2021 International Conference on Big Data, Artificial Intelligence and Risk Management (ICBAR) | 978-1-6654-9565-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICBAR55169.2021.00011

Research on Big Data Security and Privacy Risk Governance

XinRui Wang
Cybersecurity and Data Compliance Team, ANLI PARTNERS
Beijing, China
rxwang@anlilaw.com

Wei Luo
Cybersecurity and Data Compliance Team, ANLI PARTNERS
Beijing, China
wluo@anlilaw.com

XiaoLi Bai
Cybersecurity and Data Compliance Team, ANLI PARTNERS
Beijing, China
baixiaoli@anlilaw.com

Yi Wang
State Grid Zhejiang Electric Power Company Hangzhou Power Supply Company
Hangzhou, China
ruth_wang@foxmail.com

***Abstract*—In the era of Big Data, opportunities and challenges are mixed. The data transfer is increasingly frequent and speedy, and the data lifecycle is also extended, bringing more challenges to security and privacy risk governance. Currently, the common measures of risk governance covering the entire data lifecycle are the data-related staff management, equipment security management, data encryption codes, data content identification and de-identification processing, etc. With the trend of data globalization, regulations fragmentation and governance technologization, "International standards", a measure of governance combining technology and regulation, has the potential to become the best practice. However, "voluntary compliance" of international standards derogates the effectiveness of risk governance through this measure. In order to strengthen the enforcement of the international standards, the paper proposes a governance approach which is "the framework regulated by international standards, and regulations and technologies specifically implemented by national legislation." It aims to implement the security and privacy risk governance of Big Data effectively.**

Keywords- Big Data Security and Privacy; Risk Governance Points; International Standards

I. INTRODUCTION

The concept of "Big Data" was systematically introduced by American data scientist Viktor Mayer-Schönberger as early as 2010, and since then, the opportunities and challenges brought by Big Data have attracted widespread attention from the whole international community. On May 29, 2012, the United Nations "Global Pulse" program released the White Paper entitled "Big Data Development: Opportunities and Challenges", which analyzes the opportunities and challenges brought by the data revolution triggered by the development of Big Data. In general, Big Data brings three main challenges for the international community: Big Data security, Big Data privacy, and Big Data application.

The risks and challenges posed by Big Data can basically be divided into two tiers, which are the basic tier and the extended tier. As a main force in the process of technological development, Big Data poses a central and fundamental position. However, the security and privacy governance of Big Data determine whether it can be developed steadily. Besides, the Big Data application is extended further, which is used for subjective analysis.

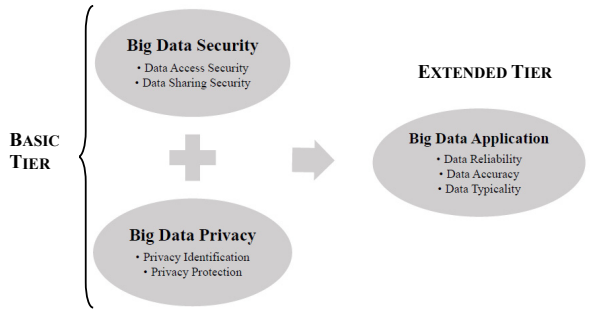

Figure 1. Risk tiers

It can be seen that Big Data security and privacy are two pillars in the development of Big Data risk governance, which are supposed to be put high on the agenda by the international community.

II. MATERIAL

The systematic risk governance points have been gradually formed with the international community's studies on Big Data security and privacy deepening and the present risks being more comprehensive and detailed.

From a horizontal perspective, the points of Big Data security and privacy governance for the international community fall into different governance domains. The governance of Big Data security risks mainly focuses on the physical and logical dimension, which means the security of staff and equipment involved are required in the physical aspect and the security of encryption code is essential for the virtual space. Besides, the governance of Big Data privacy risks mainly focuses on the context dimension, which means

978-1-6654-9565-3/21/$31.00 ©2021 IEEE
DOI 10.1109/ICBAR55169.2021.00011

the privacy protection is achieved through the identification and process of the context of data.

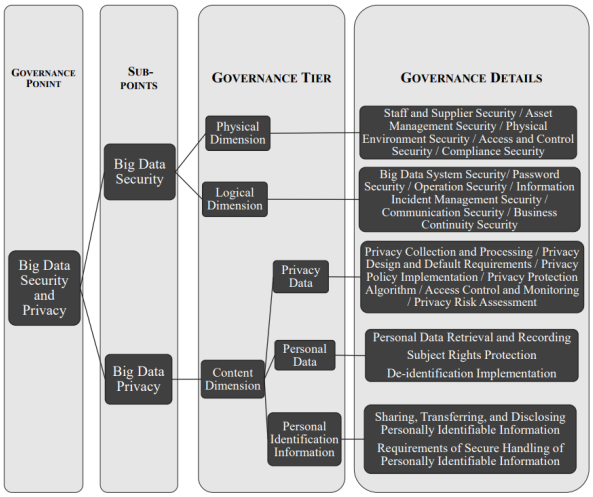

Figure 2. Corresponding specific risks

In addition, from a vertical perspective, points of Big Data security and privacy risk governance cover the process of data collection, data storage, data modification, data application, data publication and data deletion throughout the entire lifecycle of data [1].

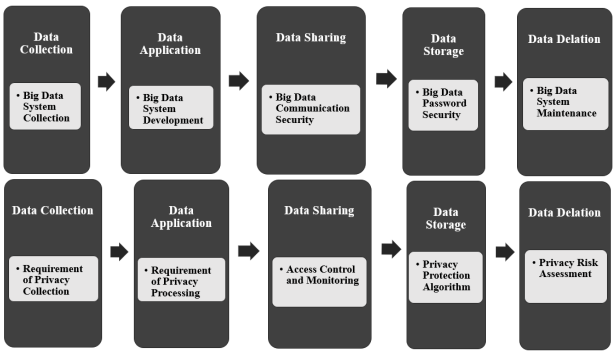

Figure 3. Risk points corresponding to the data lifecycle

Meanwhile, the international community interprets the connotation of "privacy" liberally. Some types of personal data and identifiable personal information that are not interpreted as "privacy" strictly are protected in the same level of "privacy" data [2].

It can be seen that Big Data security and privacy risk governance led by the international community has penetrated into different areas of data and the whole data lifecycle. Besides, the risk governance covers more types of data.

III. Discussion

A. Obstacles to Implementation of Risk Governance Points

Although the international community has formed a more comprehensive understanding of the security and privacy risk governance of Big Data, the nature of Big Data makes it difficult to implement these risk governance measures.

1) Globalization of Data

The contradiction between the globalization of data and the regionalization of governance is the first obstacle to implementation.

In the background of the data revolution, a large amount of data is generated and flows through different channels and from different sources. The trend of data globalization is irreversible since data hold a core position of global digital activities, coupled with the demand for cross-border data flow in multiple domains of trade, technology, politics, and security. In addition to the data globalization, the speed and frequency of emitting and transmitting data is increasing plus the more various sources and other conditions, which makes the "data deluge" emerge in the international community. Based on these phenomena, the implementation of the data governance fails to be achieved only through the efforts of single or localized sovereign states.

The globalization of data requires that the risk governance of Big Data should be structured at the global level. However, global data governance, which aims to regulate the security and privacy, is still in its infancy, and the development of corresponding regulations is seriously lagging. For the impact of COVID-19, the long-absent international data governance is even more inadequate. The area of data security and privacy, which needs comprehensive international governance, is still in the mode of "separate governance" by sovereign states.

2) The Fragmentation of Norms

There are two main pieces of fragmentation of norms for data security and privacy.

The first fragmentation refers to the existence of different norms for regulating data related to different social subsystems. For example, legislation related to security governance in different areas of critical infrastructure shows different patterns [3].

TABLE I. Regulations Related to Data Security for Different Areas of Infrastructure

Areas of Infrastructure	Rules
Finance	Gramm-Leach-Bliley Act (GLBA); Federal Securities Laws
Medical	Health Insurance Portability and Accountability Act (HIPPAA)
Energy	Guide to Industrial Control Systems Security Cyber Security Assessment Guide for Electric Power System Supervision and Control （GB/T 38318-2019）

The second fragmentation means that different regions and nations enjoy different levels of data security and privacy protection. For example, the U.S., the EU, and Russia share distinctive characteristics in this aspect [4].

TABLE II. NORMS INVOLVED IN PRIVACY DATA GOVERNANCE IN DIFFERENT SOVEREIGN STATES

States & Regions	Basic Rules
United States	Cross-border flow of privacy data is allowed with no ex-ante assessment of the level and condition of privacy protection of the states and regions which the data flows to, but it put emphasis on post-privacy infringement remedies.
EU	To a certain extent, cross-border flow of privacy data is allowed, and ex-ante assessment of the level and condition of privacy protection of the states and regions which the data flows to must be conducted, and the flow of data is allowed only when the standards established by the EU are met.
Russia	Cross-border flow of privacy data is NOT allowed, and Russia will comply with *the principle of Data Localization*

During the G20 Summit in Osaka 2019, fifteen member states still pursued the policy of data localization to varying degrees, despite agreement on the Data Free Flow with Trust Draft (DFFT) [5]. The process of data security and privacy risk governance remains unintegrated and still suffers with two pieces of fragmentation.

3)Technologization of Governance

It is essential for the digital technology to develop the governance of data security and privacy. Compared with the regulation in traditional areas, the governance of Big Data security and privacy cannot only rely on laws or other norms alone. The technical approaches such as algorithms and codes also matter.

In the era of rapid development of digital technology, the assertion that "code is law" [6] as stated by Lawrence Lessig in *Code 2.0* has been generally recognized by the international community. In the process of digital technology development, the first path for data security and privacy governance lies in code, which is also known as the technical governance. Technological governance via certification, authentication, encryption, screening, trace tracking, etc., enjoys a higher level of effectiveness than any other methods.

B.Existing Means of Implementing Risk Governance Points

There is an urgent need for a new governance paradigm which combines technical governance and regulatory governance for data security and privacy.

The governance of Big Data security and privacy relies on technical approaches, but that may inevitably produce deviations in the process of safeguarding data security and privacy due to their own loopholes, which may violate individual human rights and even public interests. Therefore, a novel path which refers to the mixture of norms and technologies is proposed. From the current practice of the international community, such approach of co-regulation is to establish an "international standard".

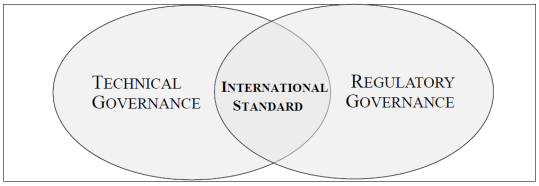

Figure 4. Governance relationship chart

The mode of the international standardization can also solve the other two obstacles mentioned above. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) both have a wide range of member states, and their international standards can solve the problem of regionalization of governance. And the structured nature of international standards has the possibility to cover multi-domain governance requirements. The principle of norms can include specific fragmented regulations to form a relatively integrated system of governance.

Therefore, international standards play an important role in the risk governance of Big Data. ISO/IEC has the following international standards and draft standard for comments related to Big Data security and privacy: ISO/IEC 20547-4 "Information technology — Big Data reference architecture — Part 4: Security and privacy", ISO/IEC 27045 "Information technology — Big Data security and privacy — Processes", and ISO/IEC 27046 "Information technology — Big Data security and privacy — Implementation guidelines".

ISO/IEC 20547-4 describes the Big Data security and privacy framework only from a functional perspective, ISO/IEC 27045 regulates from an arrangement perspective, and ISO/IEC 27046 further indicates the guidelines governing Big Data security and privacy from an implementation perspective based on both perspectives above. International standards are becoming increasingly practical, concluded by the development process of all the international standards [7].

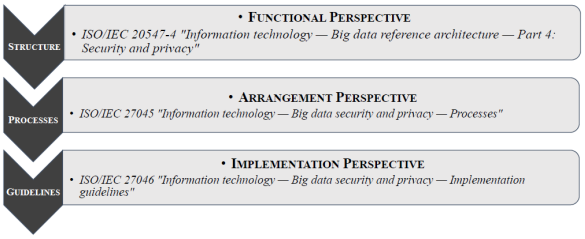

Figure 5. International standard relationship chart

C.Improvement of Implementing Risk Governance Points

ISO has been known as the global "United Nations of Technology", and it plays a positive role in Big Data security and privacy governance. Both ISO and IEC are private, non-profit organizations. International standards support the process of globalization in various fields through the coupling of technologies and norms, but it is still fundamentally based on the principle of "voluntary compliance". Although they play an important role in international trade and are generally respected by the international community, the effectiveness of "voluntary compliance" is likely to be limited due to the discrepancies in the development of digital technologies, national security, and human rights among nations.

The definition of standard officially published in the context of ISO/IEC (2004) is that "standard is a kind of document established by consensus and approved by a recognized body, that provides for common and repeated utilization, rules, guidelines or characteristics for activities or their results to establish a best practice. However, the "best" of order is an unquantifiable concept in practice and consequently the international standards only propose guidance. How to

implement international standards is at sovereign states' or enterprises' discretion. And different countries can form their own best practice in accordance with their domestic status quo and enforcement.

Considering that the limited effectiveness of international standards and the significance of Big Data security and privacy risk governance, different countries are supposed to implement the points of Big Data risk governance through domestic legislation based on international standards. The first path is to enforce the international standards directly, turning them into domestic legislation. The second path is to specify the domestic norms referring to the international standards. Both ways can lead to the best practice in the aspect of security and privacy in their countries.

Now, sovereign states have regarded the international standards as guidance for domestic legislation. However, it is worth mentioning that enterprises are actually pioneers to promote the transformation or refinement of domestic legislation currently, which means the naturalization of laws is a bottom-up process. In the initial period, enterprises rely on international standards for cross-border operations and voluntarily comply with international standards, and then the government refers to voluntary standards to form mandatory norms to reach the goals of Big Data risk governance.

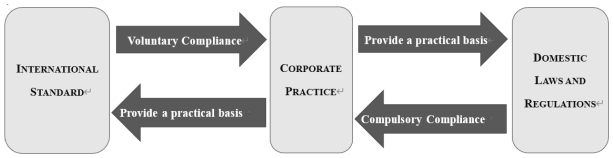

Figure 6. The relationship chart of International standards and domestic regulations

At this time, despite the governance of Big Data security and privacy by means of domestic legislation, the relevant legislation of each country is homogeneous because the domestic legislation is guided by the international standards, which can solve the difficulties in the process of security and privacy governance.

IV. Conclusion

International standards stipulated by ISO and IEC play an important role in the field of big data security and privacy governance, but the effectiveness in concrete implementation and operation is limited due to its basic principles and voluntary compliance. So, the specificity and mandatory of domestic legislation is necessary for the enforcement of the international standards. In conclusion, the most effective path of Big Data risk governance is "comprehensive regulation by international standards in terms of architecture, and concrete implementation by national legislation in terms of norms and technologies". Only through the cooperation of the international community and sovereign states can we make the regulation of Big Data security and privacy mature, grasping the opportunities in the era of Big Data.

Acknowledgment

This paper is a phased achievement of Science and technology projects of State Grid (Research on Key Legal Technologies of Power Data Ownership and Commercial Application, SGZJHZ00HLJS2000265).

References

[1]D.-G. Feng, M. Zhang, H. Li, "Big Data Security and Privacy Protection", Chinese Journal of Computers, vol. 64, no. 1, pp. 246–258, 2014.

[2]L.-X. Yang, "Personal information: legal interest or civil right", Legal Forum, vol. 33, no. 1, pp.34-45, 2018.

[3]Y.-N. Dong, G.-X. Zhao, Z.-X. Xie, "The practice of critical information infrastructure protection analysis", Cyberspace Security, vol. 9, no. 8, pp. 84-89, 2018.

[4]J. Hua, "Privacy in Internet Age—Comparison on internet privacy regulations between the United States and the European Union and its indication to internet privacy protection of China", Hebei Law Science, vol. 26, no. 6, pp. 7-12, 2008.

[5]D. Erdos and K. Garstka, "The 'Right to be Forgotten' Online within G20 Statutory Data Protection Frame-works", International Data Privacy Law, vol. 10, no. 4, pp. 7-8, 2020.

[6]L. Lessig, Code: And Other Laws of Cyberspace, 2nd ed, New York: Basic Books, pp. 5, 2006.

[7]L. Yu, F. Zhang, H. Y. Zhang, X. L. Shangguan, Y. Sun, Research on International Standard Proposal the Big Data Security and Privacy Implementation Guidelines, Topic on Data Security for International Standardization, vol. 8, pp.29-32, 2021.