Gergely Gosztonyi*

Special Models of Internet and Content Regulation in China and Russia

Abstract

According to the so-called 'cyber sovereignty', every country has the right to choose how to develop and regulate the Internet. The Golden Shield system, operated by the People's Republic of China is surrounded by a complex and ever-changing legal, technological and human background, can achieve cyber sovereignty. In the summer of 2021 Russia caught up. The question that Chinese leaders, while running the Golden Shield, and Russian leaders, while cutting down the country from the world's internet infrastructure, are trying to find the answer to is whether the 21st century can provide a solution that can simultaneously ensure economic opening and advancement and also informational isolationism.

Keywords: Golden Shield, censorship, internet, China, content control, cyber sovereignty, Russia

I Content Regulation Models in the World

The 2010s will be remembered for a new era in the development of capitalism, one of mind-boggling scale. Apple, Amazon and Microsoft are closing the decade as the world's first trillion-dollar companies. In 2018, Apple's revenue was larger than Vietnam's GDP, while Amazon's research and development spending alone is almost as much as Iceland's GDP. Facebook boasts 2.4 billion users, a population larger than that of every continent except Asia.[1]

* Gergely Gosztonyi (PhD) is associate professor at the Department of the History of Hungarian State and Law, Eötvös Loránd University, Budapest.

[1] Jay Owens, 'The tech giants dominated the decade. But there's still time to rein them in' (25 December 2019) The Guardian <https://www.theguardian.com/commentisfree/2019/dec/25/2010s-tech-giants-google-amazon-facebook-regulators> accessed 10 July 2021.

Jay Owens' late-2019 newspaper article accurately describes the change we have seen in the 2010s: growing gigantic tech companies that states are trying to bring under the umbrella of state law in some way – by fine words, begging, or even the use of force. However, new media and regulation are not always easily brought onto one platform.

In the US, the CDA230(c)(2)[2] regulates the liability of online content providers and these twenty-six short words in English have completely rewritten the history of the Internet:[3]

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

With this provision, the State actually 'privatised' the issue of free speech and decisions to remove illegal or harmful content. To simplify, we can say that, in good faith, all the tools needed to remove content are in the hands of service providers without them having to bear any kind of liability. It gave internet startups and their investors the confidence that 'they could fill their platforms with content from ordinary users, without attracting any legal liability for anything those users might write'.[4] That is why this model is called the 'immunity model'.

The European Union has set up a system unlike the CDA230 rules on one of the key issues regarding the Internet, which is that it can also be held responsible for infringing content.[5] The central element is Section 4 of the Directive on Electronic Commerce,[6] which deals with the liability of intermediary service providers. The set of rules works with a threefold system of concepts, the first two of which ('mere conduit' and 'caching') give service providers immunity from liability, just like in the US system. Hosting is the third possibility and Article 14 rules that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

a) the provider does not have actual knowledge of illegal activity or information and as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

---

[2] Communications Decency Act of 1996, 47 U.S. Code.

[3] Jeff Kosseff, *The 26 Words That Created the Internet* (Cornell University Press 2019, New York).

[4] Matt Reynolds, 'The strange story of Section 230, the obscure law that created our flawed, broken internet' (24 March 2019) Wired <https://www.wired.co.uk/article/section-230-communications-decency-act> accessed 10 July 2021.

[5] Christiane Wendehorst, 'Platform Intermediary Services and Duties under the E-Commerce Directive and the Consumer Rights Directive' (2016) 5 (1) Journal of European Consumer and Market Law, 30–33.

[6] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. OJ L 178, 17.7.2000, 1–16.

The (relative)[7] novelty of the European system is therefore the so-called notice-and-takedown system (NTDS)[8] that has put in place a multi-stage system of conditions and procedures: on the one hand, the intermediary service provider must be aware of content that is manifestly illegal and, on the other hand, take steps to remove the content within a specified period of time. Thus, it can be concluded that in contrast to the American regulation, the European Union voted in favour of another model (also called the 'safe harbour model'[9]), which focused on a non-automatic but possible exemption from liability.

Although it is less often discussed, and many politely turn a blind eye, there is a third option besides the American 'immunity model' and the European 'safe harbour model' of regulating the internet, moderating content and censorship: the Chinese (and Russian or Asian) model. This model opted for a much stricter route in handling responsibility issues regarding internet and content regulations than those in Europe or the United States. In order to observe and understand this process we have to travel back in time a few years.

II The Beginnings of Chinese Internet Regulation

Without diving deep into the history of Chinese media regulation,[10] it is worth pointing out that the Kuomintang, the leadership of the Chinese Communist Party has, since the very beginning, known that influencing people's thinking and public opinion will have a vital role in gaining and keeping their power.

> Having ruled China for more than half a century by means of political violence, ideological education and propaganda, the Communist regime has succeeded in making many Chinese people reject universal human values such as human rights, freedom, democracy, and respect for life as bourgeois principles.[11]

---

[7] The procedure already appears in the US Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998), but there it applies only to copyright infringement. For a comparison, see: Miquel Peguera, 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems' (2009) 32 (4) Columbia Journal of Law & the Arts, 481–512.

[8] Alexandre De Streel, Elise Defreyne, Hervé Jacquemin, Michèle Ledger, Alejandra Michel, 'Online Platforms Moderation of Illegal Content Online. Law, Practices and Options for Reform. Study for the committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies' (European Parliament 2020, Luxembourg) 10.

[9] Tambiama Madiega, 'Reform of the EU liability regime for online intermediaries. Background on the forthcoming Digital Services Act' (2020, May) European Parliamentary Research Service <https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRSIDA(2020)649404EN.pdf> accessed 10 July 2021, 1–2.

[10] For further details see: Qinglian He, *The Fog of Censorship: Media Control in China* (Human Rights in China 2008, New York) 2–41.

[11] He (n 11) 4–5.

Consequently, up until 1978, the Chinese press was characterised by strict political oppression, including the censorship of content for various (prior restraint or subsequent) political reasons.[12]

In the early 1980s, changes in the international political and economic environment forced the Chinese state to make certain concessions in the field of media regulation.[13] These concessions, however, were revoked in the wake of the events of 1989 (the protests in Tiananmen Square, and the dissolution of the Soviet Union and subsequently that of the Soviet bloc).[14] 'The Central Committee's Propaganda Department and General Office sent a 48-article set of top-secret instructions to lower-level officials, explaining which issues could be discussed and under what specifications. Anyone who failed to follow these secret instructions risked various legal sanctions.'[15] In the early 2000s, it seemed that general reforms would be introduced not only in economic, but also in political areas. However, these hopes proved to be in vain, as a list of detailed regulations, issued in August 2003[16] implemented measures such as:

– instructing all media to follow the 'proper political orientation';
– setting up an integrated national news agency providing news to all other media;
– the political inspection and control of the news media.[17]

III The Internet in China

These facts became of paramount importance after the internet was publicly introduced in China in 1995 and, as elsewhere, the number of users began to grow exponentially in the 2000s.

Table 1.

	Population	Number of users (June 2000)	Number of users (June 2021)	% of China's population (June 2021)	% of Asian users (June 2021)
China[19]	1,444,216,107	22,500,000	989,080,566	68.5%	35.7%

[12] Qiuqing Tai, 'China's Media Censorship: A Dynamic and Diversified Regime' (2014) 14 (2) Journal of East Asian Studies, 185–209. DOI: 10.1017/S1598240800008900

[13] Margaret E. Roberts, *Censored. Distraction and Diversion Inside China's Great Firewall* (Princeton University Press 2018, Princeton) 98–101.

[14] Gosztonyi Gergely, 'A parlamentarizmus helyreállítása' [The reconstruction of parliamentarism] in Mezey Barna, Gosztonyi Gergely (eds), *Magyar alkotmánytörténet. [The history of the Hungarian constitution]* (Osiris Kiadó 2020, Budapest) 505–507.

[15] He (n 11) 14.

[16] A detailed plan of execution can be found in the 2003 August communiqué by the Central Committee and the State Council 'On the improvement of control of Party and Government declarations distribution and on the use of jurisdiction for increasing productivity and alleviating local agriculture'.

[17] He (n 11) 18–20.

[18] Not including the population and number of users in special administrative territories (Hong Kong, Macao, Taiwan etc.) <https://www.internetworldstats.com/stats3.htm> accessed 10 July 2021.

We can clearly see that while in 2000 approximately 1.7% of the Chinese population (1,267,430,000[19]) used the internet, as of today, twenty years later, this number has risen to nearly 70%.[20] This huge number of people were not allowed freedom of speech by the Communist Party; therefore, in 1998, before the number of internet users started a steep ascent, a new Cyber Police Force was established,[21] which performed the 'traditional' tasks of blocking and controlling online discussion via various means of content regulation and censorship.[22] The measures (to be further developed later) were diverse: controlling domestic content ranged from using intimidation to bans, while foreign content was altogether blocked from Chinese users as a rule. The first signs of an 'isolationist' internet were thus already apparent in the late 1990s when 'only' 22 million – privileged, we could say – Chinese citizens had the chance to use this new means of communication.

Legal regulations have become more prominent since 2000: that year's decree no. 292 by the State Council of the People's Republic of China,[23] which ordered that certain domains and IP-addresses be recorded by internet providers, was issued. Two years later, in 2002 the Chinese government issued the Provisional Regulations on the Administration of Internet Publications,[24] which primarily – but not exclusively – targeted websites containing political content. The decrees stated, among others, the following provisions:

– any internet provider must obtain official approval (commercial goals) or registration (non-commercial goals);

– internet service providers must report all instances of topics involving national security or social unrest;

– they must make a copy of and retain content uploaded by third parties;

– they must adopt a system of editorial responsibility, whereby special editorial staff review all content submitted for publication on the internet for compliance with the law.

So it is evident that the Chinese model has, from the very beginning, opted for editorial responsibility, complemented by sanctions (such as a warning, an order to halt operations, confiscation of the equipment or a fine).[25] The annual cost of the system is huge: according to some calculations, in 2020 alone, USD 6.6 billion was spent to maintain the system.[26]

---

[19] See <https://www.statista.com/statistics/263765/total-population-of-china> accessed 10 July 2021.

[20] A huge rise in the number of users occurred between 2006 and 2012, rising from 10% to 40% of the population.

[21] However, according to Harwit and Duncan, it was not until the end of 2000 that the organisation really began to operate, first in Anhui province and then in 20 others. Eric Harwit, Duncan Clark, 'Shaping the Internet in China: Evolution of Political Control over Network Infrastructure and Content' (2001) 41 (3) Asian Survey, 394. DOI: 10.1525/as.2001.41.3.377

[22] He (n 11) 168.

[23] Premier Zhu Rongji, 'Measures for the Management of Internet Information Services' (2010) 43 (5) Chinese Law & Government, 30–35. DOI: 10.2753/CLG0009-4609430504

[24] Taylor C. Boas, 'Weaving the Authoritarian Web' (2004) 103 (677) Current History, 438–443.

[25] He (n 11) 170.

[26] Reporters Without Borders, 'China's Cyber Censorship Figures' (rsf.org, March 2021) <https://rsf.org/en/news/chinas-cyber-censorship-figures> accessed 10 July 2021.

IV 'Old style censorship is being replaced with a massive, ubiquitous architecture of surveillance: the Golden Shield'[27]

'What is better? Big Brother Internet? Or no Internet at all?'[28] asked Michael Robinson, a young American computer engineer, who participated in developing the Chinese internet from 1996, but eventually became disillusioned of Chinese practices. The Golden Shield Project provided an answer to the dilemma: internet use for millions of Chinese people, albeit on condition that they are being continuously watched.[29] Following the Great Wall of China, we have witnessed the construction of the Great Firewall of China,[30] which is part of the Golden Shield Project. According to Greg Walton,[31] the main idea behind its construction was a paradox. On the one hand, the Chinese government understood that information technologies and the internet are the engines driving the global economy, and if China wants to be a part of it, the use of information technologies is inevitable. On the other hand, China is an authoritarian single-party state, which cannot allow anyone to question or undermine its authority.

> The Great Firewall, as it is called by foreigners, is a system of limiting access to foreign websites, which started in the late 1990s,[32] and the Golden Shield is a system for domestic surveillance (*providing full national surveillance*[33]) set up in 1998 by the Ministry of Public Security.[34]

At the time of their creation, although the cyber police had already been actively supervising editorial responsibilities and blocking undesired content from Chinese users, it was

---

[27] Greg Walton, *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China* (Rights & Democracy 2001, Montreal) <https://numerique.banq.qc.ca/patrimoine/details/52327/2160163> accessed 10 July 2021, 5.

[28] Quoted by: Ethan Gutmann, 'Who Lost China's Internet?' (15 February 2002) The Weekly Standard <https://ethan-gutmann.com/who-lost-chinas-internet> accessed 10 July 2021.

[29] Ironically, the introduction of Chinese Internet censorship was abetted by major US tech companies, most notably Cisco, 'which began supplying filtering and monitoring equipment to Chinese censors in the early 1990s'. James Griffiths, *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet* (Zed Books 2019, London) 33. DOI: 10.5040/9781350225497

[30] Harsh Taneja, Angela Xiao Wu, 'Does the Great Firewall Really Isolate the Chinese? Integrating Access Blockage w ith Cultural Factors to Explain Web User Behavior' (2014) 30 (5) The Information Society, 297–309. DOI: 10.1080/01972243.2014.944728

[31] Walton (n 28) 5.

[32] Unsurprisingly, there is some disagreement about when exactly the project started: Sonali Chandel et al. mark 1996 as year zero, adding that (after various further stages) only in 2008 was it fully realised. Sonali Chandel, Zang Jingji, Yu Yunnan, Sun Jingyao, Zhang Zhipeng, 'The Golden Shield Project of China: A Decade Later – An in-Depth Study of the Great Firewall' (International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2019) <https://www.researchgate.net/profile/Sonali-Chandel/publication/338361425TheGoldenShieldProjectofChinaADecadeLater-Anin-DepthStudyoftheGreatFirewall/links/5e136bce299bf10bc392fc09/The-Golden-Shield-Project-of-China-A-Decade-Later-An-in-Depth-Study-of-the-Great-Firewall.pdf> accessed 10 July 2021, 112.

[33] Author's note.

[34] E.H., 'How does China censor the internet?' (22 April 2013) The Economist <https://www.economist.com/the-economist-explains/2013/04/21/how-does-china-censor-the-internet> accessed 10 July 2021.

technically possible to hide from the watching eyes of Big Brother. There was no need for a hidden corner in a room, as Winston Smith was hiding from the telescreen in George Orwell's *1984*, it was enough to install a Virtual Private Network (VPN).[35] The construction and utilisation of the Golden Shield,[36] however, brought about the total control of online communication, which few would have thought possible before.[37] Its main objective is naturally a political one: to block the online spread of ideas that might lead to actual political resistance. The surveillance system's main characteristics are its uncertainty and unpredictability:[38] it is unknown what kind of content is restricted and what is not and why some content is available in certain parts of the country but not in others, as well as which social group is denied access to what type of content. Bobbie Johnson calls this system hit-and-miss technology,[39] Séverine Arsène[40] and Margaret E. Roberts[41] use the term 'porous censorship', while János Boris uses the phrase 'adaptive authority',[42] referring to the consciously implemented 'safety valves', errors and omissions. It is also worth pointing out that the Golden Shield is continuously learning and improving with the help of people (the police and moderators) as well as artificial intelligence.[43]

---

[35] In 2017 controversial reports appeared about the use of VPN applications in China. According to The Guardian the Chinese government ordered the country's three greatest state-owned broadcasting providers (China Mobile, China Unicom, China Telecom) to completely block all VPNs. The Diplomat, however, quoted official statements saying only illegal VPNs would be banned in China from 2018. There is an irony behind this notion, as it is the Chinese government that has the right to decide what constitutes an illegal use of VPN. Benjamin Haas, 'China moves to block internet VPNs from 2018' (11 July 2017) The Guardian <https://www.theguardian.com/world/2017/jul/11/china-moves-to-block-internet-vpns-from-2018> accessed 10 July 2021; Charlotte Gao, 'China Clarifies Reports of VPN Ban' (13 July 2017) The Diplomat <https://thediplomat.com/2017/07/china-clarifies-reports-of-vpn-ban> accessed 10 July 2021.

[36] Chandel, Jingji, Yunnan, Jingyao, Zhipeng (n 33) 114.

[37] Valentin Weber, 'The Worldwide Web of Chinese and Russian Information Controls' (2019) 11 University of Oxford Centre for Technology and Global Affairs Working Paper Series <https://www.ctga.ox.ac.uk/files/theworldwidewebofchineseandrussianinformationcontrolspdf> accessed 10 July 2021.

[38] Many compares Project Golden Shield to Jeremy Bentham's Panopticon concept, where prison inmates do not know who among them are being observed, and whether anyone is observed at all. As Barna Mezey put it: 'This construction made any kind of conspiracy or cooperation, thus any kind of rebellion or breakout impossible.' Mezey Barna, *A börtönügy a 17–19. században. A börtön európai útja [The state of prisons in the 17th-19th centuries. Prisons in Europe]* (Gondolat Kiadó 2018, Budapest) 337.

[39] Bobbie Johnson, 'How Google censors its results in China' (The Guardian, 13 January 2010) <https://www.theguardian.com/technology/2010/jan/13/how-google-censors-china> accessed 10 July 2021.

[40] Séverine Arsène, 'La Chine et le contrôle d'Internet. Une cybersouveraineté ambivalente' (2019) 20 Annuaire Français de Relations Internationales <https://www.afri-ct.org/wp-content/uploads/2020/06/Article-Arsene.pdf> accessed 10 July 2021, 961.

[41] Roberts (n 14) 2.

[42] Boris János, 'A Nagy tűzfal és a SZORM, avagy a zárt internet orwelli világa' [The Great Firewall and SZORM, or the Orwellian world of the closed internet] (2016) 2 (1) Athenaeum, 62.

[43] Chen Qiufan, 'The Reunion: a new science-fiction story about surveillance in China' (2019) 122 (1) MIT Technology Review, 89–95.

Freedom House, in its 2020 report on the internet, stated that 'China's surveillance systems remain the most advanced and pervasive in the world'.[44] The reason for this is that various elements of the Golden Shield not only monitor and restrict, if necessary, online activities, but form an interlinked system which makes political and social profiling[45] possible using the following:

– 'monitoring of information space;
– Big Data analysis;
– monitoring of public spaces;
– cameras in and around homes;
– health status apps;
– thermal detection technology;
– contact tracing apps;
– detentions for online activities;
– facial recognition technology'[46].

The report makes this statement even more shocking by illustrating all of the above possibilities in one picture:

Figure 1.

[44] Freedom House, 'Freedom on the Net 2020. The Pandemic's Digital Shadow' (21 October 2020) <https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf> accessed 10 July 2021, 21.

[45] Asbóth Emma, Tamás Bianka, 'Szezám tárulj – a kínai szociális kreditrendszer' [Open Sesame – the Chinese social credit system] (9 January 2019) arsboni <https://arsboni.hu/a-kinai-szocialis-kreditrendszer-sesame-credit> accessed 10 July 2021.

[46] Roberts (n 14) 21.

This has led from the early times characterised by 'traditional' dangers threatening the freedom of the press to an era of total national surveillance by traditional online technologies. The People's Republic of China, however, approaches the question with a different attitude. For them, it is a question of 'internet sovereignty',[47] demonstrated by the president of China, Xi Jinping, in his 2015 speech at the second World Internet Conference,[48] where he called on all countries to respect each other's 'cyber sovereignty' and various methods of internet control. He pointed out that all countries have the right to develop and control their own internet, and, clearly referring to the United States, rejected the idea that any country should acquire hegemony in cyberspace, which is not a space without its own laws. All this leads to the question whether a 'Chinese internet', 'American internet', 'Egyptian internet' or even a 'Hungarian internet' are concepts that do or may exist. If so, the process of internet regulation should be similar to the early days of media and broadcasting regulation, where countries formulate their own rules, then – ideally, but not necessarily – harmonise them with those of neighbouring, similarly affected countries.[49] As we all know, this was the original method of media regulation, later totally transformed by the improvement of technology, first by TV and radio signals, then by the internet.

Apart from the restriction of civic and political rights, there are also economic aspects. In 2008, YouTube became unavailable due to the Tibet situation, and the same happened to Facebook (2008), Twitter (2009) and Wikipedia (2019) because of events in the Xinjiang Uyghur Autonomous Region. What options can companies have in this situation? Sacrifice hundreds of millions of users for their democratic principles? Or toe the line, imposing a form of economic censorship on themselves? Google has opted for the latter,[50] making certain content unavailable in China when searching on google.cn ever since it appeared on the Chinese internet market in 2006.[51] American politicians and the general public, however, found these practices unacceptable, and the objections eventually led to Google discontinuing its services in China.[52] However, as Ryan Gallagher uncovered in 2018,[53]

---

47 Simon Denyer, 'China's scary lesson to the world: Censoring the Internet works' (23 May 2016) The Washington Post <https://www.washingtonpost.com/world/asiapacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dcstory.html> accessed 10 July 2021.

48 N/A, 'China internet: Xi Jinping calls for 'cyber sovereignty'' (16 December 2015) BBC <https://www.bbc.com/news/world-asia-china-35109453> accessed 10 July 2021.

49 Jack L. Goldsmith, Timothy Wu, 'Digital Borders: National Boundaries Have Survived in the Virtual World and Allowed National Laws to Exert Control Over the Internet' (2006) 40 Legal Affairs <https://www.legalaffairs.org/issues/January-February-2006/featuregoldsmithjanfeb06.msp> accessed 10 July 2021; Jack L. Goldsmith, Timoty Wu, *Who controls the Internet? Illusions of a borderless world* (Oxford University Press 2006, Oxford).

50 Christopher Stevenson, 'Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World' (2007) 30 (2) Boston College International and Comparative Law Review, 543.

51 The same route was taken by Microsoft as well. Stevenson (n 51) 544.

52 Officially due to Chinese hacker attacks. Stevenson (n 51) 137–138.

53 Ryan Gallagher, 'Google Plans to Launch Censored Search Engine in China' (1 August 2018) The Intercept <https://theintercept.com/2018/08/01/google-china-search-engine-censorship> accessed 10 July 2021.

as an attempt to get back into the Chinese market, Google was planning to develop a search engine blacklisting all websites and search results pertaining to human rights, democracy, religion or peaceful resistance. The project (Project Dragonfly, as it was dubbed) was officially closed down in 2019.[54]

V Russia is Catching Up

In the 2020s, the blocking of online content for political reasons is an everyday phenomenon in numerous countries. China's internet sovereignty is the most comprehensive system, but in the summer of 2021 Russia has caught up: after having perfected the technology for a few years, between 15 June 2021 and 15 July 2021, in a test run, Russia successfully[55] disconnected itself from the World Wide Web.[56] The basis of this act was the amendment of the 2013 federal law on telecommunications:[57] the Sovereign Internet Law of 2019,[58] which:

– obliged Russian internet providers to install Deep Packet Inspection (DPI) and enabled providers and authorities to find the original source of threatening content and block it if necessary;

– obliged providers to route online traffic and information through state-controlled checkpoints;[59]

– entitled the government to disconnect the Russian internet physically from the World Wide Web in case of an emergency.[60]

---

[54] Dippold Ádám, 'A Google beszüntette gyanúsan cenzúrabarát projektjét' [Google shut down allegedly censorship-friendly project] (19 June 2019) Qubit <https://qubit.hu/2019/07/19/a-google-beszuntette-gyanusan-cenzurabarat-projektjet> accessed 25 July 2021.

[55] Ashley Collman, 'Russia disconnected itself from the rest of the internet, a test of its new defense from cyber warfare, report says' (23 July 2021) Insider <https://www.businessinsider.com/russia-cuts-self-off-from-global-internet-tests-defenses-rbc-2021-7> accessed 25 July 2021.

[56] It should be noted that Insider was not able to have this information confirmed by two independent sources.

[57] On the process leading to passing the law and on its details see: Tölgyesi Beatrix, 'Az orosz 'szuverén internet' törvényről' [On the Russian 'sovereign internet' law] (2020) 13 (2) Nemzet és Biztonság: Biztonságpolitikai Szemle, 113–132; Human Rights Watch, 'Russia: Growing Internet Isolation, Control, Censorship. Authorities Regulate Infrastructure, Block Content' (18 June 2020) <https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship> accessed 25 July 2021. DOI: 10.32576/nb.2020.2.8

[58] Federal Law No. 90-FZ of 01. 05. 2019 'On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technology and Information Protection"', <http://publication.pravo.gov.ru/Document/View/0001201905010025> accessed 25 July 2021.

[59] Moreover, similarly to China, there are extremely high fines for using VPNs. N/A, 'State Duma introduces fines for violating anonymiser law' (5 June 2018) Meduza <https://meduza.io/news/2018/06/05/gosduma-vvela-shtrafy-za-narushenie-zakona-ob-anonimayzerah> accessed 25 July 2021.

[60] Alexandra Ma, 'Russia officially introduced a 'sovereign internet' law to let Putin cut off the entire country from the rest of the web' ('1 November 2019) Insider <https://www.businessinsider.com/russia-sovereign-internet-law-cut-web-access-censorship-2019-11> accessed 25 July 2021.

The vague definition of security threats leaves it to the authorities to decide which situation requires tracking, rerouting, or blocking. The process is not transparent and opens the door to abuse, Human Rights Watch said, adding that passing the law 'is bad news for Russia and creates a dangerous precedent for other countries'.[61] However, there were signs: in its 2019 report, Reporters Without Borders puts the number of Russian laws restricting press freedom or freedom of expression at 27.[62] The report's addendum also shows that, in a short period of two years (2020-2021), another 16 similar laws were adopted in Russia.[63] The European Audiovisual Observatory 2021 highlighted that, as a result of some European Court of Human Rights' decisions,[64] Russia has moved away from blocking content in favour of imposing substantial fines to the internet platforms and providers.[65]

VI Conclusion

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression highlighted in his 2020's report that 'Internet shutdowns (or restrictions)[66] are an affront to the freedom of expression that every person is guaranteed under human rights law'.[67] In contrast, one could see similar techniques and legal solutions in the most populated (China) and the 9th most populated (Russia) countries in the world: immense surveillance systems capable of learning and evolving, the restricting or banning of the use of VPN, hybrid actions,[68] enormous fines, unpredictable legal or judicial actions for 'threatening content' – i.e. having (almost) direct control over 20% of the world's population.

---

[61] Human Rights Watch, 'Russia: New Law Expands Government Control Online. Wider Internet Surveillance' (31 October 2019) <https://www.hrw.org/news/2019/10/31/russia-new-law-expands-government-control-online> accessed 25 July 2021.

[62] Reporters Without Borders, 'Taking Control? Internet Censorship and Surveillance in Russia' (rsf.org, 27 Nov 2019) <https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Berichte/2019/russiareport_web_updated.pdf> accessed 25 July 2021, 10–20.

[63] Reporters Without Borders, 'Taking Control? Internet Censorship and Surveillance in Russia. Updated' (31 Aug 2021) <https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Berichte/2021/russiareport-update.pdf> accessed 4 Sep 2021, 9–18.

[64] *Bulgakov v. Russia* App no. 20159/15 (ECtHR, 23 June 2020); *Engels v. Russia* App no. 61919/16 (ECtHR, 23 June 2020); *OOO Flavus and Others v. Russia* App nos 12468/15, 23489/15, and 19074/16 (ECtHR, 23 June 2020); *Vladimir Kharitonov v. Russia App* no. 10795/14 (ECtHR, 23 June 2020).

[65] Andrei Richter, *Regulation of social media in Russia* (European Audiovisual Observatory 2021, Strasbourg) 10.

[66] Author's note.

[67] UNHRC: Disease pandemics and the freedom of opinion and expression. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. 2020, UN Doc A/HRC/44/49, 28.

[68] Kelemen Roland, 'Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben' [Radicalisation, disinformation and mass psychosis in a modern guise: the hybrid conflict in cyberspace] (2021) 13 (3) Jog–Állam–Politika, 82.

The question to which the Chinese leaders, while running the Golden Shield, and Russian leaders, while cutting down the country from the world's internet infrastructure, are trying to find the answer to is the same: can the 21st century's media provide a solution that can simultaneously ensure economic opening and advancement, and also informational isolationism? We will most likely have to wait quite a few years to get the answer, but it is evident that, for both conditions to apply, it needs 'the largest and most sophisticated online censorship operation in the world'.[69] Besides the American immunity-based system and Europe's 'safe harbour' method, there is a third route, based on nationwide surveillance, which does not allow for mistakes on the part of users, as it prevents them from accessing information. If any undesired information does get through to the user, via the consciously implemented 'safety valves' or other channels, the internet service providers are held directly responsible, with no immunity or acquittance.[70] Internet providers are also obliged to perform constant monitoring, which means that free opinions have to go through three barriers before they can reach the public:

– self-imposed user censorship;
– economic censorship (monitoring by providers);
– state censorship.

Is this the way of the future? Systems such as Golden Shield, with a complex and ever-changing, constantly evolving legal, technological and personal background, ensuring 'cyber sovereignty'? Moreover, as Bennett and Naim note, the alarming wave that 'China has advised Iran on how to build a self-contained '"Halal" Internet and Beijing has also been sharing know-how with Zambia to block critical Web content'.[71] Similar technologies, situations and explanations could be seen worldwide only in the first half of 2021:

– mobile internet disruptions in Iran amid water protests in Khuzestan;[72]
– social media restrictions amid widespread anti-government protests in Cuba;[73]
– restriction of Twitter in Nigeria after deleting a tweet by the Nigerian president;[74]

---

[69] Elizabeth C. Economy, 'The great firewall of China: Xi Jinping's internet shutdown' (29 June 2018) The Guardian <https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown > accessed 25 July 2021.

[70] On different cases of copyright and trademark breaches see: Danny Friedmann, 'Oscillating from Safe Harbor to Liability: China's IP Regulation and Omniscient Intermediaries' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020, Oxford) 277–294.

[71] Philip Bennett, Moises Naim, '21st-century censorship' (2015) 14 (1) Columbia Journalism Review <https://archives.cjr.org/cover_story/21st_century_censorship.php> accessed 25 July 2021.

[72] John Gambrell, 'Mobile internet disruptions seen in Iran amid water protests' (22 July 2021) AP <https://apnews.com/article/technology-middle-east-business-health-iran-98b973da755a3ccf80428570bfdd3fb6> accessed 25 July 2021.

[73] Sarah Marsh, Elizabeth Culliford, 'Faced with rare protests, Cuba curbs social media access, watchdog says' (14 July 2021) Reuters <https://www.reuters.com/world/americas/cuba-curbs-access-facebook-messaging-apps-amid-protests-internet-watchdog-2021-07-13> accessed 25 July 2021.

[74] John Campbell, 'Nigerian President Buhari Clashes With Twitter Chief Executive Dorsey' (8 July 2021) Council on Foreign Relations Blog <https://www.cfr.org/blog/nigerian-president-buhari-clashes-twitter-chief-executive-dorsey> accessed 25 July 2021.

– internet shutdown amid anti-government protests in Colombia;[75]

– restriction of Facebook in Bangladesh amid protests against the visit of Indian Prime Minister Narendra Modi;[76]

– total internet shutdown on election day in the Republic of the Congo;[77]

– social media and messaging apps disabled amid political riots in Senegal;[78]

– internet shutdown amid deadly standoff at opposition candidate's house in Chad;[79]

– internet shutdown amid riots and alleged coup attempt in Armenia;[80]

– internet disruption amid military coup in Myanmar.[81]

The 'progress' of these countries is not the same, but their direction is. Tim Berners-Lee, often called 'one of the fathers of the internet',[82] in a 2013 interview[83] said 'The Berlin Wall tumbled down, the great firewall of China – I don't think it will tumble down, I think it *(i.e. total surveillance)*[84] will be released'. It has been eight years since the interview, and it turned out that he was wrong. Moreover, thanks to the ever-evolving technologies,[85] the Golden Shield is bigger, smarter and more precise than ever before. Cyberpaternalism,[86] that is, internet regulation within a country's geographical and legal boundaries, seems infeasible, but not impossible. Chinese 'cyber sovereignty' since 2015, as well as Russia's measures since the late 2010s, have all been steps in this dark direction.

---

[75] Jon Jackson, 'Internet Disrupted in Colombia as Protesters Killed During Rally Against Iván Duque Márquez' (5 May 2021) Newsweek <https://www.newsweek.com/internet-problems-colombia-protests-1588991> accessed 25 July 2021.

[76] N/A, 'Amid anti-Modi protests, Facebook says services restricted in Bangladesh' (27 March 2021) CAN <https://www.channelnewsasia.com/news/asia/anti-modi-protests-bangladesh-facebook-restricted-14505020> accessed 25 July 2021.

[77] N/A, 'Internet shutdown in the Republic of the Congo on election day' (21 March 2021) Digital Watch <https://dig.watch/updates/internet-shutdown-republic-congo-election-day> accessed 25 July 2021.

[78] Lawrence Agbo, '#FreeSenegal: Senegal Disables Facebook, Other Social Media Apps' (6 March 2021) Allnews Nigeria <https://allnews.ng/news/freesenegal-senegal-disables-facebook-other-social-media-apps> accessed 25 July 2021.

[79] N/A, 'Chad: Internet shutdowns impeding freedom of expression' (9 April 2021) Amnesty International <https://www.amnesty.org/en/latest/news/2021/04/tchad-les-coupures-internet-une-entrave-la-liberte-dexpression> accessed 25 July 2021.

[80] N/A, 'Internet disrupted in Armenia amid political turmoil and alleged coup attempt' (25 Febr 2021) Digital Watch, <https://dig.watch/updates/internet-disrupted-armenia-amid-political-turmoil-and-alleged-coup-attempt> accessed 25 July 2021.

[81] AccessNow, 'Update: internet access, censorship, and the Myanmar coup' (15 February 2021 – updated 30 May 2021), <https://www.accessnow.org/update-internet-access-censorship-myanmar> accessed 25 July 2021

[82] N/A, 'The Fathers of the Internet' (16 March 2014) Inmesol <http://www.inmesol.com/blog/fathers-internet> accessed 25 July 2021.

[83] Guy Faulconbridge, 'Father of Web says China will dismantle 'great firewall'' (22 November 2013) Reuters <https://www.reuters.com/article/uk-china-internet-berners-lee-idUKBRE9AL00120131122> accessed 25 July 2021.

[84] Author's note.

[85] Sorbán Kinga, 'Ethical and legal implications of using AI-powered recommendation systems in streaming services' (2021) 21 (2) Információs Társadalom, 63–82. DOI: 10.22503/inftars.XXI.2021.2.5

[86] Andrew D. Murray, 'Nodes and Gravity in Virtual Space' (2011) 5 (2) Legisprudence, 195–221. DOI: 10.5235/175214611797885684