ISSN 2616-5775 Vol. 5, Issue 14: 72-81, DOI: 10.25236/AJCIS.2022.051412

On Data Security Protection Obligations of Internet Service Providers

Lu Dingliang[1], Shan Yifei[2]

[1]Law School, Beijing Normal University, Beijing, China
[2]Hillary Rodham Clinton School of Law, Swansea University, Swansea Wales, the United Kingdom

Abstract: *Multiple legal departments must coordinate for internet service providers to meet their data security protection duties. The data security requirement of ISPs necessitates the coordination of multiple legal entities. Observing the data protection obligations of Internet service providers through the lens of a single legal department or a single regulatory regulation is skewed. A better strategy is to concentrate on the issue at hand and to think broadly. By constructing a comprehensive and multi-level data security protection obligation system for Internet service providers based on the "behavior-consequence" model, it is possible to realize the conceptualization and systematization of norms and develop a comprehensive picture of data security. The normative framework of data security protection for ISPs must be constructed using abstract notions, legal principles, and external systems. The "rule-principle" style of legal system construction enables the synchronization of formal and substantive justice, as well as stability and correctness. The normative framework focusing on data security protection is favourable to Internet service provider compliance governance. Effective compliance governance can make ISPs more attentive to the use and security of data.*

Keywords: *ISPs; data security; logic structure of legal norm; system constructure; compliance regulation*

1. Introduction

In the era of big data and artificial intelligence, data has emerged as a new production factor. As the actual controller of production factors, the network operator has accomplished the transition from neutral data distributor to data producer.[1]It is common practice domestically and internationally to require network operators to assume certain data security protection responsibilities. There are a large number of regulatory documents in China's legal system that adjust the data security protection obligations of network operators. These documents pertain to various legal departments, including civil, economic, administrative, and criminal.[2] Due to improper data storage, the network operator may leak the personal information of network users, resulting in economic losses for those users.[3]In this instance, the network operator's data security protection obligations involve tort law; and in the case of cross-border data flow, the state authorities urge the network operator to fulfill its data security protection obligations and restrict the export of sensitive data, which involves economic security and administrative law between the network operator and the state (authorities). Observing the data protection obligations of network operators through the lens of a single legal department or a single normative document is biased.[4]Taking the issue as the focal point and evaluating it holistically is a more effective strategy.

2. The abstract notion of data security protection requirements

The primary characteristic of the system is the material's unified order.[5]The normative system construction for network operator data security protection must be completed with abstract concepts, legal principles, and external systems. In contrast to the hierarchical construction mode based solely on rules, the rule-principle mode allows the legal system to achieve system coherence, and its evaluative function, while pursuing formal justice, also pursues substantive justice and substantive value. The rule-principle model, on the other hand, can achieve both the correctness and the stability of the law. [6]

2.1 Pair of suppositional classifications

Every legal order consists of two elements: the subject and object of rights.[7]However, due to the

ISSN 2616-5775 Vol. 5, Issue 14: 72-81, DOI: 10.25236/AJCIS.2022.051412

limitation of "rights" , the applicability of this statement is somewhat restricted, i.e., to the legal hierarchy of equal subjects. There are both subjects and objects of legal orders or legal relations. For instance, the subject of data security protection would be the network operator and the object would be the data. The description of this pair of categories is assumed because different legal departments, or even different legal norms within the same legal department, utilize distinct textual narrative strategies. Regarding "non-strict indicative words," it is necessary to specify their reference meaning.[8]The clarity of the concept's connotation depends on determining its distinction from other concepts.[9]Therefore, the method of concept analysis should be used to determine the similarities and differences between texts in the practice of law. [10]

2.1.1 Network Administrators

A coherent system of data security regulations must begin with a unified subject of obligation. In our legal system, different conceptual terms are used to describe the subject of obligations, giving rise to two questions: How do the various titles relate to one another? What is an acceptable type of network operator?

A network service provider is the title of the required subject adopted by the Regulations on the Protection of the Right to Information Network Dissemination and the Tort Liability Law, which is carried over into the Civil Code. The Network Security Law identifies network operators as "network owners, administrators, and providers of network services."[11]This definition appears to differentiate between network operators and network service providers, establishing a clear distinction between the two. In reality, however, there is no distinction between network operators and network service providers for the reasons listed below: By way of ownership, civil subjects can privatize websites or network infrastructure, but the network, as an abstract behavioral space, does not meet the requirements to become an object of rights. Consequently, the term "network owner" cannot be established normatively. If the owner of a website or network infrastructure does not offer network services, then data security protection is not required. In addition, the network operator provides network services and manages cyberspace, which is both a legal and ethical requirement for network services. [12]Following the Network Security Law's definition, the network's owners and administrators continue to be network service providers. The title of owner and manager is not a subject type that the legislator intends to expand, but it is intended to further illustrate the possibility of the network service provider's identity rights coexisting. In other words, a network service provider also owns and manages a website or network infrastructure.

The Regulations on the Protection of the Right to Information Network Dissemination classify network service providers into four categories: transmission service providers, caching service providers, information storage service providers, and search link service providers. Different exclusion clauses are stipulated for each category. This classification is effective because of the nature of the right to network information dissemination. The purpose of the right of information network dissemination is to make the work accessible to the public at its discretion. The stable storage of the work by the network service provider is the most important technical aspect of realizing the right of transmission over an information network. Transmission service providers and caching service providers that temporarily store works for informational transmission play a secondary role in the process of information network transmission of works and are thus more likely to enter "safe harbor." Long-term storage service providers who copyright and store protected works must adhere to stricter conditions to avoid liability. Whether or not a network operator stores information in a stable and long-term manner has no bearing on its obligations concerning data security protection.

It is accurate, as Kelson asserts, that "We are at liberty to define the terms we employ in our intellectual endeavors.[13] The only question is whether or not they will serve the intended theoretical purposes." The legislative purpose of the data and cybersecurity regime is to protect cyberspace sovereignty and national security, the public interest, and the legitimate rights and interests of citizens, legal entities, and other organizations. To determine whether a network operator must comply with data security protection obligations, it is crucial to determine whether its data processing behavior may endanger the aforementioned legal interests. This standard is reflected directly in the Data Security Law, which divides data processors into data processors of critical information infrastructure and other important data processors. The Network Security Review Measures requires network operators to declare network security review when they go public abroad if they possess the personal information of more than one million users. [14]In summary, an effective classification method divides network operators according to the significance of their data processing into network operators of critical information infrastructures, network operators that handle important data, and other network operators. Network

ISSN 2616-5775 Vol. 5, Issue 14: 72-81, DOI: 10.25236/AJCIS.2022.051412

operators of critical information infrastructures have the most stringent data security protection responsibilities. Even though the State Council has not yet clarified the precise scope of critical information infrastructure, it is possible to determine that the network operator with the personal information of more than one million users is at least one of the network operators that manage essential data. In general, other network operators are not required to actively declare the review; however, if it is deemed necessary to conduct a network security review, other network operators must also cooperate.

2.1.2 Data

Any element in a language must depend on its distinctions from other elements to exist.[15] Consequently, describing the relationship between data and information is essential for the conceptual analysis of data. Step-by-step development of the description is possible on three levels: In terms of semantics, are data and information the same thing? Is there a normative distinction between data and information under the real-definition approach? Finally, do artificially-assigned meanings have any practical application for data security protection obligations?

No is the answer to the first question. The most recent version of the present Chinese dictionary stipulates that data "Information is "news," which is "the movement change of people or things" Information is "news," which is "the motion or transformation of people or things." [16]To avoid the influence of linguistic difference, the comparison does not continue to inquire about the meanings of "value" and "situation," but instead turns to an empirical analysis of actual word usage. Although data and information are not the same things in common usage, they are not a formal contradiction but rather a dialectical-logical unity of opposites. For instance, "send information to users" and "send data to users" have distinct meanings, whereas "analyze user data" and "analyze user information" are synonymous. According to the theory of information, the purpose of the information is to eliminate the uncertainty. Consequently, the processed data will become information. In semantics, there is a partial intersection between data and information.

The second question also has a negative response. Although there is a semantic distinction between data and information, the law does not recognize this distinction. If the normative system recognizes the distinction between two legal phenomena, the most intuitive manifestation of this is the juxtaposition of the phenomena as separate legal facts.[17] Regarding the classification of network service providers, the aforementioned Regulation on the Protection of the Right to Information Network Dissemination is one example. On the other hand, the normative system does not recognize their differentiation, as evidenced by their varying use of data and information. For instance, the Data Security Law stipulates that "(state organs) shall keep confidential the data such as personal privacy, personal information, commercial secrets, and confidential business information known in the course of performing their duties and shall not disclose or illegally provide them to others"; however, data and information are interpreted interchangeably. The Shenzhen Special Economic Zone Data Regulations, for instance, use the information to define the term data. "data" refers to any record of information stored electronically or otherwise. Therefore, in our legal system, the distinction between data and information is not normatively relevant. [18]

The answer to the third inquiry remains negative. The convergence of their relationship in substantive law does not preclude the investigation of their contingent dimensions. There are two schools of thought regarding the contingent relationship between data and information: "data-information monism" and "data-information dualism." Monism holds that data and information are identical and that "it is impossible to separate data from information and discuss data rights in the abstract";[19] dualism advocates separate adjustment of data and information and asserts that separate adjustment is useful in practice. The legal significance of the distinction lies in the fact that the issue of network information data can be divided into three types: data issues, information issues, and mixed issues; the more moderate dualism argues that data and information are highly symbiotic and shared; "there is no need to strictly distinguish in the use of legal concepts." Data has a broader scope than information, but personal data and personal information are essentially identical.[20]Evaluating the impact of dualism on the data security protection obligations of network operators, i.e. determining whether network operators should be subject to different security protection obligations based on the distinction between data and information.

Consider the following reasons for distinguishing between data and information: First, there is an objective data problem, such as the virtual property problem. In addition, there are purely informational concerns, such as the issue of intellectual accomplishments. In addition, data is separated into data files at the symbolic level and data information at the content level, with different adjustment methods. Personal information and data files have different legal implications; thirdly, information is meaningful

ISSN 2616-5775 Vol. 5, Issue 14: 72-81, DOI: 10.25236/AJCIS.2022.051412

data. Differentiating the two can lay the groundwork for a consensus regarding the information protection and data rights system. However, for network operators' data security protection obligations, the reasons for the distinction are insufficient: First, the concerns of network information security and network data security almost completely overlap; second, mere data files do not pose a threat to data security, and the data security protection obligations all point to the data information of the content layer; and finally, security protection issues have nothing to do with the meaning and content of data, but only consider the data and data processing capabilities. The security protection issue has nothing to do with the meaning and content of data, but rather with the potential security risks of data and data processing.

The distinction between data and information is irrelevant to data security protection obligations. The central tenets of data (information) classification should be whether or not the data is identifiable and whether or not they are of public interest. This is because the identifiability and public interest of data determine the limits of data used by network operators as well as the legal liability for breaching security protection obligations. Consequently, the types of data with practical roles are as follows: identifiable data and anonymous data based on whether the data contains information that can be used to identify a specific natural person; public data and non-public data based on whether the data is of public interest.

2.2 Several abstract concepts

The external system is constructed from abstract concepts. The interpretation work contributes to the construction of the system. The subject of the normative system's obligation - network operators - can be divided into three categories. Network operators of critical information infrastructure, network operators of significant data processing, and additional network operators. The required object of the normative system, data, can be broken down into four categories: identifiable data, anonymous data, public data, and non-public data. The classification of data can be derived from three essential abstract ideas: data security, data ownership, and data power.

2.2.1 Data protection

According to the dualism theory, the right object is an abstract category that refers to the interest embodied by the right object.[21]The object of rights is a concrete category that contains interests such as objects, behaviors, and data. According to this perspective, data is the subject of data security protection obligations, and data security is its subject. Nonetheless, a conceptual analysis of data is still required, as the clarification of the concept of data security is dependent on the definition of data.

Data security entails ensuring that data are effectively protected and lawfully utilized, as well as having the ability to guarantee a continuous state of security by taking the necessary precautions. Data security obligations imposed on network operators include the following: Data processing security, i.e., network operators ensuring legal compliance in the process of data collection and usage. The security of data dynamics is the security of data processing. Data storage protections. The operators of a network should safeguard their stored data against theft, tampering, deletion, and other threats. The security of data statistics is the security of data storage. Before providing data outside of the country, network operators should seek approval from the appropriate authorities.

2.2.2 Ownership of data

The issue of data ownership is the possession of data as an object of rights. Data ownership is the overarching principle of data security.[22] Personal data, enterprise data, and government data are included in the classification of different rights subjects for data ownership.[23] Individuals are the primary source of data generation, and the distinguishing characteristic of personal data is its identifiability in comparison to other types of data. Since personal data are generated by natural persons and can reflect the various activities of particular natural persons, natural persons hold the initial position of predominance concerning personal data. Personal data is non-public data.

Enterprise data and government data are both public data. Enterprise data consists of information generated by businesses in the course of their operations. After anonymization, network operators can convert the personal information of users into enterprise data. Government data are data collected by administrative organs as part of their statutory responsibilities. When the government is involved in data activities, not only is it the owner of government data, but it also manages data security. Since data is a "public good," the public interest should limit the ownership of data by right holders.

2.2.3 Data power

Data power only refers to public power in its broadest sense,[24] i.e., the ability of state authorities

ISSN 2616-5775 Vol. 5, Issue 14: 72-81, DOI: 10.25236/AJCIS.2022.051412

to collect, utilize, and dispose of data to preserve the public interest and national security. Data power is a particular application of the national sovereignty principle to the issue of data protection. Both government data rights and data powers involve the collection, use, and disposal of data. In contrast, when state organs exercise data powers, consent is generally not required for the processing of personal and business data. For instance, the processing of personal data in response to public health emergencies and the prohibition on the export of enterprise data are examples of state agencies exercising data power. Nonetheless, the exercise of data power must adhere to certain principles, including the principle of legal power and the principle of unity of authority and responsibility, and should coordinate the relationship between the exercise of power and data property rights.

3. The legal principles governing obligations for data security protection

Morality enters the legal system through legal principles, which not only have a normative effect but also reflect the value pursuit of the legal system. In contrast to the rule system, legal principles do not solve the problem of competing principles through an "all-or-nothing" approach, but rather by comparing which principle is more significant in a given situation;[25] the solution of competing principles also reflects the concept of proportionality. For instance, the public interest principle and the fair use principle may conflict, and resolving the conflict requires weighing the relative importance of the two principles. The normative system constructed using legal principles can realize the Supreme People's Court's principle of "organically combining legal evaluation with moral evaluation, deeply explaining the national value objectives, social value orientations, and civic value guidelines embodied in laws and regulations and realizing the rule of law and moral governance" Complementary and mutually supportive requirements.

3.1 The Proportionality principle

The obligation to adhere to the principle of proportionality to the greatest extent possible.[26] Rejecting the proportionality principle is equivalent to rejecting the proportionality doctrine. The principle of proportionality is derived from optimization commands; consequently, it is the most prevalent legal principle. The concept of necessity and adequacy, which is embodied in the principle of proportionality, is also incorporated into other legal principles. The essence of the hproportionality principle is "to adjust the rational relationship between means and ends and to assist in establishing a reasonable scale for the exercise of power and rights."[27] Therefore, the principle of proportionality mandates that network operators keep the means and ends of their data activities proportional. In the obligation system of network operators, proportionality is expressed as the proportionality of data handling and the proportionality of responsibility.

The proportionality of data processing necessitates that network operators accomplish their data processing goals with the fewest resources possible. Article 6(2) of the Personal Information Protection Law, for instance, states that "the collection of personal information shall be limited to the minimum extent necessary to achieve the processing purpose, and no excessive collection of personal information shall be permitted." Data collection practices that go beyond the required scope will result in legal liability. The cybersecurity level protection system is an example of proportionality in responsibility assumption. "Those who benefit from the enterprise are also responsible for its costs." This also implies that the enterprise should bear costs proportional to its gain. To reconcile means and ends, the obligation system classifies network operators as network operators of critical information infrastructure, network operators handling important data, and other network operators, and requires them to bear varying degrees of legal responsibility.

3.2 Public Interest principle

The public interest principle is the embodiment of the proportionality principle's concept of necessity. The public interest principle mandates that network operators conduct data processing activities and research and development of new data technologies that are conducive to promoting economic and social development, enhancing people's welfare, adhering to social morality and ethics, and assuming social responsibility. Network administrators should select data processing techniques that are more advantageous to the public. The public interest principle is the origin and purpose of network operators' data security protection obligations.

ISSN 2616-5775 Vol. 5, Issue 14: 72-81, DOI: 10.25236/AJCIS.2022.051412

3.3 Fair Use Principle

The principle of fair use embodies the notions of proportionality and appropriateness. The fair use principle stipulates that, in the context of data security protection, data security and industrial development should be accorded equal weight, and that the relationship between data security and data utilization should be balanced. The objective of the fair use principle is to "strike a balance between the protection of individual rights, the growth of the digital economy, and the distribution of data profits." In the fundamental principles of economic law, the principle of fair use has the same weight as the principle of balance and coordination. The principle of balance and coordination requires the legislation and law enforcement of economic law to adjust and coordinate specific economic relations from the perspective of the coordinated development of the national economy and the overall interests of society, as well as to promote the unification of the overall goals of society and individual interests. [28]

4. The external system of obligations for data security

In our jurisprudence, it is commonly held that any legal norm consists of two components: behavior patterns and legal consequences. To maintain the unity of legal order and scientific governance of the network ecological environment, the "behavior-consequence" model should be used to construct a holistic and multi-level system of network operators' data security protection obligations, to realize the conceptualization and systematization of norms, and to form a panoramic view of data security care.

4.1 Two modes of conduct

Typically, obligatory norms consist of two types of behavior patterns: should behave in this manner and should not behave in this manner, i.e., "command and prohibit."[29]In a general sense, imperative norms require network operators to fulfill their data security protection obligations, whereas prohibitive norms require network operators to refrain from illegally processing data. The Civil Code and the Criminal Code contain mandatory requirements governing the data security protection obligations of network operators. The Civil Code outlines the security protection responsibilities of owners and managers of commercial properties and public spaces.[30] Cyberspace is where network operators conduct business.[31]Network operators must fulfill their security obligations, which include not only the protection of the person and their property but also the security of the information network.[32] As a general crime, the Criminal Law imposes criminal liability on network operators who refuse to fulfill the obligations of information network security management. The criminal circumstances that are governed include: (1) causing the widespread dissemination of illegal information; (2) causing the disclosure of user information; and (3) causing the loss of evidence in criminal cases.

The Network Security Law and the Data Security Law impose mandatory and prohibitive requirements on network operators' data processing practices, respectively. (1) shall prevent network data leakage, theft, or tampering; (2) shall collect user information after expressing it to users and obtaining consent; (3) shall require network users to provide real identity information before providing relevant services; (4) shall develop emergency plans for network security incidents; (5) shall promptly address system vulnerabilities and other security risks; and (6) shall pro-actively address system vulnerabilities and other security risks. (1) shall not terminate security maintenance in advance; (2) shall not collect personal information unrelated to its services; and (3) shall not disclose, alter, or destroy the personal information it collects.[33] The latter stipulates that the command mode of conduct must include the following provisions: (1) shall specify the person responsible for data security and management institutions, the implementation of protection responsibilities; (2) shall strengthen the monitoring of risk, the discovery of data security flaws; and (3) must take immediate action in response to data security incidents. No unauthorized transfer of domestic information to foreign institutions is a prohibited behavior pattern[34]

By comparing the aforementioned behavioral patterns, it is straightforward to determine that the data security protection obligations formulated by various norms not only have different foci but also differ in specific content. The Cybersecurity Law seeks to ensure the stable and operable state of the network, i.e. network operation security, and the integrity, confidentiality, and availability of network data, i.e. network information security, both of which pertain to the content of data security. It encompasses the broadest spectrum of data security. Personality and property rights remain the starting point for security obligations, as stipulated by the Civil Code. For instance, the improper handling of data by the network operator leads to leakage, which in turn causes damage to the property rights of network users.[35]

ISSN 2616-5775 Vol. 5, Issue 14: 72-81, DOI: 10.25236/AJCIS.2022.051412

Liability of the network operator for damages resulting from the failure to meet safety and security obligations. The Personal Information Protection Law does not extend the information protection obligations of network operators beyond the scope of this system. The Network Security Law is the complete antecedent law norm of the Criminal Law for the crime of failing to comply with the responsibilities of information network security management. The relevant criminal acts of network operators need not violate the Civil Code's security guarantee obligations, but they must violate the Network Security Law.

4.2 Three types of legal repercussions

Only negative legal consequences, i.e. legal liability, are referred to in this context. Network operators who violate mandatory regulations will incur three types of legal liability: tort liability, administrative liability, and criminal liability. Among them, the Network Security Law, the Data Security Law, and the Criminal Law all stipulate that supervisors are directly responsible for network operators' legal liability. Except for a few advocacy norms,[36] normative behavior patterns correspond with legal consequences. Notably, the newly published "Network Security Review Measures " stipulates that network operators holding the personal information of more than one million users must declare network security review before going public abroad.[37] This requirement relates to the recently adopted trading rules for foreign company securities by the U.S. Congress.

The U.S. Foreign Company Accountability Act requires foreign companies going public in the U.S. to disclose documents beyond unqualified audit reports, and the SEC will have the authority to determine whether audit working papers are required.[38]An audit report is a written document in which the CPA expresses an audit opinion, among other things. Using the example provided by the American Institute of Certified Public Accountants, an audit report consists primarily of non-confidential introductory paragraphs, scope paragraphs, and opinion paragraphs.[39]In contrast, the audit working papers are the records of the CPA's audit work created during the audit.[40] It contains records of significant matters of the audited entity, such as incoming and outgoing emails, and meeting minutes. The contents of audit work papers about data security can be reverse-engineered, as audit work papers typically contain trade secrets and strategic intelligence attributes.

Fundamental to legal doctrine is the legal interpretation of the preceding data security standards. The higher-order function of legal dogmatics is the conceptualization and systematization of norms.[41] Components and structure make up the system's primary elements. [42]The actual law's component unity is a prerequisite for systematization. Therefore, the fundamental activity of legal interpretation is a prerequisite for the system's higher-order mode of operation.

4.3 Six protection rules

Legal principles serve as the system's subordinate norms, constituting its building blocks. Legal rules and legal principles can constitute a "chain of effective norms." The construction of the external system of norms is based on the following methodology: abstracting and generalizing the legal facts of the object of adjustment, and then forming concepts of varying degrees of abstraction by adding or removing certain characteristics. The external system of data security protection is constructed using the "act-consequence" model, which ultimately forms the framework of data security protection obligations centered on legal issues, using abstract concepts as the building blocks. The external data security protection system should be developed with the following considerations in mind.

4.3.1 Legal data collection and usage

Network operators who collect users' personal information must obtain and document their consent. In addition, it must keep the collected information strictly confidential. The network operator must disclose the collection and use rules, as well as the purpose, manner, and scope of personal data collection and use. Network operators may not collect personal data unrelated to the services they provide, nor may they collect, use, process, or provide personal data to third parties in violation of applicable laws, administrative regulations, and the parties' agreement.

4.3.2 Prevent data loss and leakage

Network operators are required to take technical and other measures to ensure the security of collected personal data to prevent information leakage, destruction, and loss. In the event or possibility of personal data leakage, destruction, or loss, the company must immediately take corrective action, following the provisions of the timely notification of users, and notify the appropriate authorities. Important systems

ISSN 2616-5775 Vol. 5, Issue 14: 72-81, DOI: 10.25236/AJCIS.2022.051412

and databases should also be backed up by the operators of the networks that support the critical information infrastructure.

Network operators must establish complaints and reporting systems for network information security, publish complaints, reporting methods, and other information, and receive and process complaints and reports about network information security promptly.

4.3.3 Data security threat mitigation

Network operators are required to take precautions against data security threats and create contingency plans for network security incidents. Data security flaws, vulnerabilities, and other risks discovered shall take immediate corrective action; for data security incidents, shall immediately initiate the emergency plan, take disposal measures, by the provisions of the timely notification of users and report to the appropriate competent authorities.

Significant data processors are required to conduct regular risk assessments of their data processing activities and submit risk assessment reports to the relevant competent authorities. At least once a year, the operator of critical information infrastructure must inspect and assess the security and potential risks of its network, either independently or with the assistance of network security services.

4.3.4 Data exit security administration

Without the approval of the competent authorities, the network operator may not provide data stored on the territory to foreign judicial or law enforcement agencies. The data collected and generated on the territory by the operators of vital information infrastructure should be stored on the territory. Provided outside the country, a security assessment must be developed by the national network information department and the relevant departments of the State Council. As a network operator, handling sensitive data, such as the personal information of more than one million users, to foreign listings requires a network security review.

4.3.5 User release data administration

For network operators to provide users with network access, domain name registration services, fixed-line, cellular phones, and other network entry procedures, or to provide users with information dissemination, instant messaging, and other services, the user should be required to provide real identity information. If users do not provide accurate identification information, network operators should not provide relevant services.

Network operators should be the management of information released by its users, and if they discover that laws and administrative regulations prohibit the release or transmission of information, they must immediately stop transmitting the information, take steps to eliminate and other disposal measures to prevent the proliferation of information, save the relevant records, and report to the appropriate competent authorities.

4.3.6 Administrative data oversight

To provide data processing-related services, a network operator must obtain an administrative license, under applicable laws and administrative regulations. Network operators should cooperate with public security organs and state security organs to maintain national security or crime investigation data, and should provide technical support and assistance to the public security organs and state security organs for the maintenance of national security and crime investigation activities. Through the implementation of supervision and inspection, network operators from the relevant departments must work together.

5. Conclusions

For Internet service providers, the subject of data security protection security must consider regulatory management and legal requirements of the sector from various legal departments' views. This includes the formation of a unified topic of responsibility, a precise understanding of the meaning and ownership of data, and the attribution of data collection authority and the scope of authority while keeping the public interest in data in mind, among other things. At the same time, Internet service providers must understand the legal principles of data security protection obligations, adhere to the principle of proportionality to the greatest extent possible, and complete data processing in the most efficient way possible following the proportionality of data processing; the principle of public interest is also fundamental and consistent in data security protection work, with the healthy development of society. The public interest principle is also essential in data security protection activities, which must

ISSN 2616-5775 Vol. 5, Issue 14: 72-81, DOI: 10.25236/AJCIS.2022.051412

be consistent with healthy social and economic development and strike a balance between the goal of improving people's welfare and social ethics. Current legislation, such as the Cybersecurity Law, the Data Security Law, and the Criminal Law, achieves a good balance between Internet service providers' behavior and the various laws that ensure the integrity, confidentiality, and availability of data while respecting users' personal and property rights. As a result, ISPs must take steps to ensure lawful data collection and use, as well as to prevent data loss and address potential leakage risks. It is also critical for ISPs to develop contingency plans to address data security threats and to prevent and avoid potential and known risks in advance. The data security protection obligations of internet service providers involve the joint adjustment of multiple legal departments. It is biased to observe the data protection obligations of Internet service providers from the perspective of a single legal department or a single normative document. A better approach is to focus on the "behavior-consequence" mode. Effective compliance governance can make ISPs to properly use and protect the data.

References

[1] Zhang Linghan (2021), "The Platform's Data Security Obligations under the Data Production Theory", in Law Forum, No. 2, p 49.
[2] Data protection responsibility of the controller under Chapter 4 of the EU General Data Protection Regulation
[3] Please refer to Shenjin v. Alipay (China) Network Technology Co., Ltd, etc., Civil Judgment of Beijing Chaoyang District People's Court. [2018] Beijing 0105 civil case No. 36658.
[4] Zhang Xiaojun (2020), "A Model and Reference for Rule Construction of Data Sovereignty — On Rule Construction of Data Sovereignty in China", Modern Jurisprudence, No.6, pp. 137-138.
[5] Xie Hongfei (2018), "The External System Benefits of Civil Code and Its Expansion", Global Law Review, No. 2, p.30.
[6] Lei Lei (2016), "Legal System, Legal Methods and the Rule of Law", China University of Political Science and Law Press, pp.55-57.
[7] Medicus, Dieter, "The Foundations of the Right of Claim", translated by Chen Weizuo, Tian Shiyong, Wang Hongliang and Zhang Shuanggen(2012), Law Press, p.16.
[8] Kripke, "Naming and Necessity", translated by Mei Wen, edited by Tu Jiliang and Zhu Shuilin(2002), Shanghai Translation Press, p.29.
[9] Fang Weigui (2020), "What is Conceptual History", Life · Reading · Xinzhi Sanlian Bookstore (preface), pp. 3.
[10] Zhu Zhen(2016), "A Conceptual Analysis of Analytical Jurisprudence", Legal System and Social Development, No. 1, p.146.
[11] Item 3, Article 76 of the PRC Cybersecurity Law, promulgated by the National Peoples' Congress, PRC.
[12] There is a view that the core concept of the CyberSecurity Law is "cyberspace security." For details, see Shou Bu(2017), "An Analysis of Some Basic Concepts of the CyberSecurity Law," in Technology and Law, No. 4, pp. 6-8.
[13] Kelsen, Hans(2013), "The General Theory of Law and the State", translated by Shen Zongling, Commercial Press, p. 31.
[14] Article 7 of the CyberSecurity Review Measures, jointly issued by Cyberspace Administration, National Development and Reform Commission, Ministry of Industry and Information Technology, Ministry of Public Security of and Ministry of State Security, etc, PRC .
[15] Ferdinand de Saussure(2011), "Manuscripts in General Linguistics, organized and edited by Simon Bouquet and Rudolf Engler", translated by Yu Xiuying, Nanjing University Edition, pp.53-54.
[16] Modern Chinese Dictionary (2016)edited by the Dictionary Editorial Office of the Institute of Language, Chinese Academy of Social Sciences, The Commercial Press, p.1216, p.1437, p.1461.
[17] Jiang Yongzhuo(2014), "Differing Language": A Reconsideration of Derrida's Criticism of Saussure, "in Foreign Language Journal, No. 6, p. 4.
[18] Article 38 of the Data Security Law, promulgated by the National People's Congress, PRC
[19] C. E. Shannon(1948), "A Mathematical Theory of Communication", The Bell System Technical Journal, No.27, p.389.
[20] Item (1) of Article 2 of the Regulations of Shenzhen Special Economic Zone on Data, promulgated by the Shenzhen Municipal People's Congress, PRC .
[21] Cheng Xiao(2018), "On Personal Data Rights in the Era of Big Data," Chinese Social Science,No 3 , pp.105-106.
[22] Ji Hailong, "Private Law Position and Protection of Data," Chinese Journal of Law, 6 (2018), pp.73-76.

ISSN 2616-5775 Vol. 5, Issue 14: 72-81, DOI: 10.25236/AJCIS.2022.051412

[23] Mei Xiaying(2020), "The Legal Significance of Distinguishing the Concepts of Information and Data," Comparative Law Studies, No.6, pp.155-159.
[24] Peng Chengxin and Xiang Qin(2019), "The Private Law Definition of" Information "and" Data ", in Henan Social Science, No. 11, pp. 30-35.
[25] Liu Deliang(2014), "The Distinction and Significance between the Object of Right and the Object of Right in Civil Law", Jinan Journal (Philosophy and Social Sciences), No.9, p.8.
[26] Wang Qinghua(2021), "The Right Structure, Legal Effect and Chinization of Data Portability Right", China Law Review, No.3, p.191.
[27] Shi Dan(2018), "A Study on Data Ownership and Its Protection Path in the Era of Big Data," in Journal of Xi 'an Jiaotong University (Social Sciences), No. 3, pp.79-81.
[28] Zhang Xiaojun (2020), "The Model and Reference of Data Sovereignty Rule Construction —Also on the Rule Construction of Data Sovereignty in China", Modern Law, No.6, p. 137.
[29] Shu Guoying (2019), "Introduction to Jurisprudence", Peking University Press, pp. 113-114.
[30] Alexi (2012), "Law: Institutionalization as Rationality", translated by Lei Lei, China Legal Publishing House, pp. 136-138.
[31] Liu Quan (2021), "Dispute and Reflection on the Application of the Principle of Proportionality," in Comparative Law Research, No.5, pp. 177-180.
[32] Dworkin, Ronald. "Justice in the Robe", translated by Zhou Lingang and Zhai Zhiyong, Beijing University Press, 2014, p. 167.
[33] Ji Weidong (2018), "A Multidimensional Perspective on the Right to Data Protection", Politics and Law, 10. 2021, p.11.
[34] Shi Jichun and Deng Feng (2001), "Economic Law: An Introduction", Law Press,No.2, p.158.
[35] Shen Zongling (2014), "Jurisprudence", Peking University Press, p.28.
[36] Article 1198 of the Civil Code, promulgated by the National People's Congress, PRC.
[37] Wang Siyuan (2017), "On the Security Obligation of Network Operators," in Contemporary Law, No. 1, p.32.
[38] Leading Group for the Implementation of the Civil Code of the Supreme People's Court, ed. "Understanding and Application of Tort Liability Part of the Civil Code of the People's Republic of China", People's Court Publishing House(2020), pp.284-287.
[39] Article 286 of the Criminal Law, promulgated by the National People's Congress, PRC.
[40] Articles 21, 22, 24, 25, 28, 37, 40, 41, 42, 47 and 49 of the Cybersecurity Law,PRC.
[41] Refer to the tort liability dispute between Li Zhong v. Wuhan Guanggu Sub-branch of China Merchants Bank Co., Ltd. and Wuhan Branch of China Mobile Communications Group Hubei Co., Ltd., the civil judgment of second instance issued by Wuhan Intermediate People's Court of Hubei Province, Hubei 01 civil case [2019] No. 5119.
[42] For example, Article 9 of the PRC Cybersecurity Law, promulgated by the National Peoples' Congress, PRC.