Péter Molnár: Comparison of the new Chinese Personal Data Protection Law (PIPL) with GDPR and CCPA

Foreword

Just a few years after its adoption, it is already clear that the Union's data protection regulation has encouraged the world's most dominant states to create their own legislation on the protection of personal data. The Californian Consumer Privacy Act can be considered the first major non-European data protection legislation. On August 20, 2021, the People's Republic of China also finalized its own data protection law. In our study, we attempt to compare the main features of the three defining pieces of legislation. As there is not yet any experience with the practical application of Chinese law, we will strictly confine ourselves to analyzing the normative text.

Regulatory history

The emergence of the first generation of data protection regulations dates back to the 1970s and is essentially a legal response to the threats posed by technological advances.[1] The first major international documents appeared in the 1980s, thanks to the growing volume of cross-border data flows. Although the OECD's Council's Guidelines on Governing the Protection of Privacy and Cross-Border Flows of Personal Data[2], adopted in 1980, are not binding, they contain a number of important basic principles. The guidelines extended to all OECD member countries, including the countries of the European Community and the United States itself. This is mainly due to the fact that subsequent European and American regulations show so many similarities. Building an information society in Europe has become an important priority since the 1990s, as indicated, for example, by the Bangemann report[3] and subsequent strategy papers. Even in these times, the duality of European regulation can be seen. On the one hand, it must ensure the free flow of data, and on the other, the private sector must be protected.[4] The process culminated in the EU Data Protection Directive adopted in 1995, under which Member States successively promulgated their own national data protection laws.

At the end of 2010s, two important personal data protection laws became applicable. The new laws attempting to regulate the area of privacy and personal data potection have been adopted on both sides of the Atlantic Ocean and although they differ in many respects, their

fundamentals are similar.[5] The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (hereinafter, GDPR) became applicable from 25 May 2018. The regulation is an evolution of an already existing EU directive[6], and was developed over a relatively long period of years. The legislation conatins 99 articles and 173 recitals. The California Consumer Privacy Act (hereinafter, CCPA), also known as AB 375, passed into California law on 28 June 2018 and became apllicable from 1 January, 2020. Compared to the GDPR, CCPA was hastily adopted and is much shorter than its European cousin.[7]

Before the adoption of the Personal Information Protection Law (hereinafter, PIPL), which had been approved by the 13th Standing Committee of the National People's Congress committee on 21 August 2021 the People's Republic Of China's (PRC) data protection law mostly viewed as being fragmentary, ineffective and difficult to understand.[8] Compared to the GDPR, the PIPL is relatively short with its 8 chapters and 73 articles, however, the effects of the European regulation can be felt in several respects.

In the next part of our paper, we attempt to compare the key features of GDPR, CCPA, and PIPL.

The territorial scope of the legislations

The GDPR and the CCPA both have an extraterritorial scope. The European regulation's territorial scope is defined in its Article 3:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a pro-cessor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.3.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international

law.

The territorial scope of the CCPA extends to any for-profit entity doing business in California, that meets at least one of the following three conditions: (1) has a gross revenue greater than $25 million, (2) annually buys, receives, sells, or shares the personal information of more than 50,000 consumers, households, or devices for commercial purposes. or (3) derives 50 percent or more of its annual revenues from selling consumers' personal information. The question is which entities can be considered doing business in California. These entities are not defined in the CCPA, but the reference to California tax and company law indicates that a broad interpretation of the term should be assumed, [9] so that the CCPA should also apply to all foreign-based entities that meet the above conditions and pays taxes in California because of its activities.

The PIPL is also applicable to activities outside the mainland PRC that handle the personal information of natural persons within the territory of the PRC, in any of the following circumstances: (1) for the purpose of providing products or services to natural persons within the territory; (2) to analyze and assess the conduct of natural persons within the territory; (3) other situations provided for by law or administrative regulations.[10]

Based on the above provision, we can state that (similar to GDPR and CCPA) PIPL also has extraterritorial effect, but the effect is narrower than the GDPR's.

Personal scope

With regard to personal scope, we can ask two main questions: who is protected and to who is regulated by the law imposes. The GDPR regulates every data controllers and data processors (natural persons, businesses, government agencies, etc.) and protects the natural persons (identified or identifiable persons to which personal data relates). The CCPA's operates with the term of business-doing entities, while it protects the „consumers" (basically California residents). The PIPL basically protects the personal informations on natural persons, and regulates any handler of these informations (both organizations and individuals).

What kind of information is protected?

The GDPR uses the term of personal data. Personal data is any information relating to an

identified or identifiable data subject. According to the CCPA personal *information* is every information that identifies, relates to, describes, is capable of being associated with, or may reasonably be linked, directly or indirectly, with a particular consumer or household. Both regulations defines specific categoires of personal data or information. According to the PIPL personal information is any type of information that identifies or can identify natural persons recorded electronically or by other means, but does not include anonymized information. The PIPL's definition is closer the the GDPR.

The legal basises of processing

The GDPR mentions six equal legal basises as the requiments of rigtful data processing (consent of the data subject, contract, legal obligation, protection of vital interests, public interest and legitimate interest), while the CCPA doesn't mention any. The latter regulation only provides for a posteriori mechanism, namely allowing customers to opt-out to the sale and disclosure of their personal information or to ask for erasure of the information.[11] The PIPL's following the method of the GDPR as it's mentions different legal basises. According to Article 13, personal information handlers can only handle personal information where one of the following circumstances is met: (1) the individual's consent is obtained; (2) as necessary to conclude or perform on a contract to which the individual is a party, or as necessary for carrying out human resource management in accordance with lawfully formulated labor rules systems and lawfully concluded collective contracts; (3) as necessary for the performance of legally-prescribed duties or obligations; (4) as necessary to respond to public health incidents or to protect natural persons' security in their lives, health, and property in an emergency; (5) handling personal information within a reasonable range in order to carry out acts such as news reporting and public opinion oversight in the public interest; (6) for a reasonable scope of handling of personal information that has been disclosed by the individual or otherwise already legally disclosed in accordance with this Law; (7) other situations provided by laws or administrative regulations.

Privacy notices

The GDPR devotes two complete articles to detail the content of the information to be provided to the data subject. The privacy notice must contian various informations: the identity and the contact details of the controller, the contact of the data protection officer, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, the recipients or categories of recipients of the personal data, etc.

According to CCPA businesses must inform consumers about the personal information categories collected, the intended use purposes for each category. Further notice is required to collect additional personal information categories. or use collected personal information.

Article 17 of the PIPL provides that before handling personal information, personal information handlers shall truthfully, accurately, and completely notify individuals of the following matters in a conspicuous fashion and in clear and understandable language: (1) the organizational or personal name of the personal information handlers; (2) the purposes of handling the personal information, the methods of handling, and the type of personal information handled, and period it will be stored; (3) the manner and procedures by which individuals are to exercise their rights under this Law; (4) other matters that laws and administrative regulations provide shall be announced.

The rights of the data subjects

The GDPR provides the following rights for the data subject: the right to acces, the right to data portability, the right to request erasure, the right to be forgotten, the right to reflectation, the right to restrict processing, the right to object to processing, and the right to object to automated decision-making.

In the CCPA we can’t find any rights that would be equivalent to the right of rectification and the right to object to processing.

The PIPL provides the data subjects the right to know and make decisions about the handling of their personal information, the right to limit or refuse the handling of their personal information by others, the right to access and reproduce their personal information from personal information handlers, the right to request correction, the right to request deletion, and the right to request that personal information processors explain their personal information processing rules.

The penalties

In 2018, the GDPR came as a surprise with its high fines. According to the regulation, the fines could reach 20 million euros, or four percent of the annual global revenue (whichever is the higher).

The CCPA defined the fines in 2 500 USD per violation or up to 7 500 USD per violation if it’s

international.

The PIPL also uses more categories of fines. According to Article 66: Where personal information is handled in violation of this Law, or where the obligations for the protection of personal information provided for in this Law are not performed in handling personal information, the departments performing duties on personal information protection are to order corrections, give warnings, and confiscate unlawful gains; applications that illegally handle personal information are to be ordered to have their provision of services suspended or stopped, and a fine of up to 1,000,000 RMB is to be given; the directly responsible managers and other directly responsible personnel are to be given a fine of between 10,000 and 100,000 RMB (cca. 1 300-13 000 euros). Where the circumstances of the illegal activities provided for in the preceding paragraph are serious, the provincial level or higher departments performing personal information protection duties are to order corrections, confiscate unlawful gains, and give a concurrent fine of up to 50,000,000 RMB (cca. 6,5 million euros) or up to 5% of the preceding year's business income, and may order that operation be suspended, suspend operations for rectification, or report to relevant regulatory departments for the cancellation of business permits or licenses; and a fine of between 100,000 and 1,000,000 RMB is to be given to the directly responsible managers and other directly responsible personnel, and a decision may be made to prohibit their serving as the board member, supervisor, senior management, or person in charge of personal information protection for an enterprise during a set period of time.

It can therefore be concluded that the PIPL allows for the imposition of fines higher than the CCPA, but still falls short of the fines indicated in the GDPR.

An overview

In this chapter we present a comparison chart for better for better clarity and applicability. The comparison is, of course, not exhaustive, it can be further developed. Nevertheless, it can serve as a good starting point for further research.

Criteria	Legislation		
	GDPR	CCPA	PIPL

Territorial scope	Data controllers and data processors: a) Established in the EU that process personal data in the context of activities of the EU establishment, regardless of whether the data processing takes place within the EU. b) Not established in the EU that process EU data subjects' personal data in connection with offering goods or services in the EU, or monitoring their behavior (…)	Any for-profit entity doing business in California and the entity meets at least one of the following: a) Has a gross revenue greater than $25 million. b) Annually buys, receives, sells, or shares the personal information of more than 50,000 consumers, households, or devices for commercial purposes. c) Derives 50 percent or more of its annual revenues from selling consumers' personal information	The PIPL is applicable to activities outside the mainland PRC that handle the personal information of natural persons within the territory of the PRC, in any of the following circumstances: a) for the purpose of providing products or services to natural persons within the territory; b) to analyze and assess the conduct of natural persons within the territory; c) other situations provided for by law or administrative regulations
Personal scope	Protected: natural persons (identified or identifiable persons to which personal data relates) Regulated: data controllers and data processors (natural persons, businesses, government agencies, etc.)	Protected: consumers (California residents) Regulated: business-doing entities	Protected: natural persons Regulated: handler of the informations (both organizations and individuals)

The protected informations	Personal data (any information relating to an identified or identifiable data subject)	Personal information (every information that identifies, relates to, describes, is capable of being associated with, or may reasonably be linked, directly or indirectly, with a particular consumer or household)	Personal information (any type of information that identifies or can identify natural persons recorded electronically or by other means, but does not include anonymized information)
The legal basis of processing	Six equal legal basis as the requiments of rigtful data processing (consent of the data subject, contract, legal obligation, protection of vital interests, public interest and legitimate interest)	None	Seven legal basis as the requiments of rigtful data processing (the individual’s consent is obtained; as necessary to conclude or perform on a contract to which the individual is a party, or as necessary for carrying out human resource management in accordance with lawfully formulated labor rules systems and lawfully concluded collective contracts; as necessary for the performance of legally-prescribed duties or obligations; as necessary to respond to public health incidents or to protect natural persons’ security in their lives, health, and property in an emergency; handling personal information within a reasonable range in order to carry out acts such as news reporting and public opinion oversight in the public interest; for a reasonable scope of handling of personal information that has been disclosed by the individual or otherwise already legally disclosed in accordance with this Law; other situations provided by laws or administrative regulations.

Privacy notices	Information have to be provided to the data subject. The privacy notice must contian various informations: the identity and the contact details of the controller, the contact of the data protection officer, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, the recipients or categories of recipients of the personal data, etc.	Businesses must inform consumers about the personal information categories collected, the intended use purposes for each category. Further notice is required to collect additional personal information categories. or use collected personal information.	handlers shall truthfully, accurately, and completely notify individuals of the following matters in a conspicuous fashion and in clear and understandable language: the organizational or personal name of the personal information handlers; the purposes of handling the personal information, the methods of handling, and the type of personal information handled, and period it will be stored; the manner and procedures by which individuals are to exercise their rights under this Law; other matters that laws and administrative regulations provide shall be announced.
The rights of the data subjects	GDPR provides the following rights for the data subject: the right to acces, the right to data portability, the right to request erasure, the right to be forgotten, the right to reflectation, the right to restrict processing, the right to object to processing, and the right to object to automated decision-making.	All the rights mentioned in the GDPR, except the right of rectification and the right to object to processing.	The right to know and make decisions about the handling of their personal information, the right to limit or refuse the handling of their personal information by others, the right to access and reproduce their personal information from personal information handlers, the right to request correction, the right to request deletion, and the right to request that personal information processors explain their personal information processing rules.
The penalties	20 million euros, or four percent of the annual global revenue (whichever is the higher)	2 500 USD per violation or up to 7 500 USD per violation if it’s international	Three categories: 1. 10, 000 – 100, 000 RMB 2. up to 1 000 000 RMB 3. up to 50 000 000 RMB

Conclusion

The PIPL reminds us of the GDPR and the CCPA in many respects, but the three legislations lots of specific elements. In extreme cases, we may also have to meet the criteria set by all three pieces of legislation for a single data processing activity.

In our short comparative study, we wanted to draw attention to the most important differences, thus helping practioners and researchers who need to consider all three regulations in their work.

Sources

Bangemann Report, Europe and the Global Information Society (1994). https://www.cyber-rights.org/documents/bangemann.htm (Downloaded: 25 October 2021).

Csáki-Hatalovics Gyula Balázs: eGovernment in the Past Few Years in Hungary. Acta Univ. Sapientiae, Legal Studies, 3, 1 (2014), 8-10.

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Marini, Alice, Katefides, Alexis, Bates, Joel, Zanfir-Fortuna, Gabriela, Bae, Michelle, Gray, Stacey, Sen, Gargi: Comparing GDPR v. CCPA, Data Gudiance – Future of Privacy Forums 23. https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf (Downloaded: 25 October 2021).

Geller, Anja: How Comprehensive Is Chinese Data Protection Law?A Systematisation of Chinese Data Protection Lawfrom a European Perspective, GRUR International, 0 (0), 2020, 1.

Heimes, Rita: Top 5 Operational Impacts of the CCPA: Part 1 — Determining if you're a business collecting or selling consumers' personal information, iapp The Privacy Advisor, July 23, 2018, https://iapp.org/news/a/top-five-operational-impacts-of-cacpa-part-1-determining-if-youre-a-business-collecting-or-selling-consumers-personal-information/ (Downloaded: 25 October 2021).

Mesarčík, Matúš: Apply or not to Apply? A Comaparative View on Territorial Application of CCPA and GDPR, Bratislava Law Review 2020. Vol.4. No. 2. 81.

OECD: Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (Downloaded: 25

October 2021).

Szőke Gergely László: Az adatvédelem szabályozásának történeti áttekintése, Infokommunikáció és Jog, 2013/3, 108-109.

Voss, W. Gregory: The CCPA and the GDPR Are Not the Same: Why You Should Understand Both, CPY Antitrust Chronicle January 2021, 3.

References

1. Szőke Gergely László: Az adatvédelem szabályozásának történeti áttekintése, Infokommunikáció és Jog, 2013/3, 108-109. ↑
2. OECD: Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (Downloaded: 25 October 2021). ↑
3. Bangemann Report, Europe and the Global Information Society (1994). https://www.cyber-rights.org/documents/bangemann.htm (Downloaded: 25 October 2021). ↑
4. Csáki-Hatalovics Gyula Balázs: eGovernment in the Past Few Years in Hungary. Acta Univ. Sapientiae, Legal Studies, 3, 1 (2014), 8-10. ↑
5. Matúš Mesarčík: Apply or not to Apply? A Comaparative View on Territorial Application of CCPA and GDPR, Bratislava Law Review 2020. Vol.4. No. 2. 81. ↑
6. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ↑
7. W. Gregory Voss: The CCPA and the GDPR Are Not the Same: Why You Should Understand Both, CPY Antitrust Chronicle January 2021, 3. ↑
8. Anja Geller: How Comprehensive Is Chinese Data Protection Law?A Systematisation of Chinese Data Protection Lawfrom a European Perspective, GRUR International, 0 (0), 2020, 1. ↑
9. Rita Heimes: Top 5 Operational Impacts of the CCPA: Part 1 — Determining if you're a business collecting or selling consumers' personal information, iapp The Privacy Advisor, July 23, 2018, https://iapp.org/news/a/top-five-operational-impacts-of-cacpa-part-1-determining-if-youre-a-business-collecting-or-selling-consumers-personal-information/ (Downloaded: 25 October 2021). ↑
10. See PIPL, Article 3. ↑

11. Alice Marini at al.: Comparing GDPR v. CCPA, Data Gudiance – Future of Privacy Forums 23. https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf (Downloaded: 25 October 2021). ↑