Preventing the Risks of Cross–border Data Flows and Protecting National Information Securities

Hui Zhibin,
Director of Information Security Research Institute, Shanghai Academy of Social Sciences

Introduction>>

As the cyberspace grew gradually intellectualized and transformed the more realistic purification effect, the significance of the data security in cyberspace was highlighted. Big data has become a core strategic resource because of its openness and the competition for control. Against this background, the author analyzed the facts of cross-border data flows and the jurisdiction of data. He listed the elements distinguishing different data, proposed the two trends in response to managing data flows and the influence of data localization.

I. Background of Internet Data Security

Data security in cyberspace has been brought up for a long time, and its importance is much valued nowadays. Edward Snowdon has caused an international trust crisis which posed real challenge for the policies and laws in the international economic field. And this has brought an urgent demand for researchers and the academic field.

According to the statistics of daily Internet use around the globe and the relevant node ,we can conclude that the cyberspace and the real world is highly simultaneous in terms of active time, and geographically speaking, it responds to human habitats . We can say that the cyber world is highly integrated with the physical world.

However, two shifts are resulted in the physical world's overall datamation. First is the realization of an intellectualized cyberspace, which includes massage mapping, control of physical space and prediction of the future; Second is the purification effect, which has more realistic sense and is probable with the development of technology.

In the process, Big Data has become a core strategic resource. The reasons can be summed up as follows: First is its openness. The exploitation and the opening of cyberspace data resources including the developing wave of the United States, started years ago. Second is the competition for control. The competition around the global data is becoming more intensive and the space structure is optimizing around the world. As countries have been aware of the global data resource as a competitive and highly strategic resource, they are eagerly taking control of data resources at home and abroad.

II. Cross-border Data Flows and Jurisdiction of Data

1. Three Elements in Differentiating the Jurisdiction of Data

As data is a strategic resource, the jurisdiction of data has gained a relevant vital significance, which can be approached from three aspects.

First is the jurisdiction in the broad sense. Google, for example, is certainly under the jurisdiction of the US in the broad sense. That is the core element. The second element concerned is the server. If Google has set servers in the UK or other countries, the location of the servers definitely affects the jurisdiction of data. Thirdly, the citizenship of the people involved in the data can play a role. If the data of an Indian is saved in a UK server, India may have some jurisdiction.

2. Two Trends in Response to Managing Cross-border Data Flows

The jurisdiction of data brings two major problems, the fast mobility of data and the local... Two trends are prominent around the globe when coming to addressing the two problems. On the one side is the US, who extols freedom and fluidity. As a pioneer of data who claims the majority of the core resource, the US cannot promote freedom and fluidity of data flows more, just like some economic organizations are prone to promote the importance of economic development. Unlike the US, India, Israel, South Africa and New Zealand, most countries are on the other side and for protecting cross-border data flows. After the Snowdon event, the whole globe started to build a data security system. Russia, for example, promulgated laws in July last year to ensure that the operators store its citizen's data within its borders, and if the cross-border operators request cross-border data flows of a citizen, they must obtain a written authorization from the citizen. Because of the legal basis, the localized management has become acceptable around the world.

3. The Influence of Data Localization

In demonstrating the influence of data localization, the researchers at the US political research center revealed that if data localization be implemented overall, China will face a economic loss of 3 billion, including its international investment. In order to avoid such losses, the government can restrict on the corporate responsibilities rather than demand the operators to store the data in local facilities. Australia, Singapore and the Philippines are test on this. Internet in the future may be unlike Internet which is initially united, a locally facilitated mode instead may become popular.

III. Advise on Policies of Chinese Cross-border Data Flows

The US and the EU are advanced in terms of data security. Before the

outbreak of the prism, the two parties had deepened their cooperation, which included Safe Harbor Agreement and US-EU Data Sharing Deal, and the conflicts between the two will go through violent changes as a consequence of the globalized Internet. During the Prism event, the situation was rather tough, and EU ended the Safe Harbor Agreement and US-EU Data Sharing Deal. But the trust between the two is longstanding, and the Prism was only recent. When the US released big data, it gave special emphasis on the protection of its citizen's and its allies' information and facilitating fluidity.

From long run, the locally facilitated policies of cross-border big data flows adopted by China achieved dynamic balance. It has conditions and routes, and fits into the policies of data fluidity and exploitation. It is worth mentioning that the locally facilitating policy will play a role for a long time, especially in the core and strategic field.

Firstly, as one of the world's leading powers, we need to manage, acquire, and exploit data resources in a global context and explore how to manage data flows and hold dialogue with others.

Secondly, we should propel the innovation in data security and the industrialized development. Many of China's problems concerning information and data security are caused by our deficiency in safeguarding ourselves. The polarized policies may contribute to the dynamic balance and a protective mode as the technological innovation and the industrialized development take shape. The policies can be more open when China succeeds in uplifting its research and development

Thirdly, we should construct a strategic theory framework and actively promote the management of data security in an international context.

Fourthly, we should be cautious about the blockade that Chinese IT companies meet when going global. Some Chinese companies such as Huawei and Alibaba are upsurging, and these companies will become the developer and main applier of China's data resources. Our country should organize talents to analyze how to break the blockades of data security faced by these companies in the globalization process, and guarantee their safe travel abroad.

Fifthly, a basic requirement of national information security is that the data security and protection of private information must take the

people into consideration. Military powers is traditionally deemed as the principle guarantee of national security, but big data has become the basis of national information security as the age of big data is coming. It is an age values on building trust among the government, companies and people and mechanism for profit allocation.

Translator/ Li Qian