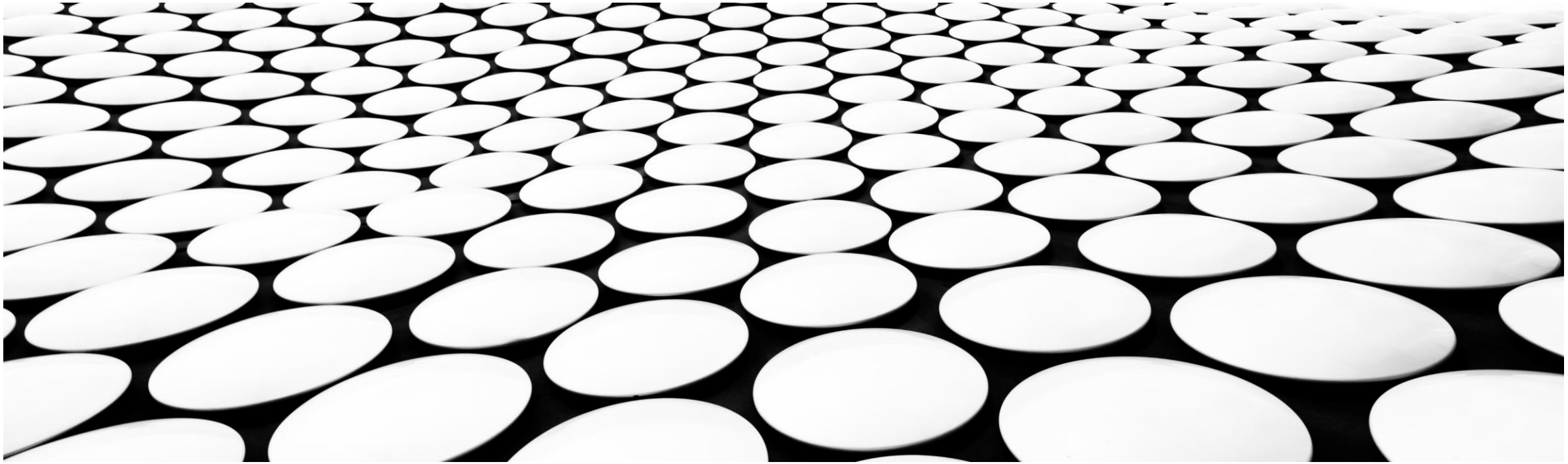
CYBERRISKS AS A CHALLENGE FOR CORPORATIONS AND THEIR EXECUTIVES (DUTIES, LIABILITY) IN THE P.R. CHINA

LOU JIANBO, PROFESSOR OF LAW, PEKING UNIVERSITY LAW SCHOOL, 23-03-2023



OUTLINES

- 1. The Evolution of cybersecurity law and regulation in China
- 2. The Quadruple Goals of Laws and Regulations Governing Internet Activities in China
- 3. A-bird’s eye view of obligations and liabilities of companies in NSL, PIPL, DSL and CSL
- 4. Litigation and Enforcement

1. THE EVOLUTION OF CYBERSECURITY LAW AND REGULATION IN CHINA

China became connected to the internet

Internet users and devices grew steadily in number. Legislation during this stage focused on network infrastructure security, specifically computer systems security and network security.

Dominated by mobile internet

Legislation has been gradually focusing on comprehensive cyberspace governance by covering areas such as network information services, information technology development, and cybersecurity.

PC as the main terminal for internet connection

As PCs and internet users grew rapidly in numbers, internet connection services became more affordable and web-based information services boomed. Legislation during this stage shifted to internet services and content management.

CONT.

- Over the years, China has promulgated more than **140** laws on cyberspace, forming a cyber legislation framework with the Constitution as the foundation, supported by laws, administrative regulations, departmental rules, local regulations and local administrative rules, endorsed by traditional legislation, and underpinned by specialized cyber laws governing online content and management, cybersecurity, information technology, and other elements.

SPECIFIC LEGISLATIONS GOVERNING INTERNET AND ITS RELATED ACTIVITIES

- **Law adopted by the NPC or Its Standing Committee**: Electronic Commerce Law(2018)/Electronic Signature Law(2004, as revised in 2019)/Cybersecurity Law(2016)/Data Security Law(2021)/Personal Information Protection Law(2021) /Law on Combating Telecom and Online Fraud(2022)
- **Administrative Regulation adopted by the State Council**: 1994 Regulations on the Security and Protection of Computer Information Systems (as revised in 2011)/2011 Regulations on Computer Software Protection (as revised in 2013)/2000 Administrative Measures on Internet Information Services (as revised in 2011)/2000 Telecommunications Regulations (as revised in 2016)/2001 Regulations on the Administration of Foreign Investment in Chinese Telecommunications Businesses(as revised in 2022)/ 2006 Regulations on the Protection of the Right of Communication Through Information Networks (as revised in 2013)/2021 Regulations on the Security and Protection of Critical Information Infrastructure
- **Departmental Rules adopted by Ministries subordinated to the State Council**: 2019 Provisions on the Protection of Children's Online Personal Information (Order No.4 of the Cyberspace Administration of China)/2017 China Internet Domain Name Regulations (Order No. 43 of the Ministry of Industry and Information Technology)/ 2021 Measures on the Supervision and Administration of Online Transactions (Order No. 37 of the State Administration for Market Regulation)/2017 Provisions on the Administration of Internet News and Information Services (Order No. 1 of the Cyberspace Administration of China)/ 2020 Regulations on the Governance of Online Information and Content (Order No.5 of the Cyberspace Administration of China) / 2022 Regulations on the Management of Algorithmic Recommendations for Internet Information Services (Order No. 9 of the Cyberspace Administration of China, the Ministry of Industry and Information Technology of the People's Republic of China, the Ministry of Public Security of the People's Republic of China, and the State Administration for Market Regulation)

CONT.

- **Local Regulations adopted by Provincial-level People's Congress**: 2021 Guangdong Provincial Digital Economy Promotion Act (Announcement No. 85 of the Standing Committee of the 13th Guangdong Provincial People's Congress)/2020 Zhejiang Provincial Digital Economy Promotion Act (Announcement No. 44 of the Standing Committee of the 13th Zhejiang Provincial People's Congress)/2012 Hebei Provincial Regulations on Information Technology Development (2021 revision)/2020 Guizhou Provincial Regulations on Government Data Sharing (Announcement No. 12 of the Standing Committee of the 13th Guizhou Provincial People's Congress)/2021 Shanghai Municipal Data Regulations (Announcement No. 94 of the Standing Committee of the Shanghai Municipal People's Congress)
- **Local Administrative Rules adopted by Provincial-Level People's Government**: 2021 Measures of Guangdong Province on Public Data Management (Decree No. 290 of Guangdong Provincial People's Government)/2020 Measures of Anhui Province on the Management of Data and Resources for Government Affairs (Decree No. 299 of Anhui Provincial People's Government)/2004 Measures of Jiangxi Province on the Protection of Computer Information System Security (2022 Revision)/2015 Interim Measures of Hangzhou City on the Administration of Online Transactions (Decree No. 282 of Hangzhou Municipal People's Government)

2. THE QUADRUPLE GOALS OF LAWS AND REGULATIONS GOVERNING INTERNET ACTIVITIES IN CHINA

- 2.1 Protecting People's Rights and Interests in Cyberspace
- 2.2 Improving Law-Based Governance of the Digital Economy
- 2.3 Safeguarding Cybersecurity by Law
- 2.4 Improving Regulation for a Sound Cyber Environment

2.1 PROTECTING PEOPLE'S RIGHTS AND INTERESTS IN CYBERSPACE

- **Protecting the freedom and confidentiality of correspondence**: Art. 7, the 1997 Measures on Ensuring Security of Internationally Connected Computer Information Networks/Art. 66,the 2000 Telecommunications Regulations/Art. 69, Regulations on Radio Administration(2016 revision)
- **Protecting personal information rights and interests**: Arts. 111, 999 and 1030, Chapter 6 (Book 4), art. 1226, the 2020 **Civil Code**/2009 Amendment VII and 2015 Amendment IX to the Criminal Law (added provisions on the crime of infringing upon citizens' personal information)/the 2012 NPCSC Decision on Strengthening Online Information Protection/Arts. 22, 37, 41-45, 64, the 2016 Cybersecurity Law/the 2021 **Personal Information Protection Law**
- **Safeguarding citizen's property**: Arts. 13, 38, 85 the 2018 Electronic Commerce Law/Arts. 127, 1194, 1197, the 2020 Civil Code/ The 2022 Law on Combating Telecom and Online Fraud
- **Protecting the digital rights of special groups (minors, elderly people, and persons with disabilities)**: Art. 13 (minors), the 2016 Cybersecurity Law/ The 2019 Regulations on the Protection of Children's Online Personal Information/Arts. 11, 32-34, 58, 64, the Law on the Protection of Minors (2020 revision)/Art. 15(providers of smart public services should take into full consideration the needs of elderly people and persons with disabilities, and make sure they do not create obstacles to their daily life), the 2021 Data Security Law

2.2 IMPROVING LAW-BASED GOVERNANCE OF THE DIGITAL ECONOMY

- **Creating institutions fundamental to data development**: The 2021 Data Security Law
- **Regulating the operation of the digital market**: Art. 85, the 2018 Electronic Commerce Law/Art. 25 (a seven-day unconditional return policy for online shopping), the Law on the Protection of Consumer Rights and Interests (2013 Revision) /Arts. 12 & 24 (ban unfair competition that takes advantage of internet technology), the Law Against Unfair Competition (2017 Revision) /The 2021 Measures on the Supervision and Administration of Online Transactions/The 2021 Anti-monopoly Commission under the State Council's Anti-monopoly Guidelines for Platform Economy/Art. 9 & 22, the Anti-monopoly Law (2022 revision)
- **Regulating new business forms and models of the digital economy**: Arts. 469, 482 & 512 (improved rules on the conclusion and execution of electronic contracts), art. 127(data and virtual assets protection), the 2020 Civil Code/The 2016 Interim Measures on the Administration of Online Taxi Booking Services (2019 revision)/The 2021 Regulations on the Administration of Algorithmic Recommendations for Internet Information Services/The 2019 Regulations on the Administration of Blockchain Information Services/The 2016 Interim Measures on the Administration of Business Activities of Intermediary Agencies for Online Lending/The 2020 Interim Regulations on the Administration of Online Tourist Services.

2.3 SAFEGUARDING CYBERSECURITY BY LAW

- **Setting rules for cybersecurity**: The 1994 Regulations on the Security and Protection of Computer Information Systems (as revised in 2011) /The 2000 NPCSC's Decision on Ensuring Internet Security/The 2016 Cybersecurity Law/The Measures on Cybersecurity Review (2021 Revision)/The 2021 Provisions on the Management of Security Loopholes of Online Products
- **Ensuring security for critical information infrastructure**: The 2021 Regulations on the Security and Protection of Critical Information Infrastructure, defines what constitutes critical information infrastructure and the principles and goals of protection (chapter 1); provides procedures for identifying critical information infrastructure (chapter 2), and the operators' responsibility for cybersecurity (chapter 3).
- **Developing the legal framework for data security management**: The 2021 Data Security Law has clear provisions on establishing mechanisms for categorized and classified data protection (art. 21), risk monitoring and early warning (art. 22), emergency response(art. 23), and data security review (art. 24); it also contains measures to facilitate data security (chapter 4) and development and provisions for the security and openness of government data(chapter 5).

2.4 IMPROVING REGULATION FOR A SOUND CYBER ENVIRONMENT

- **Regulating the orderly dissemination of online information**: Arts. 1028, 1194-1197, the 2020 Civil Code (torts)/Arts. 12, 48, the 2016 Cybersecurity Law/Art. 15, the 2000 Administrative Measures on Internet Information Services (2011 revision)
- **Sharpening the legal weapons against cyberterrorism**: The Criminal Law, Criminal Procedure Law, and Anti-Money Laundering Law/Arts. 17, 18, 19, 21, 61, 84 & 86, the 2015 Counterterrorism Law (2018 revision), specific provisions on the targets, measures and mechanisms for combating terrorism in cyberspace

3. A-BIRD'S EYE VIEW OF OBLIGATIONS AND LIABILITIES OF COMPANIES IN NSL, PIPL, DSL AND CSL

- 3.1 Obligations and Liabilities under National Security Law
- 3.2 Obligations and Liabilities under Personal Information Protection Law
- 3.3 Obligations and Liabilities under Data Security Law
- 3.4 Obligations and Liabilities under Cybersecurity Law

3.1 OBLIGATIONS AND LIABILITIES UNDER NATIONAL SECURITY LAW

- **General Obligation to Protect National Security**-Para. 1, art. 11, All citizens of the People's Republic of China, state authorities, armed forces, political parties, people's groups, **enterprises**, public institutions, and other social organizations shall have the responsibility and obligation to maintain national security/ A list of obligations, art. 77
- **To provide education on maintaining national security to their personnel, and mobilize and organize their personnel to prevent and frustrate conduct that compromises national security-** art. 78
- **To assist the relevant departments in taking the relevant security measures-**art. 79
- **Internal Control, Compliance & Compliance Audit-**Arts. 51, 52, 53 & 4
- **In-advance personal information protection impact assessment -** Arts. 55 & 56
- **Extra Requirements on Personal Information Processors that Provide Important Internet Platform services-** Art. 58
- **Special Provisions on Joint Processing of Personal Information-** Art. 20 Where personal information processors jointly processing personal information infringe upon the rights and interests relating to personal information and cause damage, they shall bear joint and several liability in accordance with the law.
- **Special Provisions on Commissioned Processing of Personal Information –** Arts. 21 & 59
- **Special Rules on Cross-Border Provision of Personal Information –** Arts. 38, 39 & 40
- **Remedial Measures and Possible Liabilities for Leakage, tampering or loss of personal information –** Art. 57

CONT.

- **Administrative Punishment**
  - Art. 66 Where a personal information processor processes personal information in violation of this Law or fails to fulfill the personal information protection obligations as provided in this Law in processing personal information, the authority performing personal information protection functions shall order the personal information processor to take corrective action, give it or him a warning, and confiscate its or his illegal income; and with respect to an application program processing personal information in violation of law, shall order the suspension or termination of provision of services by such application program. If the personal information processor refuses to take corrective action, it or he shall be fined not more than one million yuan; and any directly liable person in charge or other directly liable person shall be fined not less than 10,000 yuan nor more than 100,000 yuan. /Where a personal information processor commits any illegal act as specified in the preceding paragraph with serious circumstances, the authority performing personal information protection functions at or above the provincial level shall order it or him to take corrective action, confiscate its or his illegal income, and impose a fine of not more than 50 million yuan or not more than 5% of it or his turnover in the previous year, and may order the suspension of relevant business or suspension of business for an overhaul, and notify the relevant competent department to revoke the relevant business permit or business license; and impose a fine of not less than 100,000 yuan nor more than one million yuan on any directly liable person in charge or other directly liable person, and may decide to prohibit them from serving as directors, supervisors, senior executives or persons in charge of personal information protection of related enterprises during a certain period of time.
  - Art. 67 Where any violation of laws as prescribed in this Law is committed, it shall be entered into the relevant credit record and be published in accordance with the provisions of the applicable laws and administrative regulations.

CONT.

- **Civil Liabilities**
  - Art. 69 Where the personal information processing infringes upon rights and interests relating to personal information and causes damage, and the personal information processor cannot prove that it or he is not at fault, the personal information processor shall assume liability for damage and other tort liability. /The “liability for damage” referred to in the preceding paragraph shall be determined based on the losses incurred by individuals thereby or the benefits obtained by the personal information processor therefrom; and where it is difficult to determine the losses incurred by individuals thereby or the benefits obtained by the personal information processor therefrom, the amount of damages shall be determined in accordance with the actual circumstances.
  - Art. 70 Where a personal information processor processes personal information in violation of the provisions of this Law, infringing the rights and interests of many individuals, the people's procuratorate, the consumer organization as provided by law, or the organization determined by the national cyberspace administration may file a lawsuit with the people's court in accordance with the law.

CONT.

- **Criminal Liabilities** Art. 71 Where any violation of this Law constitutes a violation of public security administration, the public security administration punishment shall be imposed in accordance with the law; and if the violation constitutes a crime, the violator shall be held criminally liable in accordance with the law.
  - Article 253 (I), Criminal Law: Whoever sells or provides any citizen's personal information in violation of the relevant provisions of the state shall, if the circumstances are serious, be sentenced to imprisonment of not more than three years or limited incarceration in addition to a fine or be sentenced to a fine only; or be sentenced to imprisonment of not less than three years but not more than seven years in addition to a fine if the circumstances are especially serious./Whoever sells or provides to any other person any citizen's personal information obtained in the course of performing functions or providing services in violation of any relevant provisions of the state shall be given a heavier penalty in accordance with the provisions of the preceding paragraph. /Whoever illegally obtains any citizen's personal information by stealing or other methods shall be punished in accordance with the provisions of paragraph /Where an entity commits any crime as provided for in the preceding three paragraphs, the entity shall be sentenced to a fine, and its directly responsible person in charge and other directly liable persons shall be punished according to the provisions of the applicable paragraph.

3.3 OBLIGATIONS AND LIABILITIES UNDER DATA SECURITY LAW

- **General Requirements (law and ethics compliance)** - Arts. 8, 28 & 32
- **Obligations on data security management system, data security education and training, etc.** – Art. 27
- **Extra Requirements on important data processors (regular risk assessment, risk assessment reports)** – Art. 30
- **Security management of cross-border transfer of important data -** Art. 31
- **Obligations of data trading intermediary service providers** - Art. 33
- **Licenses for the provision of data processing-related services**- Art. 34
- **Remedial Measures and Notification Duties on Data Security Accident –** Art. 29

CONT.

- **Administrative Liabilities**
  - Art. 45 Where an organization or individual conducting data processing activities fails to perform any of the data security protection obligations under Articles 27, 29 and 30 of this Law, the appropriate department shall order corrective action to be taken by and issue a warning to the violator, and may impose a fine of not less than 50,000 yuan nor more than 500,000 yuan on the violator and a fine of not less than 10,000 yuan nor more than 100,000 yuan on any directly liable executive in charge or other directly liable person; and if the violator refuses to take corrective action or there is any serious consequence such as divulgence of a large amount of data, shall impose a fine of not less than 500,000 yuan nor more than 2 million yuan on the violator, and may order suspension of the related business, suspension of business for overhaul, revocation of the related business permit, or revocation of business license, and impose a fine of not less than 50,000 yuan nor more than 200,000 yuan on any directly liable executive in charge or other directly liable person./Where the national core data management system is violated, compromising national sovereignty, security, and development interests, the appropriate department shall impose a fine of not less than 2 million yuan nor more than 10 million yuan on the violator, and order suspension of the related business, suspension of business for overhaul, revocation of the related business permit, or revocation of business license according to the circumstances; and if the violation is criminally punishable, the offender shall be held criminally liable in accordance with the law.
  - Art. 46 Where any important data is provided to any overseas recipient in violation of Article 31 of this Law, the appropriate department shall order corrective action to be taken by and issue a warning to the violator, and may impose a fine of not less than 100,000 yuan nor more than 1 million yuan on the violator and a fine of not less than 10,000 yuan nor more than 100,000 yuan on any directly liable executive in charge or other directly liable person; or if the circumstances are serious, shall impose a fine of not less than 1 million yuan nor more than 10 million yuan on the violator, and may order suspension of the related business, suspension of business for overhaul, revocation of the related business permit, or revocation of business license, and impose a fine of not less than 100,000 yuan nor more than 1 million yuan on any directly liable executive in charge or other directly liable person.

CONT.

- Art. 47 Where an institution engaged in data trading intermediary services fails to perform the obligation under Article 33 of this Law, the appropriate department shall order the violator to take corrective action, and impose a fine of not less than one times nor more than ten times the illegal income therefrom, which shall be confiscated, or a fine of not less than 100,000 yuan nor more than 1 million yuan if there is no illegal income or the illegal income is less than 100,000 yuan, and may order suspension of the related business, suspension of business for overhaul, revocation of the related business permit, or revocation of business license; and impose a fine of not less than 10,000 yuan nor more than 100,000 yuan on any directly liable executive in charge or other directly liable person.
- Art. 48 Where provision of cooperation in the pulling of data is refused in violation of Article 35 of this Law, the appropriate department shall order corrective action to be taken by, issue a warning to, and impose a fine of not less than 50,000 yuan nor more than 500,000 yuan on the violator, and impose a fine of not less than 10,000 yuan nor more than 100,000 yuan on any directly liable executive in charge or other directly liable person. /Where a foreign judicial or law enforcement authority is provided with data without the approval of the competent authority in violation of Article 36 of this Law, the appropriate department shall issue a warning to the violator, and may impose a fine of not less than 100,000 yuan nor more than 1 million yuan on the violator and a fine of not less than 10,000 yuan nor more than 100,000 yuan on any directly liable person in charge or other directly liable person; or if there is any serious consequence, shall impose a fine of not less than 1 million yuan nor more than 5 million yuan on the violator, and may order suspension of the related business, suspension of business for overhaul, revocation of the related business permit, or revocation of business license, and impose a fine of not less than 50,000 yuan nor more than 500,000 yuan on any directly liable person in charge or other directly liable person.

CONT.

- **Civil Liabilities** Para. 1, Art. 52 Where any violation of this Law causes any damage to another person, the violator shall assume civil liability in accordance with the law.

CONT.

- **Criminal Liabilities**
  - Para. 2, art. 52 Where a violation of this Law constitutes a violation of public security administration, public security administration punishment shall be imposed on the violator in accordance with the law; or where the violation is criminally punishable, the offender shall be held criminally liable in accordance with the law.
  - Para. 2, art. 285, Criminal Law, Whoever, in violation of the state provisions, intrudes into a computer information system other than that prescribed in the preceding paragraph or uses other technical means to obtain the data stored, processed or transmitted in the said computer information system or exercise illegal control over the said computer information system shall, if the circumstances are serious, be sentenced to fixed-term imprisonment not more than three years or limited incarceration, and/or be fined; or if the circumstances are extremely serious, shall be sentenced to fixed-term imprisonment not less than three years but not more than seven years, and be fined.
  - Para. 2, art. 286, Whoever violates state regulations and deletes, alters, or adds the data or application programs installed in or processed and transmitted by the computer systems, and causes grave consequences, is to be punished according to the preceding paragraph (to be sentenced to not more than five years of fixed-term imprisonment or limited incarceration; when the consequences are particularly serious, the sentence is to be not less than five years of fixed-term imprisonment).

3.4 OBLIGATIONS AND LIABILITIES UNDER CYBERSECURITY LAW

- **General Requirements on Network Operators (law and ethics compliance)** -Art. 9
- **General Requirements for the Construction and Operation of the Network or the Provision of Services through the Network (law and national standards)** - Art. 10
- **General Requirements for Individual or Organization Using the Network (laws, public order and social morality)**- Para. 2, art. 12.

- **Graded Protection of Cybersecurity** - Art. 21 …… Network operators shall, according to the requirements of the rules for graded protection of cybersecurity, fulfill the following security protection obligations, so as to ensure that the network is free from interference, damage or unauthorized access, and prevent network data from being divulged, stolen or falsified. (1) Developing internal security management rules and operating procedures, determining the persons in charge of cybersecurity, and carrying out the responsibility for cybersecurity protection. (2) Taking technical measures to prevent computer viruses, network attack, network intrusion and other acts endangering cybersecurity. (3) Taking technical measures to monitor and record the status of network operation and cybersecurity incidents, and preserving relevant weblogs for not less than six months as required. (4) Taking measures such as data categorization, and back-up and encryption of important data. (5) Performing other obligations as prescribed by laws and administrative regulations.
- **Extra Requirements on Critical Information Infrastructure Operators** - Arts. 34 & 38
- **Cybersecurity Incidents** - Arts. 25, 55-57.

CONT.

- **Administrative Liabilities**
  - Art. 59 Where any network operator fails to perform the cybersecurity protection obligations as prescribed by Articles 21 and 25 of this Law, the competent department shall order it to take corrective action and give it a warning. If the operator refuses to take corrective action, or such consequences as endangering cybersecurity are caused, it shall be fined not less than 10,000 yuan but not more than 100,000 yuan, and its directly responsible person in charge shall be fined not less than 5,000 yuan but not more than 50,000 yuan.

    Where any critical information infrastructure operator fails to perform the cybersecurity protection obligations as prescribed by Articles 33, 34, 36 and 38 of this Law, the competent department shall order it to take corrective action and give it a warning. If the operator refuses to take corrective action, or such consequences as endangering cybersecurity are caused, it shall be fined not less than 100,000 yuan but not more than one million yuan, and its directly responsible person in charge shall be fined not less than 10,000 yuan but not more than 100,000 yuan.
  - Arts. 60-73

CONT.

- **Civil Liabilities** Para.1, art. 74 Whoever violates the provisions of this Law and causes any damage to any other person shall assume civil liability in accordance with the law.

CONT.

- **Criminal Liabilities**
  - Para. 2, art. 72 Whoever violates the provisions of this Law shall, if the act constitutes a violation of public security administration, be subject to public security administration punishment in accordance with the law, and if the act constitutes a crime, be subject to criminal liability in accordance with the law.
  - Art. 286 (I), Criminal Law: Any network service provider that fails to perform the information network security management obligation as prescribed in any law or administrative regulation and refuses to make corrections after being ordered by the regulatory authority to take correction measures shall be sentenced to imprisonment of not more than three years, limited incarceration or surveillance in addition to a fine or be sentenced to a fine only under any of the following circumstances: (1) Causing the spread of a large amount of illegal information. (2) Causing the leakage of users' information, with serious consequences. (3) Causing the loss of criminal case evidence, with serious circumstances. (4) Any other serious circumstance. /Where an entity commits the crime as provided for in the preceding paragraph, a fine shall be imposed on it, and its directly responsible person in charge and other directly liable persons shall be punished in accordance with the provisions of the preceding paragraph. /Whoever commits any other crime while committing a crime as mentioned in the preceding two paragraphs shall be convicted and punished according to the provisions on the crime with the heavier penalty.

4. LITIGATIONS AND ENFORCEMENT

- 4.1 Shareholder Derivative Suits
- 4.2 Securities Fraud Class Actions
- 4.3 Class Action Lawsuits by the Company’s Outside Customers or Business Partners whose Information Was Compromised
- 4.4 Administrative Agencies’ Enforcement Actions under Applicable State or Federal Laws

--Michael Hooker & Jason Pill, You've Been Hacked, and Now You're Being Sued:

The Developing World of Cybersecurity Litigation, 90 FLA. B.J. 30, 31 (2016)

4.1 SHAREHOLDER DERIVATIVE SUITS

- No obstacle legally – Arts. 147-149, 151-152, PRC Company Law
- The "Waving of Red Flag" by the Government - art. 64, PIPL/art. 44, DSL/art. 56, CSL
- Rarely happened in reality
- Business judgement rule: The seeming zero-sum relationship between security-and thus usability-and profitability. A possible Obstacle.

CONT.

- Art. 64, PIPL, Where an authority performing personal information protection functions finds during the performance of its functions that there are relatively large risks in personal information processing activities or any personal information security incident occurs, it may hold an interview with the legal representative or primary person in charge of the personal information processor in accordance with the specified authority and procedures, or require the personal information processor to commission a professional institution to audit the regulatory compliance of its or his personal information processing activities. The personal information processor shall adopt measures to make rectification and eliminate hidden risks as required. /Where an authority performing personal information protection functions finds during the performance of its functions that any illegal processing of personal information is suspected of constituting a crime, it shall promptly transfer the case to the public security organ for handling in accordance with the law.
- Art. 44, DSL, Where, in performing its duty to supervise data security, an appropriate department discovers that any data processing activities present a relatively large security risk, it may interview the relevant organization and individuals in accordance with the prescribed authority and procedures, and require the relevant organization and individuals to take measures to address issues and eliminate potential risks.
- Art. 56, CSL， Where the relevant department of the people's government at or above the provincial level finds any relatively high security risk or security incident on the network in the performance of cybersecurity supervision and administration functions, it may hold an interview with the legal representative or primary person in charge of the network operator according to prescribed powers and procedures. The network operator shall take measures to make rectification and eliminate hidden risks as required.

4.2 SECURITIES FRAUD CLASS ACTIONS

- Litigation, possible--Several Provisions of the Supreme People's Court on the Trial of Civil Cases for Damages for the Tort of Misrepresentation in the Securities Market (No. 2 [2022] of the Supreme People's Court)
- Class Action ?

CONT. SECURITIES LAW

- Art. 94 Where any dispute arises between an investor and an issuer or a securities company, among others, both parties may apply to an investor protection institution for mediation. A securities company shall not refuse an ordinary investor's request for mediation of a dispute between them over any securities business. /An investor protection institution may, in accordance with the law, support an investor in instituting an action in a people's court against acts damaging investors' interests. /Where an issuer's director, supervisor, or officer violates the provisions of any law or administrative regulation or the company's bylaws in performing corporate duties, causing any loss to the company, or where the issuer's controlling shareholder or actual controller, among others, infringes upon the company's lawful rights and interests, causing any loss to the company, an investor protection institution may, if holding shares of the company, institute an action in a people's court in its own name in the interest of the company, not subject to the provisions of the Company Law of the People's Republic of China regarding the shareholding ratio and holding period.
- Art. 95 Where investors institute civil actions for damages caused by misrepresentation, among others, related to securities, they may legally recommend and select representatives to participate in the actions if the subject matters of the actions are of the same kind and the parties on one side of the actions are numerous. /For actions instituted according to the provision of the preceding paragraph, if there may be many other investors who have the same claims, the people's court may issue an announcement to state the facts of the case involving the claims and notify investors that they may register with the people's court during a certain period. The judgment or ruling rendered by the people's court shall be valid for the registered investors. /An investor protection institution may, as authorized by 50 or more investors, participate in actions as a representative, and according to the provision of the preceding paragraph, register right holders confirmed by the securities depository and clearing institution with the people's court, except for investors who have expressly indicated their reluctance to participate in the actions.

4.3 CLASS ACTION LAWSUITS BY THE COMPANY'S OUTSIDE CUSTOMERS OR BUSINESS PARTNERS WHOSE INFORMATION WAS COMPROMISED

- **Litigation, possible—Art. 127, Civil Code, Where any laws provide for the protection of data and network virtual property, such laws shall apply.**
  - Art. 69, PIPL, Where the personal information processing infringes upon rights and interests relating to personal information and causes damage, and the personal information processor cannot prove that it or he is not at fault, the personal information processor shall assume liability for damage and other tort liability. /The "liability for damage" referred to in the preceding paragraph shall be determined based on the losses incurred by individuals thereby or the benefits obtained by the personal information processor therefrom; and where it is difficult to determine the losses incurred by individuals thereby or the benefits obtained by the personal information processor therefrom, the amount of damages shall be determined in accordance with the actual circumstances.
  - Para. 1, Art. 52, DSL, Where any violation of this Law causes any damage to another person, the violator shall assume civil liability in accordance with the law.
  - Para.1, art. 74, CSL, Whoever violates the provisions of this Law and causes any damage to any other person shall assume civil liability in accordance with the law.

CONT.

- **Class action ?—**
  - Art. 70, PIPL, Where a personal information processor processes personal information in violation of the provisions of this Law, infringing the rights and interests of many individuals, the people's procuratorate, the consumer organization as provided by law, or the organization determined by the national cyberspace administration may file a lawsuit with the people's court in accordance with the law.

4.4 ADMINISTRATIVE ENFORCEMENT

- Absolutely the Mainstream
- To Facilitate the Private-party enforcement, or to weaken the private-party enforcement

CONT.: THE 2022 RMB 8.03 BILLION (US$1.2 BILLION) FINE INCURRED BY POPULAR RIDE-HAILING COMPANY DIDI CHUXING

- The Cyberspace Administration of China said a one-year cybersecurity review has found clear evidence that Didi violated the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law and imposed more than 8 billion yuan ($1.19 billion) on Didi. On top of the fine slapped on the company, Didi CEO Cheng Wei and president Liu Qing were fined 1 million yuan each.
- The Cyberspace Administration of China launched the cybersecurity review of Didi after the company made its debut on the New York Stock Exchange in June 2021. One year later, Didi was delisted from the exchange.
- The Beijing-based company illegally collected over 64.7 billion pieces of user information over a seven-year period starting from June 2015. The amount of the illegally collected information is staggering, as it includes facial recognition data, precise location information and identity card numbers, the regulator said.
- The investigation also found that Didi has engaged in data processing activities that seriously affected national security and brought security risks to the nation's key information infrastructure. The company had refused to comply with regulatory requirements and had evaded supervision, the regulator added.

CONT.

- The CAC stated that Didi had made 16 violations covering eight different types of activity: (1) Illegally collecting almost 12 million screenshots from users' mobile phone photo albums. (2) Collecting 8.3 billion pieces of information from users' clipboards and application lists in excess of the scope necessary to carry out operations. (3) Collecting 107 million pieces of facial recognition data, 53.5 million pieces of information on age groups, 16.3 million pieces on occupations, 1.4 million pieces of information on family relationships, and 153 million "home" and "company" addresses from passengers, in excess of the scope necessary to carry out operations. (4) Collecting 167 million pieces of information on the precise location (longitude and latitude) when passengers evaluated the driver services, both when the app was running in the background and when the mobile phone was connected to the Orange Video Recorder app (an app developed by Didi that enables dashcam recordings) in excess of the scope necessary to carry out operations. (5) Collecting 142,900 pieces of information on drivers' education and storing 57.8 million drivers' ID numbers in plain text in excess of the scope necessary to carry out operations. (6) Analyzing almost 54 billion pieces of information on passengers' travel intent information, 1.5 billion pieces of information on passengers' city of residence, and 304 million pieces of information of passengers' non-local business and travel information without clearly telling passengers. (7) Frequently requesting irrelevant phone permissions of passengers when using the ride-hailing service. (8) Failing to accurately and clearly explain the purpose for processing 19 types of personal information, including user device information.
- In addition to the above, the CAC said it had previously found that Didi had engaged in data processing activity that "seriously affect national security", and had also violated other laws and regulations, including refusing to cooperate on certain requirements of the regulatory authorities and intentionally evading supervision. It also stated that Didi's illegal operations had posed serious security risks to China's critical information infrastructure and data security; however, details of these violations could not be divulged as they concerned matters of national security.
- The above violations were found to have taken place over the course of seven years, starting from at least June 2015 and lasting until the present day. The duration of the illegal activity meant that Didi was in breach of the regulations laid out in the CSL, which came into effect in June 2017, the DSL (September 2021), and the PIPL (November 2021).

CONT.

- **Excessive collection of data and personal information [**violation (2) (3) (4) (5) **].**
  - Art. 6, PIPL: The processing of personal information shall have a clear and reasonable purpose, which shall be directly related to the purpose of processing, and shall be adopted in a way that has the least impact on personal rights and interests. /The collection of personal information shall be limited to the minimum scope to achieve the purpose of processing, and excessive collection of personal information shall not be allowed.
  - Para.2, art. 41, CSL: Network operators shall not collect personal information irrelevant to the services they provide, and shall not collect or use personal information in violation of laws, administrative regulations, and agreements between both parties, and shall process the personal information stored by it in accordance with the provisions of laws and administrative regulations and the agreement with the user.
  - Para.2, art. 32, DSL: Where laws and administrative regulations stipulate the purpose and scope of data collection and use, data shall be collected and used within the purpose and scope stipulated by laws and administrative regulations.

CONT.

- **Analyzing information without clearly telling users/Failing to accurately and clearly explain the purpose for processing personal information/Frequently requesting irrelevant phone permissions [**violation (6) (8) (7) **]**
  - Art. 17, PIPL: Prior to processing personal information, a personal information processor shall truthfully, accurately, and completely inform the individual of the following matters in an eye-catching manner and with clear and understandable language: (I) the name and contact information of the personal information processor; (II) the purpose and method of processing personal information, and the type and retention period of the processed personal information; (III) the method and procedure for the individual to exercise the rights provided herein; and (IV) other matters to be notified in accordance with the provisions of laws and administrative regulations.
  - Para. 1, art. 41, CSL: When collecting and using personal information, network operators shall [...] disclose the rules for collection and use, express the purpose, method, and scope of the collection and use of information, and obtain the consent of the data subject.

CONT.

- **Illegally obtaining and failing to adequately protect sensitive information** [violation (1)]
  - Art. 29, PIPL, Individual consent should be obtained for processing sensitive personal information. Where laws and administrative regulations provide that the processing of sensitive personal information shall be subject to written consent, such provisions shall prevail.
  - Art. 30, PIPL: For the processing of sensitive personal information of an individual, the personal information processor shall inform the individual of the necessity of processing sensitive personal information and the impacts on the individual's rights and interests [...]

谢谢！

Danke!

ありがとう

감사합니다.

Thank you!

loujianbo@pku.edu.cn