December 5, 2023

China Releases Regulation on the Protection of Children in Cyberspace

Authored by: Liza L.S. Mark and Tianyun (Joyce) Ji

On October 16, 2023, China's State Council released the *Regulation on the Protection of Minors Online (《未成年人网络保护条例》)* (the "*Regulation*"), to take effect on January 1, 2024. The Regulation is promulgated in accordance with the *Law of the People's Republic of China on the Protection of Minors (《中华人民共和国未成年人保护法》)* (the "*MPL*"), the *Cybersecurity Law of the People's Republic of China (《中华人民共和国网络安全法》)*, the *Personal Information Protection Law of the People's Republic of China (《中华人民共和国个人信息保护法》* (the "*PIPL*"), and other laws to create an online environment conducive to the physical and mental well-being of minors and protect their lawful rights and interests.

The MPL was amended in 2021 to add a separate chapter for protection of minors in cyberspace. The promulgation of the Regulation now provides detailed guidance on co-governance from the whole society to provide a nurturing environment in cyberspace. For businesses offering products or services to minors, they should be prepared to integrate the requirements of the Regulation into their overall data protection and privacy spectrum.

Below are certain highlights of the Regulation:

I. SOCIAL CO-GOVERNANCE IN PROTECTING CHILDREN IN CYBERSPACE

The Regulation mandates that the Cyberspace Administration of China (the "*CAC*") be responsible for the overall planning and coordination for the protection of minors in cyberspace, and calls for collective efforts from various government agencies, including the national press and publication and film authorities, and the education, telecommunications, public security, civil affairs, culture and tourism, health, market regulation, radio and television, and other relevant authorities. (*Article 3*)

It requires social organizations (such as the Communist youth leagues, women's federations, trade unions, Young Pioneers, etc.) to assist in the effort to protect children in cyberspace. The Regulation further requires schools and children's families to educate and guide children to use the Internet in a scientific, civilized, safe, and rational manner, and not to be addicted to the Internet. (*Articles 4 and 5*) The Regulation also imposes obligations on three types of businesses: (i) network product and service providers, (ii) processors of personal information (of a minor), and (iii) smart terminal product manufacturers and sellers.

The consequences of violating the Regulation are substantial. Depending on the violation, businesses can be subject to fines of up to 1 million RMB, or up to 10 times of the illegal gains (if the illegal gains exceed 1 million RMB). Violators can also be subject to administrative penalties such as warnings, suspension of business, website shutdown, or even revocation of relevant permits or business licenses (with accompanying ineligibility to reapply within five years).

II. OBLIGATIONS OF BUSINESSES TO PROTECT CHILDREN IN CYBERSPACE

1. Online Product or Service Providers ("*OPSP*").

While not specifically defined, based on the context of the Regulation and in practice, "online product or service provider" generally refers to businesses such as online gaming, online livestreaming, online video streaming, social networking services, etc. They have the following obligations per the Regulation:

a. Post a prominent reminder before displaying certain content. If an online product or service contains information that may cause or induce minors to imitate unsafe behavior, violate social ethics, generate extreme emotions, develop bad habits, or otherwise impact the physical and mental well-being of minors, any organization or individual producing, reproducing, releasing, or disseminating such information shall provide a prominent reminder before displaying the information. (*Article 23*)

b. No easy access of certain content. OPSPs shall not display the information described in Article 23 above in any key sections of their products or services that are located prominently and easily attracting users' attention, including the above-the-fold section on the home page, pop-up windows, and most searched hashtags. (*Article 24*)

c. Establish mechanism against cyberbullying. The MPL defines cyberbullying against minors as "insulting, slandering or threatening any minor or maliciously damaging the image thereof through the Internet in the form of words, pictures, audio or video." Generally, actions such as online defamation, verbal abuse, doxing, false lighting, etc. are all considered cyberbullying.

Under the Regulation, OPSPs are required to:

i. establish and improve the early warning, prevention, identification, monitoring, and disposition mechanisms regarding cyberbullying;

ii. enable functions and channels for minors and their guardians to save records of cyberbullying targeting them and exercise their notification rights,

iii. provide protection options against cyberbullying content for minors, including blocking strangers, defining the scope of visibility for self-posted content, disabling reproduction or comments on self-posted content, and blocking information sent to them;

iv. establish and improve their cyberbullying information feature database, optimize relevant algorithms and models, and employ artificial intelligence, big data and other technical means combined with manual review to enhance the identification and monitoring of cyberbullying content.

(*Article 26*)

Cyberbullying can be particularly harmful to minors' physical and mental wellbeing and development, and thus attracts a lot of legislative attention. On July 7, 2023, the CAC also circulated the *Provisions on the Governance of Cyberviolence Information (Draft for Comment) (《网络暴力信息治理规定（征求意见稿）》)* to address

online service providers' obligations against cyberbullying, including content filtering, user account management, platform rulemaking, etc.

d. Prevent and address Internet addiction. The Regulation dedicates an entire chapter on how the society should work together in preventing Internet addiction of children. Specifically, the Regulation requires that OPSPs shall:

   i. establish and improve their anti-addiction systems, not to offer products and services to minors that induce addiction, and shall promptly modify content, functions, or rules that may lead to addiction in minors, and annually disclose their anti-addition efforts;

   ii. establish "children modes" based on different age groups so they can offer services in accordance with relevant national regulations and standards regarding usage time, duration, functions, and content, and provide time management, permissions management, expenditure management, and other control functions in a prominent and accessible manner for guardians;

   iii. employ measures to reasonably limit the single expenditure amount and single-day expenditure amount for minors of different ages when using their services, and must not offer paid services to minors that are not commensurate with the minor's civil capacity;[1]

   iv. employ measures to prevent harmful values and tendencies, such as prioritizing online traffic, and must not promote activities such as fan mobilization fundraising, fan voting to boost rankings, etc.;

   v. (for online game providers) verify the real identity information of minor users through necessary means, including the unified electronic identity authentication system for minor in online gaming, and must not provide game account rental and sales services to minors;

   vi. (for online game providers) establish and improve game rules to prevent Internet addiction among minors, and shield them from game content or game functions that may impact their physical and mental well-being.

It is worth noting that the OPSP's above anti-addiction measures should not be deployed uniformly among all children, but rather they are expected to be designed and categorized according to the levels of physical and mental perception characteristics of children of different age groups.

2. Providers of Network Platform Services Widely Used Among Minors.

Article 20 of the Regulation provides that a network platform service providers, as opposed to the providers of products or services on the platform, with a substantial number of minor users or significant influence on the minor population has the following obligations for protecting minors:

---

[1] Similarly, the MPL and *Guiding Opinions on Strengthening Standardized Management of Online Live Streaming (《关于加强网络直播规范管理工作的指导意见》)* has restricted registration of online livestreaming publisher account by minors under the age 16. Also online tipping/reward is prohibited for minors under the age of 16 (either by the minor, or for the minor).

a. Regular impact assessment. During the design, research, development, operation, and other stages of a network platform service, fully consider the characteristics of the physical and mental well-being and development of minors, and regularly conduct impact assessments on the protection of minors online;

b. Special mode or zone. Provide a special mode or zone for minors to facilitate them to access products or services on the platform that are beneficial for their physical and mental well-being;

c. Compliance system in place. Establish and improve a compliance system for protecting children in cyberspace, and establish an independent body primarily composed of external members to oversee such protection;

d. Enact specific platform rules and set prominent reminders for children's rights. Based on the principles of openness, fairness, and impartiality, formulate specific platform rules outlining the obligations of the platform's product or service providers for protecting minors online, and provide prominent reminders to minor users about their legal rights to online protection and channels for seeking remedies for cyber infringement;

e. Terminate services to violators when necessary. Terminate services to any product or service provider on the platform that gravely harms the physical and mental well-being of minors or otherwise infringe on their lawful rights and interests (such as those referred to in the MPL) in violation of laws or administrative regulations; and

f. Publish special social responsibility report. Publish annual special social responsibility reports on the protection of minors online to allow for oversight from society.

The above compliance requirements pose special challenges to a businesses' overall governance requirements, including having an independent body consisting of primarily outside members to oversee minor protection and publish an annual social responsibility report of the same. While the specific measures for how to determine a "network platform service provider with a substantial number of minor users or significant influence on the minor population" will be developed separately by the CAC, businesses with a large children user base (such as online tutoring, gaming, livestreaming etc.) should be prepared to take steps implementing those requirements.

3. Smart Terminal Device Manufacturers and Sellers.

Nowadays, smart terminal devices (such as a child's smart watch, tablets specially designed for studying, touch and talk pen, etc.) are frequently used by children both in schools and at home. Content filtering in these devices is necessary to create a nurturing online environment for children. In addition, as children are especially vulnerable in case of privacy breaches (such as leak of real-time location, hacking of camera, microphone, contact lists, etc.), it is critically important that those terminals are equipped with sufficient software against malicious attackers in the first place.

To that end, MPL's amendment in 2021 requires smart terminals to be equipped with network protection software for minors. Article 19 of the Regulation now sets forth in more detail that software as well as smart terminals specifically targeting users who are minors shall include functions that can effectively identify illegal information, protect children's personal information, prevent Internet addition, and facilitate guardians in supervising children.

In addition, manufacturers of smart terminals should either install network protection software[2] for minors before shipping out products, or prominently informing users of the installation channel and method. Note that such obligations under Article 19 are in addition to other applicable requirements under the Regulation.

III. PROTECTION OF THE PERSONAL INFORMATION OF MINORS

Personal information ("*PI*") of a minor under the age of 14 is categorized as "sensitive PI," subject to enhanced protection under the PIPL. Such sensitive PI requires the PI Processor to obtain consent of the minor's guardian before processing and special processing rules[3] should be in place. However, the current laws and regulations are unclear as to how to protect minors and their PI between the ages of 14 to 18.

Chapter 4 of the Regulation now fills the gap, which sets forth more detailed requirements for online businesses processing PI of minors of all ages. Specifically:

1. When online service providers provide information publishing, instant messaging, or other services to minors, they shall require the minors or their guardians to provide the minors' true identity information as required by the laws. They should refuse service if the minors or their guardians fail to provide such identity information.

2. Online livestreaming service providers shall establish a dynamic verification mechanism for the real identity of online livestreaming content publishers.[4]

---

[2] With respect to network protection software, relevant industry standards are in place or in progress, such as the *International Security Technology-Minors Mobile Terminal Protection Product Test and Evaluation Guidelines (GA/T 1537-2018) (信息安全技术 未成年人移动终端保护产品测评准则》)*, *Classifications and Codes of Online Unhealthy Contents for Minors (《未成年人互联网不健康内容分类与代码》)*, *Technical Specifications for Monitoring Systems of Online Games for Minors (《信息技术 网络游戏未成年人 监护系统技术要求》)*, etc.

[3] According to the *National Standard "Information Security Technology — Security Requirements for Processing of Sensitive Personal Information (Draft for Comment) (国家标准《信息安全技术 敏感个人信息处理安全要求》征求意见稿)* released on August 9, 2023, such special processing rules should at least state the following:

a) The purpose, method and scope of the processing of minors' PI, and its necessity;
b) The location, term, and disposition of minors' PI;
c) Security protection measures of minors' PI;
d) How to file a complaint by minors' guardians;
e) How minors' guardians can inquire, copy, correct, or delete information, withdraw consent, cancel an account, etc.;
f) The consequences of minors' guardians refusal to consent to PI processing rules;
g) Obtain separate consent of minors' guardians if any substantial change in any of the above in the special processing rules.

[4] Such identity verification requirements can also be found at many other regulations such as the *Circular on Prevent Minors from Addicting to Online Games (2019) (《关于防止未成年人沉迷网络游戏的通知》)*, *Measures for Business Activities of Online Performances (2021) (《网络表演经营活动管理办法》)*, *Circular on Tightening the Administration of Online Live Services (2018) (《关于加强网络直播服务管理工作的通知》)*, etc.

3. PI processors shall provide easy access, accessible functions to support, and promptly accept and process requests from minors or their guardians for accessing, copying, correcting, supplementing, or deleting minors' PI.

4. In the event of leakage, tampering or loss of minors' PI, PI processors shall immediately activate contingency plan and employ remedial measures, promptly report the incident to the CAC, and notify the affect minors and their guardians through emails, mail, phone calls, push notifications, or other applicable methods.

5. PI processors should limit access to minors' PI, and establish an approval mechanism and record access to prevent unlawful processing of minors' PI.

6. PI processors shall conduct annual compliance audits (either by themselves or through professional agencies) and report the audit results to the CAC.

The Regulation is China's first comprehensive set of regulations specially designed to protect children in cyberspace. It reinforces and integrates many existing rules scattered in various administrative agency measures related to data privacy/security and provides actionable guidance for businesses with user bases who are minors. In addition to complying with the various data privacy/data security regulations, businesses should be prepared to implement the requirements under the Regulation into the full lifecycle of the data they process, including promptly identifying and verifying children's identities at the beginning, obtaining informed consent from children's guardians, conducting a minimum collection of PI, filtering content, conducting a regular impact assessment and reporting annual audit results when necessary, establishing special PI processing rules for children, etc. In addition, businesses should also be prepared to integrate such efforts with their ESG initiatives to adopt governance requirements and fulfill social responsibilities.

For more information, please visit our China Updates page or see the following resources:

China Publishes Interim Measures for the Management of Generative Artificial Intelligence Services, August 7, 2023

Mexico Nearshoring: Opportunity for Manufacturers in China and the U.S., April 5, 2023

China MIIT Releases Data Security Management Measures for Industrial and Information Technology Sectors, February 20, 2023

A New Guideline Added to China's Data Protection Framework, August 17, 2022

China Revises its Anti-Monopoly Law 14 Years After its Initial Implementation, July 26, 2022

China Releases Judicial Interpretation of Anti-Unfair Competition Law, April 28, 2022

Select Proposed Changes to the Company Law of the People's Republic of China, March 22, 2022

A Snapshot of China's Cyberspace Administration and Data Protection Framework, February 9, 2022

China Intensifies Regulations on Cryptocurrency Trading and Mining, November 2, 2021

China's Amended Administrative Penalty Law Took Effect on July 15, October 8, 2021

China Issues New Rules Regulating Personal Information Collection by Mobile Apps, April 28, 2021

A New Gateway to China – Recent Policy Developments in the Hainan Free Trade Port, April 6, 2021

China Issues Measures for the Security Review of Foreign Investments, February 9, 2021

China Patent Law Fourth Amendment—Impact on Foreign Companies, January 26, 2021

China Regulators Remove Restrictions on Insurance Fund Investment, December 14, 2020

China Adopts Interim Provisions on the Review of Concentrations of Business Operators for the Anti Monopoly Law, November 30, 2020

China Releases Draft Personal Data Protection Law for Comments, November 12, 2020

China Adopts Export Control Law, November 5, 2020

China Releases New QFII/RQFII Rules, October 27, 2020

China Releases Provisions on Strengthening the Supervision of Private Equity Investment Funds (Draft), October 15, 2020

China Releases Provisions on the Unreliable Entity List, October 5, 2020

China Releases Revised Measures on Handling Complaints of Foreign-Invested Enterprises, September 23, 2020

China Releases Administrative Measures for Strategic Investment by Foreign Investors in Listed Companies, September 10, 2020

China Releases Draft Data Security Law, September 8, 2020

China Releases Circular on Further Stabilizing Foreign Trade and Foreign Investment, August 24, 2020

China Releases Draft Measures for the Administration of Imported and Exported Food Safety, August 18, 2020

U.S. Listed Chinese Companies: Regulatory Scrutiny and Strategic Options, July 30, 2020

China Passes Controversial Hong Kong National Security Law, July 9, 2020

China's Relaxed Financial Sector May Aid Foreign Investors, June 18, 2020

Is There a Law in China Similar to the US Defense Production Act?, May 8, 2020

Coronavirus Brings Force Majeure Claims to LNG Contracts, March 4, 2020

The Rise of China, March 4, 2020

Coronavirus Fears Cast Cloud Over Dealmaking, February 27, 2020