

On Network Information Contents Ecological Governance Provisions

By David Pan | Susan Deng | Tony Zhang

The Cyberspace Administration of China has recently reviewed and approved the *Provisions on the Ecological Governance of Network Information Contents* (the "Provisions"), which will officially take effect on March 1, 2020. The Provisions for the first time brings forward the concept of "network ecological governance", systematically and comprehensively elaborates on the governance objects, governance criteria, relevant subjects' obligations and responsibilities, legal liabilities, regulatory cooperation and other contents.

Origin of Network Ecological Governance

Originally a biology concept, "Ecology" refers to a unified whole formed by lives and the environment in a certain space in nature. In the unified whole, lives and the environment interrelate and interact with each other, and within a certain period of time, maintain a relatively stable dynamic equilibrium. The Internet ecology refers to a holistic environment in which the entities involved in Internet activities interact with each other to enable the stable development of the Internet world.

如果您需要本出版物的中文本,
请联系:

Publication@llinkslaw.com

For more Llinks publications,
please contact:

Publication@llinkslaw.com

Cyber ecosystem is a system composed of various elements of civilization, which mainly includes network subjects, network information, network technology, network infrastructure, network policies and regulations, and network culture.¹ The Provisions at the stage of seeking public opinions was named as "Network Ecological Governance Provisions", and the words "Information Contents" were added to the title when the Provisions were officially issued. Combining the specific contents of the Provisions, we note that the Provisions focuses on targeted governance of network information elements in the cyber ecosystem.

Before the Provisions was issued, regulations in the legal regime of China regarding Internet information contents / ecological governance were scattered in various laws and regulations:

Article 12 of the <i>Cybersecurity Law</i>	Individuals and organizations shall not engage in activities, by making use of the network, which spread violent and pornographic information, fabricate and disseminate false information to disrupt economic and social orders, or infringe upon the reputation, privacy, intellectual property and other legitimate rights and interests of others.
Article 47 of the <i>Cybersecurity Law</i>	A network operator shall strengthen the management of the information released by its users. If it finds any information that is prohibited by laws and administrative regulations from release or transmission, it shall immediately cease transmission of such information, and take measures such as deletion to prevent dissemination of such information. The operator shall also keep relevant record, and report the case to the competent authority.
Article 15 of the <i>Administrative Measures on Internet Information Services</i>	An internet information service provider shall not produce, duplicate, publish or disseminate the following information which: (1) are against the fundamental principles set out in the Constitution; (2) endanger national security, leak state secrets, incite to overthrow state power, or undermine the national unity; (3) damage the State's honor and harm the interests of the State; (4) incite ethnic hatred and ethnic discrimination or undermine solidarity among all nationalities; (5) undermine the State's policies on religions, and advocate religious cults and feudal superstition; (6) disseminate rumors to disrupt social order and undermine social stability; (7) disseminate obscene materials, advocate gambling, violence, killing and terrorism, or instigate others to commit crimes; (8) humiliate or defame other persons or infringe the legitimate rights and interests of the others; and (9) are otherwise prohibited by laws and administrative regulations.
Article 5 of the <i>Administrative Measures on</i>	Entities and individuals may not make use of international connections to produce, reproduce, consult or transmit any of the following content: (1) that which incites defiance or violation of the Constitution, laws or administrative regulations;

¹ Fu, Z., Wang, H. and Wang, Y. (2015). Review on a Ten-Year Research on Ecological Issues in Chinese Internet Speech. Development and Research, 6.

Security Protection for International Connections to Computer Information Networks	(2) that which incites subversion of State power and the overturning of the socialist system;
	(3) that which incites national division and harms national unification;
	(4) that which incites hatred and discrimination among nationalities and destroys national unity;
	(5) that which fabricates or distorts the truth, spreads rumors or disrupts social order;
	(6) that which spreads feudal superstition, involves obscenities, pornography, gambling, violence, murder, horrific acts or instigates criminal acts;
	(7) that which openly humiliates another party or slanders another party through a fabrication of the truth;
	(8) that which damages the reputation of a State organ; or
	(9) other content which violates the Constitution, laws or administrative regulations.

Worldwide Governance Practices of Network Information Contents

With the increasing impact of the Internet on real life, in terms of the extensive governance practices worldwide nowadays, creating healthy and clean cyber ecology has become the common goal of the international community. In this context, how to regulate the expression of speech in open and shared cyberspace has become a new topic of national legislation. Because countries differ in culture and face different cybersecurity threats, each country have adopted significantly different governance policies for Internet information contents:

- Germany passed the *Social Media Management Law* in 2018, which strengthened the supervision towards social media network platform providers, including imposing reporting obligations on platform providers, creating responsibility of proactively blocking and removing illegal speech, in order to restrict inappropriate expressions on social media; clearly classifying the content of information, and dividing information into three categories: speech of defamation, slander, neo-Nazi and incitation to violence, speech that apparently violates laws, and speech of controversy.
- The United Kingdom comprehensively adopts a two-pronged approach, "industry self-regulation + government supervision", to regulate cyber rumors, establishes the "Internet Monitoring Foundation" to address internet pornography, internet rumors and other issues, and encourages industry self-regulation and public reporting.
- France has passed the *Anti-Fake News Act*, which focuses on tackling false information, mainly political rumors.
- Russia has passed the *Internet Defamation Act*, which allows the government to regulate websites which post information that slanders public figures. Russia recently also successfully held a national-level "network disconnection" exercise to test whether the government and competent departments are capable to maintain online services under any circumstances, especially under external cyber-attacks (which may include political incitement using social media).

Similar with the practices of other countries, the Provisions regulates adverse information (such as pornography and violence) and illegal information (such as rumors and slander). Moreover, by implementing the classification strategy, the Provisions also encourages producing, copying and posing "positive energy information".

Major differences between the Provisions and its exposure draft

- Add the *National Security Law* as one of the top-level legal bases of the Provisions.
- Specify the network ecological governance to ecological governance of "network information contents".
- Adopt the "cultivating and practicing core values of socialism" as the basic principle of ecological governance of network information contents.
- Add information that promotes "inciting terrorism and extremism" as illegal information that is prohibited from being produced.
- Replace "no producing adverse information" with "taking measures to prevent and resist production of adverse information".
- Delete information that promotes lifestyles of wealth flaunting and money worship, extravagance and decadence, from adverse information.
- Add the responsibility of "developing the ecological governance outline of the network information contents of the platform, improving user registration and account management" for the network information content service platform (hereinafter referred to as the "Platform")
- Replace the prohibited behavior of "bulk trading accounts" with "falsely registering accounts".
- Add requirements of "establishing detailed rules for content review criteria, guiding member entities to establish and perfect service specifications, and accepting social supervision", and revise the requirement of "establishing evaluation reward and punishment mechanisms" to "promoting the construction of industry credit evaluation systems" for industry associations.
- Add the requirement of cooperation for Platforms in the process of supervision and inspection by the cyberspace administrations and competent departments.

Highlights of the Provisions:

I. Clearly classify network information contents and implement classified management

The Provisions divide all network information contents into three categories: positive energy information (information that is encouraged to be produced, reproduced, and released), illegal information (information that is not allowed to be produced, reproduced, and released), and adverse information (information that should be prevented and resisted)², and the content of each type of information is listed in detail (see the list after the paragraph). For example, the Provisions encourages to produce, reproduce and release information that displays the highlights of economic and social development, and reflects the

² Relevant persons in charge of the Cyberspace Administration of China answered questions from reporters on the *Provisions on the Ecological Governance of Network Information Contents*.
<http://www.npc.gov.cn/npc/c30834/201912/163c24c5594d41efbbc860dc6d0ef8f3.shtml>

hard-working and positive life of the masses. It is not allowed to produce illegal information that spreads rumors and disturbs with economic and social order, insults or slanders others, or infringes upon the reputation, privacy and other legitimate rights and interests of others. The production of any adverse information that uses an exaggerated title to present seriously inconsistent contents shall be prevented and resisted.

The detailed enumeration serves as a guide for the entire process of information flow, clarifies the upper and lower limits of content standards, and brings the focus of ecological governance of information contents to source control. The release and review of information by network information practitioners can be carried out in accordance with the Provisions.

1. It is encouraged to produce, reproduce and release information with contents as follows:
(1) those propagating Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era, and interpreting the road, theory, system and culture of socialism with Chinese characteristics in a comprehensive, accurate and vivid way; (2) those publicizing the theory, guidelines and policies of the Party and the major decisions and arrangements of the Central Committee; (3) those displaying the highlights of economic and social development, and reflecting the hard-working and positive life of the masses; (4) those carrying forward socialist core values, publicizing excellent moral culture and the spirit of the times, and fully demonstrating the positive spirit of the Chinese nation; (5) those effectively responding to social concerns, explaining doubts, analyzing issues with reasons, and being conducive to guiding the masses to reach consensus; (6) those conducive to enhancing the international influence of Chinese culture and presenting a real, three-dimensional and comprehensive China to the world; and (7) those stressing taste, style and responsibility, eulogizing the truth, virtue and beauty, and promoting unity and stability.
2. Producers of network information contents shall not produce, reproduce or release illegal information containing any of the following contents:
(1) those opposing the basic principles determined by the Constitution; (2) those endangering the national security, disclosing State secrets, subverting State power or damaging national unity; (3) those harming the honor or interests of the State; (4) those distorting, vilifying, desecrating or negating the deeds or spirit of heroes and martyrs, or infringing upon the names, portraits, fame or honors of heroes and martyrs in an insulting or defamatory way or otherwise; (5) those promoting terrorism or extremism, or inciting terrorist activities or extremist activities; (6) those inciting ethnic hatred or discrimination to undermine ethnic unity; (7) those sabotaging state religious policies or propagating heretical teachings or feudal superstitions; (8) those spreading rumors and disturbing the economic and social order; (9) those disseminating obscenity, pornography, gambling, violence, homicide, terror or instigating

others to commit crimes; (10) those insulting or slandering others, or infringing upon the reputation, privacy and other legitimate rights and interests of others; and (11) any other content prohibited by laws or administrative regulations.
3. Producers of network information contents shall take measures to prevent and resist the production, reproduction and release of any adverse information with the following contents:
(1) those using an exaggerated title to present content seriously inconsistent with the title; (2) those speculating in gossip, scandal or notoriety, etc.; (3) those improperly commenting on natural disasters, major accidents or other disasters; (4) those containing sexual innuendo or sexual teasing or others that are easily suggestive of sex; (5) those causing physical or mental discomfort such as bloodiness, horror and cruelty; (6) those inciting mass discrimination or regional discrimination, etc.; (7) those preaching tasteless, vulgar and kitsch contents; (8) those probably inducing minors to imitate unsafe acts or acts violating social morality, or inducing minors to have unhealthy hobbies; and (9) any other content that has an adverse impact on cyber ecology.

II. Clearly classify all relevant subjects involved in ecological governance of network

The Provisions points out that the main subjects involved in the ecological governance of network information contents include network information contents producers (hereinafter referred to as “Producers”), Platforms, users of network information contents services (hereinafter referred to as “Users”), network industry associations, and the cyberspace administrations at all levels. The Provisions systematically stipulates the roles and corresponding responsibilities of these five main subjects chapter by chapter. In summary, Producers shall comply with the requirements for the release of three types of information content for source controlling purpose; Platforms shall appoint a person-in-charge for ecological governance of network information contents to conduct audit control and technical management of the network information Platforms transmit; Users (netizens) shall assume the role of “public opinion supervision” and abide by regulations on the use of network information services, for example, insulting or slandering others, or infringing upon the reputation, privacy and other legitimate rights and interests of others shall be prohibited; network industry associations shall establish and perfect an industry self-regulation mechanism, and shall play a leading role in regulating and standardizing; cyberspace administrations at all levels have the right to supervise and inspect the performance of information content management obligations of Platforms, establish an accounting management system for the illegal activities of Platforms.

III. Closely integrate with the current Internet technology innovation

For example, Article 12 regulates that Platforms which adopt a personalized algorithm recommendation technology for delivering information, shall set up a recommendation model that meets the requirements of the Provisions, and establish and perfect a mechanism for human intervention and secure users’

independent choice; Article 23 regulates that Users, Producers, and Platforms shall not engage in activities prohibited by laws or administrative regulations by using new technologies or applications such as deep learning or virtual reality; Article 24 regulates social hotspot issues such as traffic fraud, false registration that disrupt the order of cyber ecology.

From the perspective of industry development, emerging technologies such as personalized algorithms and deep learning play a vital role in improving user experience and establishing a network information contents ecosystem. Although the technology improves information content distribution efficiency, it also brings about new problems, such as user privacy infringement and information cocoons. Together with other relevant provisions in the *Administrative Measures on Data Security (Exposure Draft)*, the Provisions sets forth clear regulations on hotspot issues and specifications for new technologies, which reflects the determination of the regulatory authorities to stay on top of the cyber ecology governance. Therefore, regardless of the identity as a Producer, Platform, or User, emerging technologies should be dealt with discretely. The algorithm model should be continuously and carefully optimized in a timely manner, and managed appropriately by manual intervention.

IV. Introduce the concept of building credit management system and credit evaluation system

Compared with previous laws concerning network contents governance, such as the *Cybersecurity Law*, the *Administrative Measures on Internet Information Services*, the *Regulations on Internet News Information Services*, the Provisions for the first time introduced the concepts of building credit management system and credit evaluation system. According to the Provisions, Platforms shall establish a user account credit management system and provide corresponding services according to the user's credit; industry associations are encouraged to promote the development of an industry credit rating system, establish industry appraisal and other evaluation reward and punishment mechanisms in accordance with association bylaws. From the perspective of Producers and Users, violations of the requirements set forth in the Provisions will directly affect their online accounts and corresponding services; Platforms could be punished by industry associations for any violations.

In addition to the above highlights, there are still parts of the Provisions that need to be further explained and clarified. For example, Article 12 of the Provisions specifies that Platforms which adopt a personalized algorithm recommendation technology for pushing notifications, shall set up a recommendation model that meets the requirements of the Provisions, and establish and improve a mechanism for human intervention and securing users' independent choice. Understandably, human intervention is to ensure that the network information content published by Platforms conforms to the three types of network information content stipulated by the Provisions. Meanwhile, users' "right of independent choice" should also be guaranteed, which makes the cyber governance a paradox. As a result, the so-called "right of independent choice" of users is restrained by the requirements of the Provisions, and this echoes another expression for the "users withdrawal right from personalized recommendation mechanism" proposed by the *Administrative Measures on Data Security (Exposure Draft)*. For another example, Platforms are required to appoint a person in charge of ecological governance of network information contents, but how to determine the specific job responsibilities of such

person? Is this position equivalent to what is now commonly known as the “network administrator”? After establishing a credit management system and credit evaluation system, how to “provide corresponding services according to the credit information of the user account” and how to avoid new types of discriminatory service behaviors?

Article 6 of the *Cybersecurity Law* stipulates that the State advocates network practices in a good-faith, trustworthy and civilized manner, promotes dissemination of core socialist values, and adopts measures to raise social awareness of cybersecurity in order to create a sound environment for the promotion of cybersecurity with the participation of the public. The management system and specific and directional requirements established in the Provisions are the response, implementation and refinement of such general requirements of the *Cybersecurity Law* on the management of network information contents. It is obvious, from the full text of the *Provisions*, that all the requirements are condensed from the practical experience in managing network information contents and organizing network platform contents. Enterprises involved in the publication and dissemination of network information contents should re-examine the existing content management system, implement the requirements set forth in the Provisions as soon as possible, and strengthen the control of network information contents.

If you would like to know more information about the subjects covered in this publication, please contact:



David Pan

+86 21 3135 8701

david.pan@llinkslaw.com

For any further questions on this subject or other business consultation,
please feel free to contact us: master@llinkslaw.com

SHANGHAI

T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING

T: +86 10 8519 2266
F: +86 10 8519 2929

HONG KONG

T: +852 2592 1978
F: +852 2868 0883

LONDON

T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by LLinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

© Llinks Law Offices 2020