BCLP. Client Intelligent

Insights

PART 4 OF 5: PENALTIES AND LIABILITIES UNDER CHINA'S DATA PROTECTION LAWS

Feb 19, 2022

SUMMARY

This article discusses briefly the various possible liabilities for data protection breaches under China's main laws, regulations and statutory instruments governing the protection of personal information.

INTRODUCTION

In Parts 2 and 3 of this series, we set out the main operative provisions in China's major data protection laws, regulations and instruments as identified by the Hong Kong Privacy Commissioner for Personal Data ("PCPD"). Those main operative provisions inform us of what principles and requirements are to be complied with. In this present article, we turn to discuss the possible consequences for failing of comply with China's data protection requirements.

In an Information Booklet[1] published by the Hong Kong's Privacy Commissioner for Personal Data ("PCPD") in November 2021, the PCPD set out the penalties and liabilities for breach of data protection requirements, and did so by reference to three main laws, namely (1) the Personal Information Protection Law ("PIPL"), (2) the Cybersecurity Law ("CSL"), and (3) the Law on the Protection of Minors.

We will consider, separately, statutory penalties, criminal liability and civil liability.

STATUTORY PENALTIES

The PIPL has attracted a lot of interest and attention by many companies doing business with Chinese citizens, perhaps primarily because it is a law which comes with possibly very hefty fines. The CSL and the Law on the Protection of Minors also contain penalty provisions which apply specifically to breaches of data protection provisions. The table below summarises the financial penalties provided by each of these laws:

	Penalties for the data handlers	Penalties for individual staff members responsible for the breach
§66 of the PIPL	Maximum fine of RMB 50,000,000 or an	Fine ranging from RMB 10,000

	amount which represents 5% of its revenue of the preceding year	to RMB 100,000
§§64-66 of the CSL	For breaches of the specified data protection provisions: - Where the amount of earnings derived from the breach exceeds RMB 1,000,000: fine equivalent to 1x to 10x of the amount of earnings derived from the breach - Where the amount of earnings derived from the breach does not exceed RMB 1,000,000: fine ranging from RMB 100,000 to RMB 1,000,000 For breaches related to cross-border data transfers: fine ranging from RMB 50,000 to RMB 500,000	
§127 of the Law on the Protection of Minors	Fine equivalent to a maximum of 10x of the amount of earnings derived from the breach (for breaches in relation to the handling of PI belonging to minors where the amount of earnings derived from the breach exceeds RMB 1,000,000)	

The maximum fine under the PIPL as stated above applies to failures to remedy “serious” breaches after having been warned by state authorities (provincial level or above). The PIPL does not further explain how “seriousness” is to be determined. Financial penalties under both the CSL and the Law on the Protection of Minors are determined with reference to the amount of earnings derived by the company from the offending act. These penalty provisions may shed some light on how “seriousness” would be determined under the PIPL.

There also are various non-pecuniary penalties provided under the PIPL. Offending companies may face warnings, correction orders, forfeiture of earnings, and/or orders for suspension or cessation of the relevant part of business. Responsible members of staff also may be faced with revocation of business permits and be prohibited from taking up directorate or senior management roles in related businesses for a certain period of time. The CSL and the Law on the Protection of Minors provide similar non-pecuniary penalties for breaches of their respective data protection regulations[2].

CRIMINAL LIABILITY

The PIPL, the CSL, the Law on the Protection of Minors and the Provisions on the Cyber Protection of Children's Personal Information do not provide for any standalone criminal sanction[3]. They simply refer to other administrative and criminal laws. Specifically, breaches which also constitute breaches of public security may be subject to sanctions under public security administration laws; and breaches which constitute criminal acts would be subject to criminal prosecution.

According to the Ninth Amendment to the Criminal Law, a person commits a criminal offence if he (a) obtains PI belonging to Chinese citizens by unlawful means, or (b) sell or provide PI belonging to Chinese citizens to third parties "*contrary to relevant statutory provisions*". In "*serious*" cases, offenders may be fined and imprisoned for a maximum of three years. In "*particularly serious*" cases, offenders may be sentenced to imprisonment for a maximum of seven years[4].

The Supreme People's Court and the Supreme People's Procuratorate jointly issued an interpretation[5] which elaborated, among other things, on the meaning of each of the quoted terms in the paragraph above:

- "Contrary to relevant statutory provisions" means "violating any law, administrative regulation, or departmental guideline in relation to the protection of citizens' personal information".
- "Serious" crimes include the sale or provision of location tracking data to others for the purpose of committing crimes.
- Crimes are considered "particularly serious" if significant amounts of PI are involved in the breach, or if the crimes result in serious consequences such as the death, serious injury, mental incapacitation or kidnapping of the affected data subjects.

The PCPD's Information Booklet identified two criminal judgments handed down by the People's Court of Haidian District, Beijing, in 2018 and 2019 which involved employees unlawfully obtaining PI belonging to Chinese citizens by accessing their respective company's internal systems without authorisation. The Court found both instances to be "particularly serious" crimes:

i. In the 2018 case, the offender accessed his company's system using a computer programme he wrote, obtained nearly 59,000 items of PI and transferred such PI to third parties[6]. The offender was sentenced to imprisonment for 21 months and also was fined RMB 5,000.

ii. In the 2019 case, the two offenders disclosed to third parties their login details for the company's system in order to allow the third parties to obtain more than 100,000 items of customer PI for use in their own businesses[7]. The offenders respectively were sentenced to imprisonment of 36 months and 38 months, and each was fined RMB 6,000.

CIVIL LIABILITY

In addition to statutory penalties and criminal liability, breaches of data protection laws also may lead to civil liability

(a) The PIPL, the CSL and the Law on the Protection of Minors

The PIPL specifies clearly the burden of proof with regard to such civil liability[8]: in cases where the mishandling of PI causes loss or damage, the data handler is liable to pay damages if it is unable to prove that it was not at fault. The amount of damages depends on the amount of loss suffered by the affected data subjects or the amount of gain obtained by the data handler as a result of the offending act.

The CSL and the Law on the Protection of Minors also contain express provisions which recognise civil liability arising from personal or property damage caused by breaches with regard to protection of PI[9].

(b) The Civil Code

The Civil Code recognises the right to privacy as one of the "personality rights" it protects[10] and states that PI belonging to natural persons is protected by law[11]. Persons affected by breaches of their "personality rights" may pursue civil remedies such as injunctive relief, impact elimination, restoration of goodwill and formal apology[12]. Injunctions also may be granted in cases where there is evidence showing that (i) an act of infringement of "personality rights" is being or shortly will be committed, and (ii) irreparable damage will be caused to a person's legal rights in the absence of timely injunctive relief[13].

The Civil Code further provides that any person who causes damage by wrongly infringing another person's civil rights needs to bear liability for infringement. Compensation payable would be determined either based on the loss suffered by the victim or the gain obtained by the wrongdoer as a result of the infringement. Parties may apply to the PRC Courts for determination on a case by case basis[14]. Victims are entitled to ask for compensation for pain, suffering and loss of amenity in cases where the infringement is proven to have caused serious mental impact[15].

Unless otherwise provided by law, the Civil Code states expressly that internet service providers and internet users have to bear liability if they infringe upon other people's civil rights using the internet[16]. Note that network operators are required to take necessary actions such as deletion or blockage of content in order to stop infringement actions when informed by victims, even though the act of infringement has not been committed by the network operators. Failure to take timely and necessary actions upon notice will make the network operator jointly liable for the infringement[17].

(c) The SPC's Decision

Specifically in relation to human facial information, the Decision of the Supreme People's Court regarding the applicable laws to civil cases involving the handling of personal information using face detection technology[18] (the "SPC's Decision") set out the following examples which constitute acts of infringement of a natural person's "personality rights" with regard to facial information:

i. Recognition, verification or analysis of human facial information in public places such as hotels, shopping malls and traffic stations in violation of the law;

ii. Failure to make available to the public the rules regarding the handling of human facial information or clearly specify the handling purpose, method and scope in such rules;

iii. Failure to obtain separate or written consent from the data subjects or their parental guardians;

iv. Failure to take necessary security measures which causes the leakage, alteration or loss of human facial information;

v. Provision of human facial information to third parties in breach of the law or agreement with the relevant data subjects[19].

(d) Case authority

The first public interest litigation case for the protection of PI under the Civil Code was closed in Hangzhou, Zhejiang in January 2021. The offender in this case purchased over 45,000 items of personal information (including names, contact numbers and email addresses) from the internet, and resold them for gain via chat platforms[20]. In light of the large number of individuals affected, the Procuratorate of Xiacheng District, Hangzhou initiated public interest litigation against the offender. The Court demanded compensation in the amount of RMB 34,000 (representing the amount of gain obtained by the offender) and a formal apology broadcast in public through a provincial-level news agency. These demands were endorsed and accepted by the Court.

In March 2021, another case for the protection of PI under the Civil Code was concluded by the People's Court of Gweiyang District, Hunan. This case was a public interest civil claim brought by the People's Court as an ancillary claim to a criminal prosecution. The offender took advantage of his position as an employee in a network communications company to obtain customers' PI, which he then resold on social media platforms. The offender was sentenced to six months' imprisonment and was fined RMB 20,000 (again, representing the amount of gain obtained by the offender) and was required to make a formal apology broadcast in public through a provincial-level news agency.

CONCLUDING REMARK

It is important for businesses to understand the potential civil, criminal and statutory liabilities which may result from data protection breaches. An understanding of what may be at stake will assist businesses in making decisions as to what levels of human and financial resources should be put in place and regarding what measures to adopt in light of China's data protection requirements.

---

[1] Available on the website of the PCPD at: https://www.pcpd.org.hk/tc_chi/resources_centre/publications/books/files/pcpd_china_pipl_book2021.pdf

[2] §§64-66 of the CSL; §127 of the Law on the Protection of Minors.

[3] See §71 of the PIPL, §74 of the CSL, §129 of the Law on the Protection of Minors and §26 of the Provisions on the Cyber Protection of Children's Personal Information.

[4] §253(1) of the Nineth Amendment to the Criminal Law.

[5] See “Interpretation on certain issues relating to laws applicable to the criminal cases involving mishandling of citizens’ personal information issued by the Supreme People’s Court and the Supreme People’s Procuratorate” dated 8 May 2017 (in Chinese language only), available at https://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170509_190088.shtml.

[6] Case no. :（2018）京0108刑初958號

[7] Case no. :（2018）京0108刑初1873號

[8] §69 of the PIPL.

[9] §74 of the CSL; §129 of the Law on the Protection of Minors.

[10] §990 of the Civil Code.

[11] §1034 of the Civil Code.

[12] §995 of the Civil Code.

[13] §994 of the Civil Code.

[14] §1182 of the Civil Code.

[15] §1183 of the Civil Code.

[16] §1194 of the Civil Code.

[17] §1195 of the Civil Code.

[18] Available (only in the Chinese language) on the website of the Supreme People’s Court of the PRC.

[19] §2 of the SPC’s Decision.

[20] Case reported in the website of the Supreme People’s Procuratorate of the PRC at https://www.spp.gov.cn/spp/sp/202101/t20210109_505879.shtml (available in the Chinese language only).

RELATED CAPABILITIES

- Corporate
- Data Privacy & Security

MEET THE TEAM

Glenn Haley

Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450
