6 | 2019
20th Year
15 December 2019
P. 161–192

CRi

Computer Law Review International

A Journal of Information Law and Technology

cr-international.com

With Index 2018/2019

ottoschmidt

86203501906

pears to be sufficiently effective for ensuring that the person targeted by the defamatory statements is protected. On the other hand, that protection is not provided by means of an excessive obligation being imposed on the host provider, in so far as the monitoring of and search for information which it requires are limited to information containing the elements specified in the injunction, and its defamatory content of an equivalent nature does not require the host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies.

47 Thus, such an injunction specifically does not impose on the host provider an obligation to monitor generally the information which it stores, or a general obligation actively to seek facts or circumstances indicating illegal activity, as provided for in Article 15(1) of Directive 2000/31.

48 In the third place, although the referring court does not provide any explanations in that regard in the grounds for its order for reference, the wording of the questions which it addressed to the Court suggests that its doubts also concern the issue whether Article 15(1) of Directive 2000/31 precludes injunctions such as those referred to in paragraphs 37 and 46 above from being able to produce effects which extend worldwide.

49 In order to answer that question, it must be observed that, as is apparent, notably from Article 18(1), Directive 2000/31 does not make provision in that regard for any limitation, including a territorial limitation, on the scope of the measures which Member States are entitled to adopt in accordance with that directive.

50 Consequently, and also with reference to paragraphs 29 and 30 above, Directive 2000/31 does not preclude those injunction measures from producing effects worldwide.

51 However, it is apparent from recitals 58 and 60 of that directive that, in view of the global dimension of electronic commerce, the EU legislature considered it necessary to ensure that EU rules in that area are consistent with the rules applicable at international level.

It is up to Member States to ensure that the measures which they adopt and which produce effects worldwide take due account of those rules. 52

Conclusion

In the light of all the foregoing, the answer to the first and second questions is that Directive 2000/31, in particular Article 15 (1), must be interpreted as meaning that it does not preclude a court of a Member State from: 53

– ordering a host provider to remove information which it stores, the content of which is identical to the content of information which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information;

– ordering a host provider to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content, or

– ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.

In the light of the reply given to the first and second questions, it is not necessary to consider the third question referred. 54

Updates

China: The 2019 Draft Measures on Security Assessment of Cross-Border Transfer of Personal Information

The Cybersecurity Law of the People's Republic of China was issued on November 7, 2016, and officially put into effect June 1, 2017. The *Cyberspace Administration of China (CAC)* has released supportive measures to implement provisions of the Cybersecurity Law. These Draft Measures provide guidelines for cross-border transfer of data, data security assessments, and the protection of data in relation to national and public interest. In 2017, the CAC published Measures on Security Assessment of Cross-Border Transfer of Personal Information and Important Data. The draft received immense feedback, leading to a revised draft released in June 2019, Measures on Security Assessment of Cross-Border Transfer of Personal Information. The revised Draft Measures will affect a wide range of domestic and foreign entities in China that have cross-border transfer needs.

1. Separating "Personal Information" and "Important Data"

On June 13, 2019, the CAC released Measures on Security Assessment of Cross-Border Transfer of Personal Information. Regulations and guidelines provided in the draft pertain to network operators that export personal information data to recipients outside of China. It should be noted that the 2017 Draft Measures applied to both "important data" and "personal information" data. However, the 2019 Draft Measures omit the

term "important data" and solely focus on the export of "personal information." The removal of the term implies that the CAC is now treating "important data" and "personal information" as separate categories that are subject to different requirements.[1] Therefore, the content in the new Draft Measures only concerns the cross-border transfer of "personal information" collected within the territory of China.[2]

2. Data Localization Requirement

China's Cybersecurity Law requires data localization for "critical information infrastructure operators" (CIIO's) that collect and generate data within China. In other words, the provision requires that "personal information" and "important data" collected by CIIO's within the territory of China will be stored on Chinese servers. The 2017 Draft Measures attempted to bring clarification to this data localization rule. However, the 2017 Draft Measures expanded the data localization requirement to all "network operators," causing controversy and confusion in the international community. Since "network operator" is more vaguely defined than CIIO's, the 2017 Draft Measures broadened the scope for the data localization requirement.

To make things more complicated, the CAC published the 2019 Draft Measures without any mention of data localization requirements. Although there is no data localization provision in the new Draft Measures, it does not mean that network operators are exempt from data localization. Legal experts point out that China's Cybersecurity Law overlaps with the new Draft Measures, and CIIO's are still obligated to follow data localization rules. However, with the cybersecurity law referring to "CIIO's", and the 2019 Draft Measures only referring to "network operators," there is room for interpretation regarding what entities will be impacted by data localization requirements.

3. Data Security Assessment Guidelines

a) General Overview of Security Assessments

Network operators[3] are required to conduct data security assessments before the outbound transfer of "personal information".[4] While the 2017 Draft Measures listed the CAC as the primary coordinator for security assessments, the 2019 Draft Measures assign provincial-level cyberspace departments to perform data inspections.[5] In addition, every individual recipient of data requires a separate security assessment. However, the export of personal information several times to the same recipient does not require multiple assessments. Furthermore, network operators must perform a new security assessment every 2 years or in the case that "there are changes to the purpose, type, or overseas retention period related to the outbound transfer of personal information."[6]

b) Filing for Security Assessment

Network operators must file with a provincial-level cyberspace administration to organize a security assessment of the personal information to be exported. Network operators are required to submit specific documentation when requesting the assessment. Documents include a declaration form, the contract between the network operator and the recipient(s), and an analysis report on the security risk of the data. The provincial-level cybersecurity department will then conduct a security assessment within 15 working days. The time limit to complete the security assessment was reduced from the 2017 Draft Measures' timeframe of 60 working days.[7] However, some experts doubt the provincial CAC administrations will have the capacity to perform extensive amounts of security assessments within this established deadline.[8]

c) Results and Follow Up

Once the provincial-level cybersecurity department has conducted a security assessment of the personal information data, the department must notify the network operator of the results. Article 7 states that network operators can file an appeal with the CAC if the network operator objects to the results that the provincial-level cybersecurity department provides.[9] At the end of each year, network operators are obligated to report all personal information transfers of the calendar year to their provincial-level cybersecurity department, along with any other requested information. Furthermore, the provincial-level cybersecurity departments will conduct regular inspections of the outbound transfer of personal data by network providers to check on contract fulfillment, violations of rules or regulations, and protection of rights of the personal information subjects.[10]

1 "China Issues Draft Regulation on Cross-Border Transfer of Personal Information." Privacy &Information Security Law Blog. Hunton Andrews Kurth LLP, June 19, 2019. https://www.huntonprivacyblog.com/2019/06/19/china-issues-draft-regulation-on-cross-border-transfer-of-personal-information/.

2 "Personal information" is defined in the draft Measures as "various information recorded by electronic or other means that, alone or in combination with other information, can identify a natural person's personal identity, including but not limited to the name of the natural person, date of birth, ID number, personal biometric information, address, phone number, etc.").

3 Network operators are defined in the June 2019 draft as "network owners, managers, and network service providers."

4 L, Cindy, Mingli Shi, and Kevin Neville. "Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China." New America, June 13, 2019. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-crossborder-transfer-personal-information-out-china/. (Article 2).

5 Luo, Yan, Zhijing Yu, and Nicholas Shepherd. "China Seeks Public Comments on draft Measures Related to the Cross-Border Transfer of Personal Information." Inside Privacy, June 18, 2019. https://www.insideprivacy.com/international/china/china-seeks-public-comments-on-draft-measures-onsecurity-assessment-for-the-cross-border-transfer-of-personal-information/.

6 "China Issues Draft Regulation on Cross-Border Transfer of Personal Information." Privacy & Information Security Law Blog. Hunton Andrews Kurth LLP, June 19, 2019. https://www.huntonprivacyblog.com/2019/06/19/china-issues-draft-regulation-on-cross-border-transferof-personal-information/.

7 Sohu. Legal Executive Board, June 25, 2019. https://www.sohu.com/a/322835797_100055948.

8 "China Proposes More Stringent Rules on Security Assessment of Export of Personal Information: Insight: Baker McKenzie." Baker McKenzie, July 3, 2019. https://www.bakermckenzie.com/en/insight/publications/2019/07/china-proposes-more-stringent-rules.

9 Sohu. Legal Executive Board, June 25, 2019. https://www.sohu.com/a/322835797_100055948.

10 L, Cindy, Mingli Shi, and Kevin Neville. "Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China." New America, June 13, 2019. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-crossborder-transfer-personal-information-out-china/. (Article 10).

d) Security Assessment Details

The 2019 Draft Measures provide various details concerning security assessments including:

- Article 6 lists the type of information that is critical to the assessment, when cyberspace departments conduct a security assessment..
- Article 8 lists specifics on what the records should include, which network operators are required to maintain records of personal information data for five years.
- Article 9 lists the cases in which prohibition/suspension of the export of personal information by the cyberspace department is justified.
- Article 17 lists what type of information the analysis reports should include which network operators must provide describing the security risks of the outbound transfer of personal information.

4. Contracts Between Network Operators and Data Recipients

The 2019 Draft Measures provide contract requirements between the network operator and the data recipient. The following articles enumerate what the legal agreements should explicitly state:

- Article 13 lists general content that should be included in the contract between the network operator and data recipient.
- Article 14 and 15 defines the obligations of network operators and data recipients, which must be stated in the legal contracts.
- Article 16 describes the rules for when data recipients transfer personal information data to third-parties. These requirements must also be specified in the contract.

5. 2019 Draft Measures and Overseas Organizations

The 2019 Draft Measures mandate that overseas organizations that collect personal information of Chinese users on the internet are subject to the same rules and regulations as network operators in China.[11] To fulfill these obligations, foreign entities are required to go through a domestic legal representative or organization.[12] Since "network operators" is a broad term, it will have a sweeping effect on a variety of companies and industry sectors that collect personal data of domestic users in China.[13] Once the 2019 Draft Measures are implemented[14], foreign businesses that collect personal data in China may need to review their contracts with data recipients to ensure compliance. Overall, non-domestic companies that perform cross-border transfer of data should become familiar with the 2019 Draft Measures in order to navigate China's cybersecurity landscape.

6. The Impact of the 2019 Draft Measures on Foreign Businesses

In comparison to China's Cybersecurity Law, the 2019 Draft Measures widen the scope of who will be subject to data review and regulations. The 2019 Draft Measures concern all "network operators," which is broadly defined as "network owners, managers, and network service providers."[15] Consequently, the 2019 Draft Measures will impact multinational companies in a wide variety of industries and sectors that operate and use information networks in China. Foreign businesses that collect personal information data in the territory of China should prepare for compliance with the 2019 DraftMeasures. In addition to assessing the new obligations, foreign firms should also be aware of the challenges that may occur, such as administrative burdens, inefficient business operations, and new costs.

In general, the 2019 Draft Measures will make foreign business operations in China less efficient. This is largely due to the mandatory security assessments of the personal information data. For instance, the 2017 Draft Measures expected companies to perform self-assessments of personal data. This meant companies would be subject to government assessments only when reaching a threshold, such as exporting a high quantity of personal data or highly sensitive data. However, the 2019 Draft Measures require the government administrations to conduct security assessments of all outbound transfer of personal data, with no regard to the quantity or the sensitivity of the information. The consequence of this change is that even basic customer information or human resources information that a company collects in China would require a security assessment before the outbound transfer of the data.[16] Therefore, the 2019 Draft Measures create more obstacles for foreign businesses that frequently share data overseas.

Another way the 2019 Draft Measures may slow down foreign business operations is the ambiguous legal language that leaves companies vulnerable to the local cybersecurity administrations' control. For example, Article 5 states that security assessments should take place within 15 days, but that this period can be extended for "complex situations." Since it is unclear what the CAC considers a "complex situation", data security assessments could take longer than necessary before the local cybersecurity administrations permit the export. The CAC uses

11 Sohu. Legal Executive Board, June 25, 2019. https://www.sohu.com/a/322835797_100055948.

12 *L, Cindy*, *Mingli Shi*, and *Kevin Neville*. "Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China." New America, June 13, 2019. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-crossborder-transfer-personal-information-out-china/. (Article 20).

13 *Li, Barbara*, and *Bohua Yao*. "New Chinese Measures for Personal Data Cross-Border Transfer Security Assessments." Data Protection Report, July 1, 2019. https://www.dataprotectionreport.com/2019/07/new-chinese-measures-for-personal-data-crossborder- transfer-security-assessments/.

14 Currently expected for March 2020.

15 *L, Cindy*, *Mingli Shi*, and *Kevin Neville*. "Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China." New America, June 13, 2019. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-crossborder-transfer-personal-information-out-china/. (Article 21).

16 "Into the Eye of the Storm: Update on China's Long-awaited Data Export Review Measures." Hogan Lovells, July 2019.

similar obscure language in Article 3 of 2019 Draft Measures, where new security assessments will be carried out every two years unless there is "a change in the purpose of personal information export or a change in the overseas storage period."[17] Because it is also not specified what constitutes "a change in purpose", foreign firms could experience more security assessments in a given period. Therefore, the 2019 Draft Measures grant local cybersecurity administrations the authority and discretion to make security assessments more complicated for foreign firms.

Once the 2019 Draft Measures are implemented, foreign businesses will most likely have additional administrative burdens. For instance, network operators will need to provide various materials to the local cybersecurity administrations to declare a security assessment of the export of personal information. Such documents include an analysis report that will be tedious to produce and must consist of detailed information regarding the network operator and each data recipient. In addition, record keeping and reporting of personal information data will be additional administrative obligations. Records must contain specific information that is laid out in Article 8. Annual reports on the conditions of the personal information export must be submitted to the local cybersecurity administration by the end of each calendar year. Moreover, legal contracts will need to be updated between network operators and data recipients to comply with the 2019 Draft Measures. Multinational corporations will have to adjust to these time-consuming administrative tasks that are mandatory for data transfer overseas.

Lastly, foreign companies should be aware that the 2019 Draft Measures may significantly add to the cost of doing business in China. Many foreign firms do not have a presence in China but collect personal data from Chinese users online. In Article 20 of the 2019 Draft Measures, corporations such as these would be required to fulfill the obligations of the Draft Measures via "domestic legal representatives or organizations."[18] Therefore, obtaining a legal representative in China will be an extra cost to consider for some companies. Other expenses may go towards additional administrative assistance and management to ensure that the company is preparing and submitting documents in accordance with the regulations. In conclusion, foreign businesses that collect personal data of domestic users in China should prepare for the time and resources needed to comply with the 2019 Draft Measures.

7. Domestic Businesses

It is important to note that the 2019 Draft Measures do not solely apply to foreign businesses operating in China. Foreign firms in China do not face stricter regulations than domestic firms. The 2019 Draft Measures also apply to all domestic network operators that collect the personal information data of Chinese users. Overseas organizations are simply held to the same standards as domestic entities. Therefore, domestic and foreign firms are both responsible for fulfilling the same obligations when transferring personal information data overseas.

Attorney at law Daniel Albrecht

Guest Professor for Civil Law UWEE Beijing, China and Managing Counsel at Starke, Beijing

Corporate Law, Trademark Law, E-Commerce

law@beijing-starke.com

www.beijing-starke.com

17 *L*, *Cindy*, *Mingli Shi*, and *Kevin Neville*. "Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China." New America, June 13, 2019. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-crossborder-transfer-personal-information-out-china/. (Article 3).

18 *L*, *Cindy*, *Mingli Shi*, and *Kevin Neville*. "Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China." New America, June 13, 2019. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-crossborder-transfer-personal-information-out-china/. (Article 20).