizens, nor does it pretend to uphold freedom of expression the same way as Western countries. Liao Canliang, chief analyst at the People's Daily Online Public Opinion Data Center, said directly in a 2020 article that "The ultimate purpose of analysis and prediction is to guide and intervene in public opinion," and that "public data from social network users can be used to analyse the characteristics and preferences of users, and then guide them in a targeted manner."[99]

This is a stark contrast with the NSA up till the Snowden leak, which accidentally advanced the call for more internet control as Snowden revealed that the NSA hacked Chinese telecommunications companies, among others.[100] Compared to that of diplomatic relations, the consequences of unearthing NSA's spying practice were more severe on private parties, such as U.S. tech companies operating in China at the time when they

---

[99] Cate Cadell, *China harvests masses of data of western targets, documents show,* THE WASHINGTON POST, Dec. 31, 2021, https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html.

[100] Toby Helm et al., *Snowden spy row grows as US is accused of hacking China*, THE GUARDIAN, June. 22, 2013, https://www.theguardian.com/world/2013/jun/22/edward-snowden-us-china.

complained to President Obama regarding their heavy loss of customers,[101] as well as a grave decline of trust in government from the U.S. citizens.

B. Different Standards of Freedom of Expression

As elaborated in Section II, freedom of expression is a Constitutional right but is often shadowed by other overriding factors such as national security and public interest. As a matter fact, the level of protection of free speech differs even among democratic jurisdictions. Among many exceptions to free speech, the concepts of public interest and national security come at play under different capacities. For instance, in the U.S., free speech with its First Amendment status overrides almost any other consideration and it is so rarely placed on balance with a "compelling state interest".[102] While under the European Convention of Human Rights, the term is formulated as "necessary in a democratic society", which also entails "in the interest of national security, territorial integrity […][103]".

In China's case, such public interest refers largely to national security, and more specifically, the preservation of a socialist regime ruled by the Party. Several dispositions relevant to regulating China's cyberspace, especially the controversial ones pertinent to online censorship, all find their legal basis in arguments of national security. Consequently, technologies employed to satisfy the regulative goals constantly compromise fundamental human rights in a disproportionate manner. Where stands then the limitation of the national security argument?

C. A Priority on Collective Good

---

101 Cheng Li & Ryan McElveen, *NSA Revelations Have Irreparably Hurt U.S. Corporations in China*, BROOKINGS, Dec. 12, 2013, https://www.brookings.edu/opinions/nsa-revelations-have-irreparably-hurt-u-s-corporations-in-china/

102 For a discussion of this kind, *see* Michael Birnhack & Jacob Rowbottom, *Shielding Children: The European Way*, 79 CHI-KENT L. REV. 175 (2004).

103 European Convention on Human Rights, art. 10.

The role of the State, as opposed to that of individuals, is very dominant in China throughout its history. This is as true to the government as to the governed. The lack of emphasis on individuals is also demonstrated in a focus on advancing collective benefit and public goods. One reason for China's advocacy for cyber sovereignty could be explained by its dissenting belief of what is the most vital question at stake. For a socialist regime with a Confucian culture background, such vital question is rather communitarian than individual.

Therefore, China does not wish to be assessed in "their" terms, such as the European terms. As laid out by Dr. Rogier Creemers that, while the EU continuously pays attention to what China is not doing, it should give credit to China for what the EU is not doing. While the EU focuses on protecting personal interest, such as privacy and other fundamental human rights against harm, China prioritises protection of public interest and national security, namely cyber infrastructure, industrial data, natural resources as detailed its data protection laws. It is a pioneer in including those areas into serious data security concern as well as in trying to diagnose and understand the externalities of what full spectrum digitalisation brings to social, economic and political life. [104]

Chinese individuals had also exhibited less reluctance in the government's practice reflecting digital authoritarian features. Covid 19 is a catalyst for China to expand drastically its employment of surveillance technologies on its citizens. By the time such technologies appeared necessary for the country's anti-covid policy, they were timely ready to be massively employed as a result of decades of refining data collection and algorithm training. Unlike in most Western jurisdictions, such an intensification of digital surveillance received little opposition from Chinese citizens who saw the involvement of such technologies justified for the greater good of fighting against the pandemic.

---

[104] Webinar: China's Tech Landscape, Feb 11, 2022 by China Research Group, *available at*: https://www.youtube.com/watch?v=CqP16drqXNc.

Some studies suggest that such an attitude is based on three socio-political aspects of the Chinese society: the popularity of the guardian model of governance, a communitarian tradition with less concern over individual rights, and a belief that technological development is intertwined with national rejuvenation.[105] The guardianship and communitarian features are also observed in other Asian countries with a Confucian culture background, such as Singapore.[106] The link between technology and reviving the state is however less evident as such specific aspiration is not necessarily shared among Chinese citizens depending on at least three elements. First, it depends on one's proximity to the State which holds such a vision; Second, it is related to one's place in China's demography as fast development of technology is not only less relevant for the elderly population, but also make their life harder due to inability to catch up with the vast application of digital payment, online shopping, health QR code, a problem that became more exposed during 2022 Shanghai lockdown; Third, one's professional background is implicated as whether it relies heavily on a traditional ecosystem or that of high-tech.

On the other hand, the attitude towards online censorship, which is another digital authoritarian feature, is less harmonised than that towards surveillance. Certainly, indifference towards inability to access a substantial amount of the cyberspace could be common among millennials.[107] Nevertheless, the Covid crisis has made netizens realise the cost of having their right to information and freedom of expression deprived, although the real cost is significantly more serious.

---

[105] Jun Liu & Hui Zhao, *Privacy lost: Appropriating surveillance technology in China's fight against COVID-19*, 64 BUSINESS HORIZONS, 744, 743-756 (2021), https://doi.org/10.1016/j.bushor.2021.07.004.

[106] Victor Cha, *Asia's COVID-19 Lessons for the West: Public Goods, Privacy, and Social Tagging*, 43 THE WASHINGTON QUARTERLY, 1-18, https://www.tandfonline.com/doi/full/10.1080/0163660X.2020.1770959.

[107] *Supra* note 58.

4.2 Legislation by Convenience

Section II provided for a simplified elaboration of China's legal framework to roadmap the most recent and pertinent aspects regulating the current surveillance state, although the body of rules related to online speech and surveillance is immense yet disperse. It is reasonable to regulate behaviours in cyberspace vis-à-vis physical space because it is important to anticipate possible risks in the cyberspace which more and more resembles the physical world. Metaverse would be one example, although its very concept and meaning are debated. The fact that the online community could transform and merge with the real one[108] calls for government's concerns.

Nevertheless, the problem of heavy regulation in contrast with its inconsistent enforcement is deeply rooted in what the author would call a "legislation by convenience". The concept is three-fold. First, it refers to enacting laws to oblige people to assist the government in achieving the latter's aim more easily while it already has the technological means to do so; Second, it suggests a heavy reliance on enacting laws to compel people to help realise the government's goals, even when the legislation is immature.

A. Legislation to Alleviate Authorities' Work

The current legal framework, as complex as it is, reflects a governing style where it is already possible for the ruling class to achieve an end via technological and/or administrative means, yet it still chooses to enact as many laws as possible where it sees convenient, to make execution easier for enforcement departments.

---

[108] *See* examples of 2012 Beijing flood, 2011 Wenzhou high-speed train accident and 2009 Deng Yujiao case presented in Elizabeth C Economy, *The great firewall of China: Xi Jinping's internet shutdown*, THE GUARDIAN, June 29, 2018, https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.

To understand with the example of real-name registration, technically it was already possible for the police to know who posted what and track down IP addresses, yet the requirement to register one's real identification at various internet forums was codified in law because it would make the police's job even easier as personal information of online content authors would be immediately available in their hands due to obligations of the ISPs. In this way, the police are capable of doing their job more efficiently, and the scope of control hence becomes much wider.

Similarly, the tracking system designated to fight Covid 19 also demands a large proportion of self-reporting of one's itineraries as well as persons of close contact, although the government possesses the tools to find out about such information on their own. For instance, the colour of one's health code would automatically turn yellow, or itinerary code would be marked with an asterisk, if one has passed by a location exposed to covid case(s), and therefore becomes restricted in his next movements. The big data accomplishes it all, yet citizens are still obliged by law to voluntarily report online (and offline as may be required by many local governments) when they travel to another city, the failure or inaccuracy of which could result in criminal punishment. Such a legal obligation to disclose constantly one's whereabouts has significantly helped ameliorate the overall infrastructure and training of big data, thereby enhancing the performance of surveillance practice.

B. Substantial Reliance on Enacting Laws

In terms of excessive reliance on legislative activities, the increase of laws aimed at regulating the cyberspace provides a vivid example of relying on making laws with the hope of achieving the government's vision of orders in the cyberspace. This is especially true under President Xi's incumbency, as "law-based governance" has been made a cornerstone of the Party's governance strategy.[109] The problem is that law tends to lag behind technology, and it is premature to heavily regulate matters without a thorough assessment

[109] *Supra* note 49.

and reasoned analysis of their risks. China's current problem is no longer the absence of laws because there are too many[110], but the fact that those laws are not aligned in many ways and that they solve one problem by creating more problems. The power of law is overrated when it merely reflects the will of the few.

Therefore, legislation by convenience excels at codifying and even criminalising behaviours with a catch-all vision. It reflects not so much as a legislative activeness as it is a governing laziness, when most punished cases cannot find their basis in substantive provisions but only in the catch-all provision. For instance, the crime titled "Picking quarrels and provoking troubles" is a well-known "pocket crime" in Chinese criminal law, mostly when arrests and convictions do not find grounds in other provisions of the law.[111] During the first wave of Covid 19 outbreak, i.e., the first quarter of 2020, 897 penalised cases of online speech were documented. 93% of them were punished for "spreading misinformation" and/or "disrupting public order".[112]

Online censorship follows this same logic. The State is entitled to punish those that have actually committed a crime such as regime subversion or other behaviours harming national security. But it is unreasonable to imagine that a technology could be used to commit such a crime, and subsequently ban the enjoyment of a substantial part of the said technology, as the State did to the internet. Nor is it reasonable to deprive the entire population its fundamental rights such as privacy, information and expression, just because it is foreseeable that a minority would abuse these rights.[113] By not allowing free

---

110 Dalin Fu, *A real rule of law society should cure the symptom of legislation dependency,* ZHONGJIAN PRESS (PROSECUTORS DAILY), June 6, 2012, http://www.jcrb.com/opinion/zywy/201206/t20120606_877453.html.

111 Stanley Lubman, *'Picking quarrels' casts shadow over Chinese law*, THE WALL STREET JOURNAL, June. 29, 2014, https://www.wsj.com/articles/BL-CJB-22915.

112 *"A Healthy Society Should Not Have Just One Voice" – China Must End Crackdown on Online Speech in Response to Covid-19*, CHRD, Apr. 1, 2020, www.nchrd.org/2020/04/a-healthy- society-should-not-have-just-one-voice-china-must-end-crackdown-on-online-speech-in-response-to-covid-19.

113 Ping Chang, *Mandatory real-name registration online: is it really necessary?* SOUTHERN METROPOLIS DAILY, July. 25, 2005, http://news.sina.com.cn/o/2005-07-25/09346521549s.shtml.

discussions and free flow of information, the cyberspace is effectively deprived of its most valuable features.

C. Direct Consequences of Legislative Reliance

This legislative style affects significantly a certain governing style of local governments, as well as the managing style of tech companies. Because of overwhelming legislation from the central government, local governments and institutions are responsible to implement the rules while dealing with complex matters generated by diverse real-life situations. During various waves of Covid-19, local governments always introduce stricter measures in order to ensure non-violation of Beijing's rules and pandemic fighting goals. This ends up fulfilling Beijing's requirement (and keeping one's job in the world's biggest bureaucracy) at the cost of creating more problems. Sometimes devastatingly, the cost is citizens' life.

As for tech companies, their managing approach has been deeply influenced as well in censoring sensitive content published on their platforms as they, manually or automatically, tend to delete content that is only remotely related to sensitive topics, or simply by mistake. The cost are users' right to be informed and possibilities to make more appropriate decisions. One of the biggest consequence is what later came to be known as our lifetime's biggest pandemic crisis, which spread rapidly across the country and soon the whole world, because Dr. Li Wenliang's message, among others, was censored.

4.3 The Limitations of Cyber Sovereignty and Legislative Reliance

As argued in 4.1 above, under the claim of cyber sovereignty, China shows how its cyberspace is governed differently from the West, such as its straightforwardness in conducting digital surveillance and online censorship, how limitations of fundamental rights such as privacy and free speech are respected differently across jurisdictions, and a favourable position from the State as well as individuals on collectivity and public benefit. However, if the argument stops each time at cyber sovereignty, as advocated by China and

some other states, as well as supported by certain global tech giants over the decade, we would then obtain a flawed approach of legitimising or otherwise acquiescing in government practices that are inacceptable in democracies.

One of the flaws is interwind with the inherent defect of a reliance on legislative activities, as argued in 4.2, to impose a will of order which exposes abuses from lawmakers and enforcement. Another is the endless violation of human rights extended to other aspects of the society.

A. Existing Social Issues Deteriorate Under Cyber Sovereignty

Under digital authoritarianism, technology does not solve problems. It hides the problems and creates some more. The call for cyber sovereignty under the circumstances of unlimited state power would generate substantial disasters of human rights and social injustice which are more easily accomplished with technology.

The Open Trials policy since 2016 where court proceedings are broadcast live and recorded is widely seen as an applaudable judicial reform.[114] People are led to believe that court transparency is greatly enhanced thanks to technology while not paying attention to how such technology can be easily manipulated. For instance, as is in practice, judges turn off the microphone when they are not following certain fundamental professional conduct. They also tend to use a recess to converse with the plaintiff and the defendant separately outside the court room, sometimes in blatant violation of the law, such as bluffing or telling a party that she will rule against the party if the latter does not do or say certain things. None of these will be recorded on camera or audio, so there will be no evidence to complain about the injustice coming directly from the judicial body. Yet, people will think that court transparency is significantly improved, when the reality is quite the opposite.

---

[114] Guodong Du et al., *You can watch trails in Chinese courts on the internet now,* CHINA JUSTICE OBSERVER, May 20, 2018, https://www.chinajusticeobserver.com/a/you-can-watch-trials-in-chinese-courts-on-the-internet-now.

Online censorship worsens its offline equivalent of the situation by making even private conversations insecure as the ISP servers are watching for the government. The practice filters and manipulates information so that only a certain narrative is available to citizens. Yet this will unlikely make the majority feel ignorant exactly because we live in a digital age with an explosive amount of information. So we absorb information constantly without actually being informed because our freedom of conscience is taken. Once more, technology, in this case the internet, does not solve the problem of limiting free speech. Instead, it hides free speech as well as information that would cause the kind of speech disliked by the authority.

Another shortcoming of cyber sovereignty lies in the argument which overwhelmingly assumes that attempted interference comes from foreign governments and companies because the latter are dissatisfied with China's practice in the cyberspace, without taking into account of domestic complaints which, together with "foreign interference", suggest the controversial nature of using law and technology to more efficiently monitor the governed and restrain the rights to information, to free speech and to privacy. The belief that Chinese citizens do not have a problem with such practices for cultural or social political reasons is naïve and lacks factual support.

Even for periods outside of the two largest waves of Covid,[115] people's movement has been severely restricted because of the health code system powered by big data, which marks the code yellow if you have merely passed by certain areas with Covid cases in the past 14 days. People have been pocessed by a brand-new conscience where they check constantly the colour of their health code, hoping it stays green to avoid compulsory

[115] Namely the first one in the first quarter of 2020 with Wuhan as the epicentre, and the second one from March 2022 with Shanghai as the epicentre. Both experienced harsh lockdowns and humanitarian crisis.

quarantine. During the Wuhan and Shanghai lockdowns, the problems of online surveillance and censorship emerged more intensely, with daily cat-and-mouse chase between netizens and ISPs targeting vital information. The claim on cyber security is not accepted by Chinese people who are in a constant race with censorship only to stay minimum informed.

Human right is a universal right and ought to be treated equivalently despite different governing styles or values. Compromising one seemingly less esteemed human right will result in the deprivation of many other rights as showcased in China's Covid crises. For instance, being able to exercise the right to privacy is important for the realisation of other fundamental rights, such as the freedom of opinion and expression[116]. Moreover, surveillance capabilities and the assumption that Chinese citizens care little about their privacy rights have led to a full invasion into citizens' private life where personal data collected are routinely used to achieve the State's policy ends.[117]

Power is insatiable by nature and it will become extremely formidable when equipped with technological and legal tools. The reason why Harari believes that technology favours tyranny is that technology makes centralised information more valuable than diffused systems. In the end, the conflict of between democracy and authoritarianism is actually "a conflict between two different data processing systems," and that "AI may swing the advantage toward the latter." [118]

B. Legislative Reliance Leads to Rule by Law

[116] UN General Assembly, "The Right to Privacy in a Digital Age," Resolution 68/167, A/RES/68/167, Jan. 21, 2014, https://undocs.org/A/RES/68/167.

[117] Some netizens shared online that ever since they got married, they suddenly started getting calls from authorities on a regular basis nudging them to get pregnant.

[118] *Supra* note 2.

Yuegang Lu, a former senior reporter at China Youth Daily drew an analogy to explain China's crackdown on cyberspace backed by heavy regulation: "There are all sorts of birds when the forest is big, but we should not start cutting down the forest."[119] Claiming a law-based governance is insufficient as the Party maintains a dual system, under which the majority of citizens "generally enjoy the protection of an increasingly sophisticated body of law and legal institutions, but those deemed a danger to the party-state are handled outside the law."[120] Nonetheless, the situation appears to be an increase of the "minority" which are handled outside the law, while the legal system becomes more sophisticated.

Since Covid-19, a growing proportion of legal grounds for limiting free speech has been shifted from national security to "disinformation and fake news", although so many "rumours" ended up being the truth that citizens have developed a sense that something must be the truth if the authority steps out to call it a rumour. Self-censorship is encouraged by the State to increase credibility of the internet[121], but it also puts those who speak candidly in danger. The new disinformation framing mechanism makes the authority a truth decider. Gradually, Chinese netizens developed a silent consensus of what constitute "secret facts", which refer to knowing things and understanding at the same time that they cannot be shared.[122]

Self-censorship is dangerous also because it not only accompanies but also fuels the government's appetite to further restrain free flow of information which obstructs its ideal way of governance. For instance, despite China's relative candidness in not hiding the fact that it practices surveillance and blocks foreign websites, it is still becoming increasingly sensitive about this fact being discussed among citizens. Take the Great Firewall as an

---

119 Ling Zhao, *The truth of the Li Guangxi incident,* SOUTHERN WEEKLY, June 6, 2003, http://tech.sina.com.cn/me/2003-06-06/0007195125.shtml

120 *Supra* note 49.

121 Harriet Moynihan & Champa Patel, *Restrictions on online freedom of expression in China*, CHATHAM HOUSE, Mar.17, 2021, https://www.chathamhouse.org/sites/default/files/2021-03/2021-03-17-restrictions-online-freedom-expression-china-moynihan-patel.pdf.

122 *Supra* note 43.

example, paragraphs referencing its very existence are erased in the Chinese version of Snowden's memoir Permanent Record.[123] This resembles a non-disclosure agreement with a clause dictating that the existence of the agreement itself is confidential and demonstrates how censorship only worsens and goes far beyond the notion of national security, disinformation, or other pretext.

The socio-political argument where collective benefit is prioritised over individual rights in China and some other Asian countries stands on weak ground in light of numerous desolate events during the Shanghai omicron wave. Strict measures to prevent people from leaving home for reasons of pandemic control caused substantial humanitarian crisis. To accomplish the zero-Covid goal, Covid-free cancer and emergency patients often cannot receive prompt medical attention; resident starve for days at home because of categorical lockdown implementation; epidemic staff or police break into residents' homes to "arrest" them for being tested positive.[124] These extreme measures taken for safeguarding collective benefit is a false benefit, as explained by Mill's On Liberty, when such benefit cannot be recovered to every individual.

Law enforcement or government institutions can get rid of their responsibilities for disproportionate and harmful measures as easily as how they initially decided to take actions under any vague provisions. Towards the end of the Shanghai lockdown, when citizens asked for a timeframe of reopening the city, an official said at the government

---

123 *Edward Snowden claims Chinese edition memoir has been censored,* THE BOOKSELLER, Nov. 12, 2019, https://www.thebookseller.com/news/edward-snowden-claims-chinese-edition-memoir-has-been-censored-1111611.

124 *See* Dan Macklin, *Political tensions simmer over Shanghai covid-19 crisis,* THE DIPLOMAT, Apr.20, 2022, https://thediplomat.com/2022/04/political-tensions-simmer-over-shanghais-covid-19-crisis/; *Even some covid-free Shanghai residents say they've been forced into distant quarantine centres,* CBS NEWS, May 2, 2022, https://www.cbsnews.com/news/covid-china-shanghai-lockdown-beijing-cases-quarantine-centers/. Jane Duckett et al., *China's Covid crisis and the dilemma facing its leaders, by experts who have monitored it since the Wuhan Outbreak,* THE CONVERSATION, May 10, 2022, https://theconversation.com/chinas-covid-crisis-and-the-dilemma-facing-its-leaders-by-experts-who-have-monitored-it-since-the-wuhan-outbreak-182451 , Tracy Wen Liu, *Shanghai's food shortages spur voluntarism and cynicism,* FOREIGN POLICY, May 3, 2022, https://foreignpolicy.com/2022/05/03/shanghai-food-shortages-covid-lockdown-china/.

press conference that there had never been a lockdown in Shanghai and that what happened was a "pause" as part of the "citywide static management."[125] The authority also pointed out, conveniently at the end of two months of repeated miseries, that extreme measures taken by Residents' Committees (juwei) had no legal effect and do not represent the government, despite the fact that the Committees were carrying out direct orders from upper-level authorities. It is true that there was no formal legal or policy document designated specifically for the lockdown and its measures, although everyone knew it was the will of the government. This recent event is another vivid demonstration that legal instruments are not always necessary to justify the government's actions, but they can certainly get the government out of its responsibilities.

C. Digital Authoritarianism – How Far Have We Gone?

When a government determines what its citizens can and cannot see, think and express by taking full control of the cyberspace, it manifests the Party's parenting position in all aspects of a citizen's life. This goes beyond freedom of expression and amounts to a violation of freedom of conscience in that the attempt for thought-control is also present. One would not assume it to be an incident that President Xi has been inventing a lot of new vocabularies[126] since his term, a scenario too similar to what is depicted in George Orwell's 1984 where the official language of Oceania was invented as a tool to control citizens' thoughts. Some vocabularies get invented as much as some others get replaced, such as when the authority said that Shanghai was under a "citywide static management" instead of lockdown. Similarly, the State media recently published a list of additional 57 nuanced vocabularies to be applied by journalists and translators.[127]

---

[125] Wanming Gu, "*上海"封城"原来是乌龙，让人情何以堪",* May 31. 2022, https://chinadigitaltimes.net/chinese/682358.html.

[126] Examples include "key minorities", "a community with a shared future of mankind", etc. Note that the literal meaning is not evident in Chinese and these new vocabularies are challenging to understand, but they are trendy and one is better off being equipped with those new words. Interestingly, President Xi also invented the phrase "a community with a shared future *in* cyberspace."

[127] *See* https://www.xwpx.com/article/2021/1115/article_66336.html.

The process of digital censorship ironically also disturbs the advancement of AI technologies as the sources for the machines to learn are significantly limited. For instance, the range of conversation with iphone's Siri in China is substantially narrower compared to elsewhere because search engines as well as their search results available to Siri are limited. On the other hand, two robots were censored in China and supposedly "taken to re-education" because they started answering questions in ways much to the Party's distaste, reflecting the flaws in deep learning and the government's vigilance towards AI.[128]

As we enter deeper into the digital age, the curiosity towards our relationship with the cyberspace has not fundamentally changed from what was pondered upon by Barlow and Kelly. Although unrealistic as seen from now, the liberal and idealistic stance advocated by Barlow where the cyberspace is a new home to the mind reminds us what this marvelous part of technological revolution was initially promised of – freedom of choices, as argued by Kelly. It is not a tool for any government to centralise more power while taking away our rights which we are already deprived of in physical space. Covid-19 has revealed the worrisome and unfortunate fact that even though we have entered the digital age, the Chinese people might have been driven into a path less promising and have gone too far into digital authoritarianism, if not digital totalitarianism.

[128] *Chinese rebel robots apparently re-educated after rogue rants,* REUTERS, Aug. 4, 2017, https://www.reuters.com/article/china-robots-idUKL4N1KQ1UW.

V. Conclusion

China's treatment of law and technology is deeply influenced by its overriding concern of safeguarding the socialist regime. To ensure social stability which largely consists of monopolising information, by blocking, monitoring and suppressing the free flow of information, a massive range of technologies are employed and a substantial number of laws are enacted. However, recent social events linked to Covid-19 increasingly reveal unacceptable violation of human rights which go beyond those of privacy and freedom of expression. The citizens' awakening and discontent caused by immoderate reliance on cyber sovereignty and legislative activities is counter-productive to the original goal of regime stability, since one rationale of free speech is to reckon with a stable social change because suppressing dissent would drive opposition to the underground.[129] And because technology is a double-sided sword, it weakens the governed but also teaches them ways to toughen up.

[129] Thomas Emerson, Toward a general theory of the First Amendment, 72 YALE L.J.877-956 (1963)