smart cities

MDPI

Article

Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)

Igor Calzada [1,2]

[1] Fulbright Scholar-In-Residence (S-I-R), US-UK Fulbright Commission, California State University, Bakersfield (CSUB), Institute for Basque Studies (IBS), 9001 Stockdale Hwy, Bakersfield, CA 9331, USA; calzadai@cardiff.ac.uk; Tel.: +44-7887661925

[2] Wales Institute of Social and Economic Research and Data (WISERD), Social Science Research Park (sbarc/spark), School of Social Sciences, Cardiff University, Maindy Road, Cathays, Cardiff CF24 4HQ, Wales, UK

Abstract: The Personal Information Protection Law (PIPL) was launched on 1 November 2021 in China. This article provides a state-of-the-art review of PIPL through a policy analysis. This paper aims to compare the three main worldwide data privacy paradigms that exist at present: (i) the General Data Protection Regulation (GDPR) in the E.U., (ii) the California Consumer Privacy Act (CCPA) in the U.S., and (iii) PIPL in China. The research question is twofold: (i) how will PIPL affect the data privacy of Chinese citizens and consequently, (ii) how will PIPL influence the global digital order, particularly paralleling the existing GDPR and CCPA? In the first section, this article introduces the topic of data privacy as a global concern, followed in the second section by an in-depth policy context analysis of PIPL and a literature review on privacy that elucidates in particular the impact of the Social Credit System (SCS). In the third section, a comparative benchmarking is carried out between the GDPR, CCPA, and PIPL. Methodologically, policy documents around PIPL will be analyzed. In the fourth section, the case study of Shenzhen will be examined by undertaking a multi-stakeholder analysis following the Penta Helix framework. The article concludes by responding to the research questions, acknowledging limitations, and presenting future research avenues.

Keywords: PIPL; data privacy; China; Social Credit System; smart cities; GDPR; CCPA; benchmarking; DAOs; Shenzhen

Citation: Calzada, I. Citizens' Data Privacy in China: The State-of-the-Art of the Personal Information Protection Law (PIPL). *Smart Cities* **2022**, *5*, 1129–1150. https://doi.org/10.3390/smartcities5030057

Academic Editor: Pierluigi Siano

Received: 12 August 2022
Accepted: 5 September 2022
Published: 8 September 2022

1. Introduction: Data Privacy as a Global Concern

Broadly speaking, a smart city should be a city that utilizes data science and technology to gather data, improve citizen life, and manage resources effectively and efficiently. Technology, embodied through so-called smart cities, has been therefore integrated into nearly all aspects of public and private urban life, promising opportunities to optimize key components of human settlements including mobility, energy, water, healthcare, education, housing, public services, public space, physical infrastructure, and the environment [1].

However, over the last several years, a debate has emerged worldwide about citizens' data privacy issues [2,3]. With the advent of big data, the value chain of such data seems effective in smart cities, which cannot be understood without the technological success of the smart city [4]. Big data is also closely connected to the way citizens can be surveilled [5]. Data sharing, trust, governance, stewardship, and co-operatives are, among other things, several related notions that have arisen around the idea of the city as a platform [6]. Citizens should not only be considered data providers insofar as their lives may depend increasingly on their decisions regarding their data [7]. However, we still witness the same promise of data-driven cities attempting to materialize by a burgeoning compliance with data privacy needs. Despite the sensorization of smart cities, they have created

an ongoing industry, which, despite its advances, has raised privacy concerns, sparking a variety of regulatory frameworks worldwide [8]. As Véliz argues, surveillance is creeping into every part of our lives—from the moment we wake up and check our phones, to when we are listening to our smart speakers or surfing the Internet—our personal data is being constantly captured by Big Tech corporations in a hyperconnected data economy [9].

Data privacy nowadays is a triggering issue. Reports focused on privacy issues and digital rights have become numerous in popular media. Indeed, there is an exponentially increasing number of online users on the Internet. In particular, more and more online events like remote working and online classes have become more widespread during COVID-19. However, more online events mean more personal data that one is required to share, which calls for a system that can soundly protect personal information. Citizens are facing the simultaneous need to maintain privacy and reveal personal information for the purpose of obtaining diverse services [10]. Under the conditions of the digital economy, data privacy thus has already become a global concern, and probably a geopolitical battleground in terms of data and digital sovereignty [6].

Against this backdrop, there are the regional typologies in data governance worldwide: (i) the GDPR in the E.U. [11], (ii) the California Consumer Privacy Act (CCPA) in California in the U.S. [12], and (iii) the recent data regulation called the Personal Information Protection Law (PIPL) in China [13]. The latter seems to emulate the goals of the so-called GDPR, and being effective from 1 November 2021. Furthermore, data sovereignty will prevail in an increasing number of policy debates and discussions around the globe including E.U., U.S., and China, thus sparking an insightful diversity of reactions [6]. It goes without saying that the so-called Social Credit System (SCS) in China may also be deeply influenced by this new regulation insofar as data privacy is at the core of this main regulation [14,15]. Reijers et al. define the citizenship regime associated with SCS in China as *cybernetic citizenship* arguing that "SCS shapes the space, time, and interactions among peer citizens, and these are turned into communicating nodes that are put into a systemic relation with defined ends of their political community" (p. 8). Privacy needs stemming from PIPL cannot be explained without the deep influence that SCS—even beyond technical interpretations—has been imposing over citizens and the emerging citizenship regime called *cybernetic citizenship* that has been exacerbated in postpandemic China. This article takes a technopolitical position to analyse data privacy from a global perspective rather than from a particular technical perspective or with an eye for the practical implications of data privacy [16]. In doing so, this article adopts a comparative policy approach. As such, comparing three global paradigms is presented as a macropolicy analysis that is far from a pure technical perspective. Moreover, given the scope of the policy analysis suggested, technical cases should be made case by case, while taking into account the point of departure that this article elucidates. Failing to do so might potentially disable comparative global academic observations by taking an extremely partial focus and not focusing on context-specific dimensions, such as SCS and *cybernetic citizenship*.

The globally widespread phenomenon of algorithmic disruption has led to new consequences—such as hypertargeting through data analytics, facial recognition, and individual profiling—perceived by many as threats and resulting in undesirable outcomes, such as massive manipulation and control via a surveillance capitalism push in the United States (U.S.) and the SCS in China [5,14]. In contrast, these technopolitical concerns raised a debate in Europe that crystallized into the General Data Protection Regulation (GDPR), which came into being in May 2018. The emergence of the algorithmic disruption has spurred a call to action for cities in the European Union (E.U.), establishing the need to map out the technopolitical debate on "datafication" or "dataism" [2]. Moreover, the disruption has also highlighted the potential requirements for establishing regulatory frameworks to protect digital rights from social innovation and institutional innovation [17]. Such policy experimentation frameworks for urban governance cover not only demands for privacy, but also ownership, trust, access, ethics, AI transparency, algorithmic automatization, and, ultimately, democratic accountability [18].

With a particular focus on China that dates back to the 1980s, we see that along with China's reforms and its opening to a new version of urban capitalism [19], some researchers have started to consider the definition of privacy in China as a general idea [20]. Although experts oversaw the legal protection of privacy based on China's existing situations, their work remained out of public view for years. In China, personal information was often leaked, leading to identity theft. In fact, there are a lot of laws, such as the Consumer Protection Law and the Cybersecurity Law, which contain content related to personal information protection [21]. But these laws are hard to implement, owing to ineffective law enforcement and little public attention.

In recent years, with the rapid development of Internet of things (IoT) and mobile payments and especially online shopping on sites like Taobao and JD in China, many consumers are willing to offer their personal information to purchase items on these platforms, given the ability to shop 24/7 and the trust that exists between buyers and sellers [22]. Only when brands offer more information proactively and guarantee consumers' information protection will the consumers build up a sense of trust. As online consumers, Chinese citizens began to defend their interests by using the power of the Internet [23]. In this scenario, the issues of data privacy are highly considered because it is much easier to sell the personal information of customers. In addition, current big data discrimination issues are widely considered; this refers to intelligent algorithms that decide price in a biased manner based on big data analytics [24]. For instance, such unfair algorithms can learn the potential customers who perhaps buy cars frequently by using big data analysis and offer them at higher prices to buyers because of the built trust.

In particular (and this is the focus of this article), during the COVID-19 pandemic, too many facial recognition platforms and other forms of information collection further led to higher demands for protection of personal information [25]. A variety of social issues regarding technological development urged the Chinese government to establish and launch PIPL. PIPL, the recent data privacy regulation, basically focuses on personal information protection and social problems that concern citizens [26]. PIPL regulates data privacy based on individual and data-handler perspectives. Moreover, the government constricts data transmission and algorithmic requirements that risk personal information leakage.

Before the publication of PIPL, GDPR and CCPA were the two regulations stressing the right to personal data. GDPR is one of most comprehensive regulations on data privacy worldwide. Compared with the GDPR and CCPA, PIPL has several similarities with regard to data privacy issues, but it is much shorter and has less detailed content. Additionally, PIPL takes several innovative articles based on Chinese current conditions into consideration, which was not the case for the previous two regulations.

Hence, this article aims to shed light on the recent PIPL regulation in China while providing a benchmarking and comparative study about the existing three hegemonic paradigms in the global digital order at present. This article opens a new research line on comparative data privacy by examining the main three data privacy paradigms at present: the General Data Protection Regulation (GDPR) in the E.U., the California Consumer Privacy Act (CCPA) in the U.S., and PIPL in China. Consequently, the research question of this article is twofold: (i) how will PIPL affect the data privacy of Chinese citizens and, more broadly, (ii) how will PIPL influence the global digital order, particularly by paralleling the existing GDPR and CCPA [27]?

This article focuses pre-eminently on a provision of PIPL's state of the art through a policy analysis by comparing the abovementioned three worldwide data privacy paradigms. Hence, despite the existence of a rich and vast amount of technical literature on data privacy (and in particular data protection), this article aims to open up a new research avenue from a policy perspective, rather than providing practical applications from a technical perspective. In order to respond to the research questions above, this technical perspective, though necessary and extremely interesting, goes beyond the scope of this article. Nonetheless, given that the main contribution of this article is framing the global

digital policy context by locating PIPL in the core of the analysis, this article invites further technical interpretations and examinations about practical applications not only about PIPL but also about GDPR and CCPA. Moreover, given the extremely timely launch of PIPL, it could be still too nascent to conduct empirical research on technical differences when the global regulatory frameworks are currently being deployed. In summary, this article should be understood as a point of departure to initiate a new research avenue on data privacy regarding the main digital policy paradigms.

The article is structured as follows. In the next section, a literature review on data privacy and policy context analysis on China's PIPL will be described, followed by a comparative analysis of the three paradigms. The fourth section revolves around the case of Shenzhen to provide insights on the way stakeholders are interpreting the aftermath of PIPL. The article concludes by (i) answering the research questions, (ii) highlighting some limitations about the scope of this article given the timely content, and (iii) suggesting future research avenues.

2. Literature Review on Data Privacy and Policy Context Analysis on PIPL

This section provides an in-depth analysis of the policy context of PIPL in China. This section shows how PIPL could be a game changer not only in the global digital order but also internally with regard to SCS.

The SCS was launched by the Chinese Communist party in 2014 to give shape to civic life in the urban realm, through city pilots and commercial platforms in cyberspace. This article argues that SCS represents the introduction of *cybernetic citizenship* governance [15], by systematizing a range of recursive feedback loops that harbor the potential to affect the lives of citizens anywhere, at any time. During the pandemic, the SCS has been used to adapt governance to impact the behavior of citizens [28]. The costs and benefits imposed by the SCS are not of a monetary nature, but rather attach to one's general standing as a citizen, bestowing certain privileges and restrictions. With regard to data privacy, the SCS has introduced a radically new form of citizenship governance, one that most likely must still be proven in terms of effectiveness but which nonetheless is rigorously pursued by the Chinese government. The literature review shows the value that the Chinese government places on citizens' data privacy, and this should ensure a proxy to consolidate data sovereignty internally and externally [6,29–36]. Thus, PIPL and SCS might be seen as mutually reinforcing a data governance model and data sovereignty.

Regarding data sovereignty, it is worth mentioning the key contribution made by Yanqing, which reinforces the main idea of this article around data sovereignty, data privacy, and cross-border data access. According to Yanqing [37], "China has chosen to uphold the traditional concept of sovereignty in cross-border data access, based on the overall international situation and the need to safeguard China's overall sovereignty, security, and development interests. (…) Can China strike a balance between old principles and flexibility and smartly safeguard data sovereignty?" (p. 16). The more data flows China attracts, the more control it can gain. Unlike physical territories, data inevitably flows across borders. Thus, data sovereignty should be more than a government's control over data within its jurisdiction: it must enhance the capability to access, process, and utilize local and extraterritorial data through flows and ecosystems [8]. To safeguard data sovereignty, China should allow Chinese private firms to access and utilize more data globally, even competing with the broad U.S. network of global firms. PIPL should be understood to be entirely connected with the idea that the scope of data sovereignty should be extended. While adhering to the traditional concept of sovereignty and multilateralism, in the digital era, China, through PIPL, seems to establish a good data flow order for Chinese private firms with globally integrated operations. Thus, PIPL is a critical component in the local and extraterritorial design of China's model of cross-border data access; consequently, SCS serves to internally consolidate data feeds and flows.

Before conducting the literature review on data privacy, it is worth addressing several points on the SCS [14,15]: (i) the SCS is preeminently a sociotechnical system that

explicitly targets citizenship by (ii) involving city pilots and smart city initiatives, agencies of regional and national government, and Big Tech platforms [38–41]. Thus, this article establishes a linkage between SCS and data privacy through the main, common idea that both are based on professional ethics and behavioral norms. Data privacy, with an initial emphasis in terms of rolling out commercial interests for consumption, shows—alongside SCS—that the main motivation is covering all of society and thus establishing a new rationale behind the nexus of data and citizenship [42–44]: a data governance framework driven by cybernetic citizenship while being monitored through data sovereignty [6,14,15]. This article does not attempt to cover this interesting dimension, but it encourages future research avenues about it at the end of the article.

2.1. Literature Review on Data Privacy

Privacy is a concept containing a series of social situations, and thus general ideas of privacy are quite intuitive considering the daily lives of citizens [9]. Many definitions of privacy prefer to point out an important feature of privacy [45]. Data privacy is an area of data protection, with particular attention paid to sensitive data, which is personal information privacy [46]. Data privacy refers to the right to select what personal information is known to different groups of people [47]. The definition points out the content of information controls on individuals and their conversation and behaviors [48]. Privacy in Chinese can be translated as *yinsi*, which means personal things that people are not willing to tell one another or discuss in public [49]. Regulations nowadays usually look for terms that have strong connections with data privacy like information protection. The definitions vary based on the development of technology because advanced techniques might have the risk of introducing new data privacy issues. In society nowadays, most people hold some idea about the importance of data privacy, but it is difficult to provide citizens with an exact definition of data privacy [50]. Therefore, regulations like GDPR and CCPA propose norms on data privacy and illustrate the rights of companies and individuals to set constraints on the issue rather than defining them. Such regulations that protect individual fundamental rights can play an essential role in the construction of datafied societies that aim to be known as "democratic" [51]. During the pandemic in China, there is no doubt that providing some personal information like contact tracking could help stop the spread of COVID-19 [52–54]. In such conditions, to tackle the surveillance issue of concerned citizens, data privacy regulation could develop a consensus on how to use personal data based on current issues.

Globally speaking, the questions regarding personal information date back to the 1970s, the period during which computer usage became widespread. When governments and organizations coped with a large amount of data through large-scale computers, it was hard for traditional legislation to handle issues pertaining to the illegal collection and use of personal data [55]. Since then, personal data privacy has become highly regarded, and the legislation on this subject keeps evolving in both the U.S. and the E.U. Coob [56] tracks the development of data privacy legislation in the U.S. Starting with the Fair Credit Reporting Act (FCRA) in 1970, which addressed the interest of individuals, the U.S. government has enacted various data protection legislation, aiming to ensure that personal interests in a wide range of situations can be protected. In the E.U., the Data Protection Directive regulated the processing of personal data, until even more comprehensive regulation, the GDPR, evolved toward the European Data Governance Act, which was framed through the European Strategy for Data [57–61].

China has seen rapid growth regarding the Internet and IoT, despite the fact that the Chinese GDP is still a quarter of the North American GDP. China's embrace of capitalism has allowed unprecedented growth due to the highly interregional competition between civil servants' leadership [19,53]. This resonates with the recent publications on the importance of city-regional data ecosystems [8,62]. The hypothesis of this present article, in light of the recent PIPL regulation, is that the Chinese government is interested in data privacy insofar as it can be arranged in sectoral data ecosystems at the city-regional level

as a way to deploy data devolution with city-regional civil servants competing for the best data privacy program for their fellow citizens [33,63].

In the 1980s, the Township and Village Enterprises promoted by Deng Xiaoping contributed to this growth. Citizens started to consider their individual interests due to the developing economy. At that time, the awareness of the right to data privacy had been discussed a great deal outside China, but only a few scholars began to develop this area [20] within China. Since 2003, the Chinese government has worked on regulating personal information protection in digital processes and formed a preliminary patchwork of regulations, and such scattered regulations have been spread out among a variety of laws [21]. However, the outcome of the implementation was not obvious because the Internet was not universal. Over the course of the decade, with the rise of online shopping, and especially due to the pandemic, citizens in China have been providing a large amount of data when purchasing products. The Chinese government is aware that they should overcome the 25% of the North American GDP if they need to become the most innovative country worldwide. To achieve this, citizens' data privacy needs to be highly considered as a critical factor.

In conducting a literature review on data privacy, this article found several remarkable sources in China. According to authors such as Yao-Huai, data privacy development in China was shifting due to the influence of Western values [49]. Jingchun also demonstrates historical data privacy in China compared with Western countries [20]. These sources suggested that the discussions on data privacy were once popular at the beginning of the 21st century. However, a comprehensive development of the literature on the privacy issue is absent and scarce from the policy perspective.

By contrast, there is a rich and remarkable literature from the technical perspective that provides practical interpretations [64–72]. Peng et al. interestingly elaborate on the need to design a privacy-preserving, contact-tracing framework by proposing P2B-Trace based on blockchain [64]. Blockchain has gained its momentum in the postpandemic technopolitical era, and key literature has already addressed the idea of crypto-politics with regard to encryption and democratic practices in the digital era [65]. As such, it is worth going back in history to trace the origin of such cutting-edge technical developments that are at the origin of blockchain. Timothy May [66] argued in 1988 by launching *The Crypto Anarchist Manifesto* that "Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable…. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation."

Despite the fact that there is a long discussion about how to protect data privacy from the technical perspective, this article does to aim to cover this scope. Nonetheless, Chen and Zhao [67] present an analysis on data security and privacy protection issues associated with cloud computing across all stages of the data life cycle. Peng et al. [68] overcome the data-sharing, server-centric approach by suggesting BlockShare as a privacy-preserving, verifiable data-sharing system based on blockchain. Tavani and Moor [69] controversially suggest an interesting standpoint around privacy from the technical perspective. According to them, privacy-enhancing technology (PET) tools do not necessarily ensure privacy protection; instead, these tools can actually blur the need for privacy protection. In order to avoid such technical issues, Gao et al. [70] suggest reducing the transmission cost of blockchain confidential transactions through the novel communications of an efficient, non-interactive, zero-knowledge, range proof protocol that does not have a trusted setup called SymmeProof. This protocol is based on blockchain cryptocurrencies to avoid tampering attempts from minority attackers by maintaining a copy of all transactions at distributed participants. Wang et al. suggests a survey with results on the privacy

protection of blockchain [71]. Interestingly, these authors provide several existing solutions to the current problems of user identity and transaction privacy protection, including the coin-mixing mechanism, zero-knowledge proof, ring signature, and other technologies. Finally, Peng et al. [72] suggest BU-Trace, a novel permissionless mobile system for privacy-preserving intelligent contact tracing based on QR codes and NFC technologies. These authors found that BU-Trace can achieve a privacy-preserving and intelligent mobile system for contact tracing without requesting geo-location or other privacy-related permissions.

More recently though, the Stanford Decentralized Autonomous Organizations (DAO) Workshop that took place on 1 September 2022 at the University of Stanford showed new developments regarding data privacy, blockchain, and DAOs [73]. The author of this article has been selected to be among the group of participants and contributed to the main conclusions of the workshop in Palo Alto, California (U.S.). Consequently, among the outcomes of the workshop, there are several practical implications about data privacy worth noting in this article. There are emerging applications around privacy protection that are increasingly related to DAOs. As such, depending on the specific global scenarios we are referring to, data privacy levels could vary and thus could be personalized differently to satisfy different demands. Stemming from the workshop conclusions, this article argues that user privacy protection schemes are reliant on the specific data privacy global paradigm. Generalizations about how to tailor users' privacy protection schemes will result in a rather difficult task. This analysis and conclusion are based on discussions with global experts on blockchain and DAOs regarding data privacy. What is also true is that data diversity and dynamics should be considered when conducting privacy protection initiatives. At present, there is an exponential emergence of data privacy protection around the three different data privacy regulations worldwide that this article aims to cover.

To back up this analysis regarding the technical perspective on data privacy, it is worth considering the article published by Rennie et al. [74]. According to them, data privacy and blockchain governance occur through a combination of social and technical activities, involving smart contracts, deliberation within a group, and voting. In their article, SourceCred open-source software is used through decentralized communities to allow data privacy and anonymous interactions. This ethnographic research suggests the importance of merging and blending technopolitical, social, and pure technical perspectives on data privacy and blockchain governance. Furthermore, the more applications about data privacy protection are emerging, the more obvious seems to be the fact that the technical perspective needs to include a macro-technopolitical perspective about global regulations as well as the context-specific social and community-driven factors.

Consequently, beyond the scope of this article, there is a remarkable amount of technical literature on data privacy. Nevertheless, being consistent with the research question of this article, the focus of this article is a policy analysis rather than a technical, nuanced examination of data and its privacy. The article preeminently aims to provide a point of departure for further nuanced detailed research on this topic. Therefore, it would be extremely ambitious to cover more perspectives. Having said that, the research question in itself invites future research technical initiatives, examinations, and developments that could contribute to the preliminary framework of this article in responding in two directions: (i) how PIPL will be affecting the data privacy of Chinese citizens, paying special attention to the SCS, which is indeed the emphasis of this article; and (ii) how PIPL is already influencing the global digital order, paralleling the existing GDPR and CCPA.

This article asks, therefore, why data privacy has jumped onto the policy table in China. In order to learn why, the literature review of this article has found a great number or reports and news recently emerging, which began to pay more attention to the citizens' data privacy issue, especially at the governmental level beyond the purely technical perspective. Consequently, the next subsection focuses on the policy content analysis of these sources.

2.2. Policy Content Analysis on China's Data Privacy Regulation, PIPL

PIPL is a milestone for regulating the protection of personal information specifically, which will guarantee the right of individuals and place constraints on enterprises. Together with the Cybersecurity Law (CSL) and Data Security Law (DSL) that were established previously [28], PIPL constructs a comprehensive framework for regulating information protection and cybersecurity [75]. In this subsection, this article basically refers to the translation of the finalized PIPL provided by Stanford Digichina [76] and an official finalized version can be found on Chinese websites [77]. Generally, the policy analysis is divided into three parts: (i) a general description and explanations of key terms, (ii) rights and obligations from a multi-stakeholder perspective [78], and (iii) special regulations connected to social issues.

2.2.1. General Description

Within PIPL, personal data privacy is the main focus of regulation. The regulation first clearly defines several terms that apply frequently. First, the key term, personal information, is regarded as all kinds of information related to identified or identifiable persons, excluding the information after anonymization processing (Article 4). Personal information in PIPL stresses the electronic approach to record data, implying that there is a large amount of online data that needs to be regulated. Additionally, personal information handling includes all basic operations on personal data such as collection, storage, use, and processing (Article 4). In addition, PIPL sets a standard norm for most enterprises on personal information protection. Thus, it is essential to clarify the definition of enterprises or companies. Such roles are so-called personal information handlers, indicating organizations and individuals that decide handling purposes and handling methods automatically in personal information activities (Article 73). Under this description, PIPL can be effective in most enterprises because it places a lot of constraints on such handlers. To illustrate more specifically, we will apply Shenzhen as a case study. The selection of Shenzhen is due to the many high-tech companies that are based in this city; this provides an insightful manner by which to approach to the impact of PIPL on city-regional stakeholders [78].

2.2.2. Right and Obligation from a Multi-Stakeholder Perspective

After demonstrating well-defined terms, we need to figure out what rights that citizens or individuals have and what obligations that handlers should take. In Chapter 4, individuals are enabled to make decisions about and limit their own personal information; they have the right to know how data handlers process private information (Article 44, 47). In particular, the range of individuals is expanded to include deceased individuals (Article 49).

As for handlers, PIPL sets multiple constraints on them in Chapter 5, which mainly requires data compliance and internal management. In Article 51, handlers are required to take measurements of personal information with secure techniques and to raise employee's awareness by security education training. For special personal data such as sensitive data, evaluation of such data is needed for checking the impact of protection (Article 55, 56). In particular, for those larger handlers such as Big Tech companies like Alibaba, which hold large amounts of user data, protection systems should be established and supervised by outsiders, and there is remarkable punishment for larger handlers who violate regulations (Article 58). This suggests that the larger handlers should be more transparent in processing personal data.

In addition, PIPL illustrates the responsibilities of departments that fulfill the protection of personal information as outlined in Chapter 6. Acting as supervisors, such departments generally oversee the personal information handlers and cope with complaints from citizens (Article 61). Notably, PIPL points out the duties of state cybersecurity and informatization departments, which includes tech support, security promotion, and

personal information system construction (Article 62). This article implies that the state departments are required to establish more specific adjustments based on PIPL. From Chapter 4 to Chapter 6, PIPL ensures the rights of citizens to have their private information managed by handlers or enterprises with more obligations and constraints.

2.2.3. Special Regulations Connected with Social Issues

There are several articles that deserve to be pointed out, as they connect to issues in Chinese society, particularly with regard to SCS. In Article 24, automated decision-making is particularly mentioned as the price of various applications nowadays, which largely depends on intelligent algorithms that extract information from big data [24,79–82]. With this article, the process of decision making is required to be more transparent and eliminate unreasonable treatment in trading. With the exception of decision making, PIPL also addresses the issue of face recognition in Article 26 and Article 28 [83].

The surveillance system in China is already well developed [84]. In the construction of smart cities, mass surveillance serves to measure, track, and analyze data from various aspects of life including air quality and traffic congestion [85]. During the pandemic period in particular, tools that tracked people who had contracted the virus resulted in slowing its spread. However, Article 28 clarifies the nature of sensitive personal information, which includes individual location tracking. Image collection and identity recognition equipment are only acceptable under the purpose of maintaining public security (Article 26). It is a tradeoff between personal privacy and digital measurement [86].

In the description of sensitive personal information, the personal information of teenagers under 14 are included. Nowadays, an increasing number of adolescents are addicted to online games [87], which means their personal information is exposed much more easily and without any protections. Therefore, when PIPL handles sensitive personal information in Chapter 2, this type of data is stressed in Article 28 and Article 30. It implicitly suggests that the Chinese government highly considers the development of adolescents.

From the general analysis of PIPL above, this article analyzed the policy regulation with three main parts. It is essential to learn about citizens' rights and the duties of companies or enterprises. In addition to endowing citizens with basic rights, there are more constraints on enterprises to set boundaries for managing private information. In addition, for those articles that relate to current social issues, the Chinese government highlights issues that citizens are urged to understand with regard to PIPL, because any behaviors in violation could be recorded immediately in the Chinese SCS. This point might open new lines of inquiry regarding the consequences of PIPL and the relation to the SCS and the associated *cybernetic citizenship* emerging in postpandemic China [14,15]. This article does not aim to focus on this relationship insofar as it aims to provide a state-of-the-art report on PIPL from the policy perspective.

3. Method: Comparative Analysis of Data Privacy Regulations Worldwide

The debate that is at stake at present is about *people-centered smart cities* and the appropriateness of data governance models in different regions worldwide [18,88]. There are a wide range of factors related to different typologies of cities, cultural aspects, urban traditions, levels of development, and political systems that provide a complex landscape of smart city approaches [89,90]. However, all these factors are embedded in a real context, making it difficult to extrapolate or generalize. Therefore, to reduce the complexity of each regional typology (North American, European, and Chinese) could be problematic and pose insurmountable hindrances with regard to making generalizations about data governance models. How can the people-centered approach be a good lens by which to distinguish regional typologies by respecting each region's singularity and contextual factors? At present, at least in the North American, Chinese, and European regional typologies, data regulation, and governance models vary from each other and co-exist by influencing smart city approaches, as it is depicted in Table 1 [1].

Table 1. Depicting three data privacy regulations in the global digital order: GDPR, CCPA, and PIPL.

Global Digital Orders	Data Privacy Regulations	Smart City Policy Approach
European	General Data Protection Regulation (GDPR) [11] Data Governance Act (DGA) [58–60] Digital Markets Act (DMA) Digital Services Act (DSA)	H2020-Smart Cities and Communities [1]
North American	California Consumer Privacy Act (CCPA) [12]	Surveillance Capitalism [5]
Chinese	Personal Information Protection Law (PIPL) [77]	SCS [14,15]

The GDPR in Europe is considered to be one of the strictest privacy laws; it was put into effect in May 2018. Another law with significant meaning is CCPA in the U.S.; it took effect in January 2020. The advent of these two privacy laws grabbed a huge amount of attention from researchers and law experts [91]. With swift growth in new economic sectors like the consumer and technology sectors, there is no doubt that the upcoming implementation of PIPL in China takes a wide variety of factors into consideration and compares with the previous two privacy laws.

While PIPL was launching in November 2021 [26], the European Commission published the Data Governance Act [60]. The latter sought to ensure fairness in the allocation of value from data among actors in the data economy and sought to foster access to and the use of data by establishing some access and sharing obligations for companies collecting and generating data. Despite the ambitious goal of the Data Governance Act, it focuses on data generated by IoT products and related services, but left out Big Tech, digital platforms, and Telcos, which were arguably the largest producers and holders of data. Still, given the importance of IoT for cities, the Data Governance Act might have important effects on the creation of urban data markets and in city governments' ability to access data to make better policy choices. To complete this gap, and primarily to attempt to regulate Big Tech companies, in December 2020 and on 25 March 2022, the European Commission launched, respectively, two legislative initiatives to upgrade rules governing digital services in the EU: the Digital Services Act (DSA) and the Digital Markets Act (DMA). Two main goals were addressed: (i) to create a safer digital space in which the fundamental rights of all users of digital services were protected, and (ii) to establish a level playing field to foster innovation, growth, and competitiveness, both in the European single market and globally.

To develop the in-depth comparisons emphasizing similarities and differences among PIPL, GDPR, and CCPA, this article basically refers to the content of these three privacy laws and regulations [11,12,77], expanding several comparative perspectives based on PIPL. Since PIPL was released, there have been many online reports making comparisons between PIPL and GDPR. However, few papers and other online resources have made a sound comparison between PIPL, GDPR, and CCPA. Therefore, by organizing the existing online sources, primarily dividing comparisons between PIPL and GDPR and comparisons between GDPR and CCPA, this article first analyzes these laws and regulations from the perspective of four dimensions (Table 2): (i) coverage, (ii) key terms (enterprise duties, personal information, and sensitive personal information), (iii) individual digital rights [17], and (iv) restrictions on cross-border data handling. Thereafter, this article concludes with the similarities and differences among them and an analysis of potential factors that affect these differences, as shown in Table 2.

Table 2. Comparing three data privacy regulations through four dimensions.

4 DIMENSIONS	PIPL	GDPR	CCPA
		1. COVERAGE	
	All entities within China's border. Apply to those who process personal information about Chinese individuals outside China's border. (Article 3)	All entities that process personal data, established in the EU. Apply to those non-EU entities that process personal data inside the EU.	All Californian residents living within California federal state.
		2. KEY TERMS	
1. Enterprise duties	Regards as personal information handler, referring to organizations and individuals autonomously deciding handling purposes and handling methods under the activities of personal information handling. (Article 73)	Regard as controllers who holds data with authority of decision making.	Regards businesses that operate for profit and decides why and how personal information is processed, located in California.
2. Personal information	All kinds of information, recorded by any means, related to identified or identifiable natural persons. Anonymous information is excluded. (Article 4)	Any information relating to identified or identifiable natural citizen.	Information that identifies directly or indirectly with a consumer or household.
3. Sensitive personal information	Includes biometric characteristics, religious beliefs, specially designated status, medical health, financial accounts, individual location tracking and personal information under the age of 14. (Article 28)	Regards special category information, including racial or ethnic origin, political opinion, religious beliefs, trade union membership, genetic or biometric data, health data, sex life or sexual orientation.	Does not mention the related term explicitly but enhances several types of data such as health information and social security number.
		3. INDIVIDUAL DIGITAL RIGHTS	
	Data portability is allowed if CAC conditions are satisfied.	Data portability is allowed.	The right to equal services and prices.
		4. RESTRICTIONS ON CROSS-BORDER DATA HANDLING	
	Pass security assessment, obtain authoritative certification, or make standard recipient contract.	"Appropriate safeguards": binding corporate rules (BCRs), standard contractual clauses (SCCs) and a conduct code.	No restrictions.

3.1. Dimension 1: Coverage

The territorial scope, basically demonstrated as citizens, points out the kinds of person and behaviors that are applicable to laws. This analysis can observe that the scope of PIPL and GDPR is similar and is not limited inside the borders of their respective regions. However, the applicable range for CCPA is relatively narrow because it is used only for California.

3.2. Dimension 2: Key Terms (Enterprise Duties, Personal Information, and Sensitive Personal Information)

As for the key terms, all definitions of enterprises stress the entities that process personal information. However, whereas the GDPR, reinforced with DGA, DSA, and DMA,

attempts to regulate Big Tech companies in the EU, PIPL seems relatively more concerned with gathering data from businesses for the government in order to potentially feed and improve SCS. Lastly, CCPA seems to address consumer transactions. Personal information emphasizes the words "identifiable" or "identified". Apart from personal information, there is a specific category called sensitive personal information in PIPL, Chapter 2, Section 2, whereas GDPR regards it as special category information. Both PIPL and GDPR list several kinds of information such as categories with extra protection and more tough regulations. Though CCPA does not mention such data types clearly, it does augment the several types of data needed to be highly considered. Compared with GDPR and CCPA, sensitive personal information in PIPL is described with more granularity and is framed in a broader list.

3.3. Dimension 3: Individual Digital Rights

Individual rights are another critical dimension by which we can measure the three data privacy laws. Basically, these three laws endow individuals with rights to information, accession, deletion, withdrawing consent, and lodging complaints. In PIPL and GDPR, individuals have the right to refuse automated decision-making, which is akin to the right to equal services and prices in CCPA. Unlike CCPA, both PIPL and GDPR also enable individuals with rights to data portability. But it only works in PIPL if conditions followed by the Cyberspace Administration of China (CAC) are satisfied.

3.4. Dimension 4: Restrictions on Cross-Border Data Handling

Between PIPL and GDPR, restrictions on cross-border data handling are clarified, whereas CCPA has no such restrictions [37,41]. With regard to globalization, adjusting cross-border data is of great issue in the digital era. The term "trilemma" is proposed, containing three components: personal data protection, free transborder flow of information, and the expansion of national jurisdiction [92]. What both GDPR and PIPL attempt to achieve is the assurance of personal data protection, one of the elements in the "trilemma". To transfer data outside a defined border, both regulations build up several measurement protections. In the GDPR, binding corporate rules (BCRs), standard contractual clauses (SCCs) and a conduct code are listed, which are regarded as "appropriate safeguards" [93]. Concerning PIPL, personal data handlers are required to pass a security assessment, obtain authoritative certification, or make standard recipient contracts (Article 38). Moreover, PIPL particularly stresses data localization once there is a large amount of data that needs to be dealt with [36,94]. Apparently, GDPR has a list of measurements on data protection, which is sound and robust. Surprisingly, the security assessment in PIPL has grabbed a lot of attention. It is possible that a security assessment can set tougher rules on specific regulations in the future. Additionally, data localization in PIPL ensures the security of citizens' data and prevents data privacy and data sovereignty from being breached by foreign surveillance [6,29].

Based on comparisons of the four dimensions above, we can see that from the perspective of coverage, it is obvious that fewer individuals benefit from CCPA because it only affects residents in one state. On the contrary, PIPL and GDPR hold the nearly same idea that not only do the regulations consider the entities from the inside, but they also consider entities from the outside. Such coverage suggests that both governments have capabilities to manage such a considerable number of citizens' data in both a technological and practical way. As for the key definitions, CCPA is only suitable for large businesses in California whereas PIPL and GDPR contain almost all enterprises that handle personal information within their respective boundaries. In addition, all explanations of personal information emphasize the word "identified". Specifically, personal information has a broader definition in CCPA including the household. Regarding sensitive information, both PIPL and GDPR define it as a special field of personal information and mention it with details whereas CCPA only enhances several kinds of sensitive information among its regulations. In PIPL, Chapter 2, Section 2 [77], all kinds of sensitive information are

listed. Similarly, a special category information in GDPR is demonstrated. PIPL covers more diverse sensitive information compared with GDPR. Because of technological development and advancement algorithms, a large amount of information may cause risks to individuals and thus are clarified as sensitive information.

In summary, even though PIPL is an innovative law in China, it is still a general concept, which needs to be specified by citizens from different aspects, including data privacy technical advancements. On the other hand, GDPR publishes more concrete ideas on personal information protection and updated regulations such as DGA, DSA, and DMA. By observing different reactions from different perspectives, the adjusted regulations are necessary. For instance, the DGA was proposed recently to address the gap that small- and medium-scale companies are reluctant to share data because of the fear of breaking privacy laws in the E.U. [95]. Therefore, PIPL should be considerate to the further adaptation on the different stakeholders as the next section will highlight with the case of Shenzhen.

4. Case Study Results: PIPL Policy Impact and Multi-Stakeholder Analysis in the City-Region of Shenzhen

This section analyzes the policy context of the PIPL in China by providing examples of stakeholders based in Shenzhen. This section illustrates the impact of PIPL through this case study. The justification of the selection of Shenzhen is explained as follows: Shenzhen has been selected and identified as a city-region in China concentrating many high-tech companies and having witnessed a rapid urbanization process over the last decade. However, a caveat should be made. The inclusion of the case study of Shenzhen does not aim to legitimize any extrapolation or generalization in this article. Consequently, the aim of this section is to describe a paradigmatic urban area in China in the early adoption of the recent PIPL regulation.

Shenzhen, located in southern China in the Pearl River Delta Region, was a small village before establishing the Special Economic Zone in 1980 [96]. For forty years, Shenzhen, as an experimental city, has gone through rapid urbanization. Shenzhen's GDP exponentially increased, achieving the total amount of 2.77 trillion yuan in 2020 [97]. Many people are attracted by its promising development. Moreover, thanks to the ideal location of Shenzhen, being near to Hong Kong and Macao, the Outline Development Plan for the Guangdong–Hong Kong–Macao Greater Bay Area [98], established in February 2019, points out that Shenzhen nowadays plays a critical role in the construction of the international modern city. Basically, the rapid growth of the economy in Shenzhen is portrayed by shipping and logistics, high-tech industry, and financial services [19,99]. It is worth noting that many headquarters of high-tech companies are located in this young city, including Tencent [100], Huawei [101], DJI [102], OnePlus [103], and SF Express [104]. For such high-tech companies, there is no doubt that they hold a large amount of personal data for developing their services. Hence, the upcoming PIPL might have a remarkable impact on the burgeoning digital city-region, especially on those high-tech enterprises.

Several months before the launch of PIPL on 1 November 2021, Shenzhen, the leading financial and production center for China and home of many Chinese Internet and tech giants such as Huawei and Tencent, enacted its regional data protection law entitled *Data Regulation of the Shenzhen Special Economic Zone* (also known as *Shenzhen Data Regulation*) on 29 June 2021. Shenzhen Data Regulation became effective on 1 January 2022.

To specify how PIPL might be currently affecting the Shenzhen city-region, this article basically considers the multi-stakeholder ecosystem in this city-region by using the Penta Helix framework (Figure 1) [38,39,78]. Extending from the triple and quadruple-helix, Penta Helix appends a fifth helix that plays a transformational intermediary role, which refers to social entrepreneurs or activists [39]. Because of the technopolitical awareness and ownership of data itself, Shenzhen, abundant with high-tech companies, should emphasize the active role of citizenship and the connection about different sectors [7]. Followed by the Penta Helix framework, several stakeholders are described inside the model, consisting of the public sector, the private sector, academia, civic society, and social

entrepreneurs. Therefore, in the following analysis, this article describes various stakeholders' attitude towards PIPL and how PIPL might affect them based on current context in Shenzhen. This analysis has been undertaken by identifying key stakeholders from the policy analysis and the literature review on PIPL with a special consideration of the case of Shenzhen. This preliminary analysis encourages further and more in-depth research in this direction.

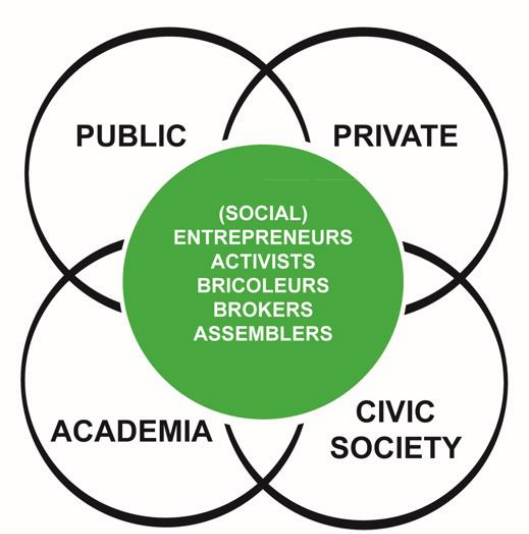

Figure 1. Penta Helix multi-stakeholder framework [1,38,39,78].

4.1. Private Sector

Shenzhen data regulations have the same set of rules for data processing as mentioned in PIPL. Violation of the personal data protection and data security rules could attract fines of up to 5% of turnover but no more than CNY 50 million. Like PIPL, for the private sector, Shenzhen data regulations restrict discriminatory treatment to customers by using data profiling. Shenzhen data regulations provide a five data minimization test that requires that personal data shall have a direct relation with the processing purpose, that the amount and frequency of data processing shall be kept to a minimum, that the time of personal data storage shall be the minimum, and that only the authorized person shall be allowed to access the minimum amount of personal data.

Companies in Shenzhen are (i) redesigning information systems to localize data for the Chinese internal market, (ii) assessing and segmenting vendors and supply chains to mitigate risks, (iii) reevaluating deals in light of altered costs and returns on investment, and (iv) modifying legal-entity structures and tax strategies to adapt to altered business operations.

It is unavoidable that private companies will manage a variety of personal information-based data and use it to unearth potential customers. Thus, PIPL might be a good regulation by which to protect citizens' data among those companies. Many private companies in Shenzhen, especially the large companies, are highly concerned about the new constraints on data because they might have a huge punishment because of the establishment of PIPL. Amazon was punished last year for breaking GDPR rules with an $886.6 million fine [105]. In China, PIPL basically holds a similar idea as GDPR, by increasing the regulatory scrutiny of data handlers. Moreover, in Shenzhen, cybersecurity inspections are initialized on popular applications such as DIDI for rideshare and BOSS for job recruitment [106]. Hence, for companies in Shenzhen, it has become necessary to adopt new regulations to protect citizens' information.

Judging from the information available in the policy documents and the literature review on specific cases in Shenzhen [107], companies generally seem to hold a positive

attitude toward PIPL. In particular, those high-tech companies are willing to employ advanced technologies and algorithms to ensure privacy security. For smartphone companies like Huawei and OPPO, this means making secure measurements of issue of users' privacy. A new operating system, Harmony OS, has been invented by Huawei, passing the highest security certification in China. The new system ensures the safety of data storage, transmission, and usage. Similarly, OPPO owns their system known as Color OS. In this system, they propose a new function to hide the users' identity, preventing the theft of personal information from applications [107]. As an online services provider, Tencent is a company owning widely used social media outlets such as WeChat. It also realizes the importance of privacy, applying various security techniques and training for employees [108].

Although the private sectors have provided a sound plan for customers by ensuring their personal information privacy, PIPL is conducive to construct a healthier system among personal data protection. As PIPL shows, data handlers need to adopt technical security measures, security education, and training, incident-response plans, and information-protection impact assessment (Article 51, 55 in PIPL). Notably, large data handlers such as Tencent and Huawei are required to be supervised by outsiders, which is the main modification made by PIPL. More importantly, because these private companies are located in the Greater Bay Area, PIPL can conduct more strict regulation on cross-border transfer data. According to Liang Zhenying [109], the vice chairman of the National Committee of the Chinese People's Political Consultative Conference, China could be the pilot program of international multilateral rules through cross-border data governance in the Greater Bay Area. Undoubtedly, this represents a significant opportunity for Shenzhen to reinforce its existing technopolitical and geopolitical position.

4.2. Public Sector

The local government in Shenzhen might be optimistic about PIPL. One piece of explicit evidence is that Shenzhen local authorities had established Shenzhen special economic zone data regulations in response to the previous data security law (DSL) [110]. As an experimental city, Shenzhen specifies that the national law clearly prohibits the illegal recommendation of algorithms and data discrimination, which plays a critical role in supervising private companies. Moreover, to achieve the goal of data commons, departments in government that hold rich resources of public data must be willing to share them with citizens [7,111]. The open-source data have been encouraged and utilized by setting up the Shenzhen innovative competition since 2019 [112]. Considering the spread of COVID-19, the Shenzhen government, like those of other cities in China, took the action of immediately including a broad application of health codes [113]. This indicates that the government in Shenzhen is capable of handling big issues in a timely manner. The research conducted found that the government might publish tougher supervisions on large companies, technical and managerial guidance on small companies, and data security education on local residents [114].

More recently, the Shenzhen city administration has started mobilizing all resources to curb a slowly spreading COVID-19 outbreak, ordering a strict implementation of testing and temperature checks, and lockdowns for COVID-affected buildings. The city has gone into full weekend lockdown with the bus and subway services being suspended, and other restrictions put into effect. This situation might reinforce the local authorities in sharing data with citizens while being compliant with PIPL and Shenzhen data regulations on privacy issues. However, as previously demonstrated during the pandemic, tough lockdown regulations go hand in hand with data privacy concerns given the increasing peak in data flows during isolation. Local authorities may take this recent situation to implement both PIPL and Shenzhen data regulations.

4.3. Academia

A handful of higher education institutions are located in Shenzhen, including Shenzhen University [115], the Chinese University of Hong Kong (CUHKSZ) [116], and the Southern University of Science and Technology [117]. All these universities make a great contribution to the research of specific fields of science. Specifically, CUHKSZ positively impacts the fields of computer and information science, big data, and data science respectively. In addition, Shenzhen University establishes regulation on data security protection, including the records of sensitive information, such as students' grades and faculties' salaries. The universities are eager to construct a public data storage system [118]. Therefore, with the establishment of PIPL, the universities are more willing to do relevant research on data privacy fields as the exploration of pertinent knowledge, especially new algorithms, might be applied in a practical way.

However, as Grobe–Bley and Kostka found [114], digital systems in Shenzhen entail a creeping centralization of data that potentially turns lower administrative government units into mere users of the city-level smart platforms, rather than being in control of their own data resources. Smart city development and big data ambitions thereby imply shifting stakeholder relations at the local level and also pull non-governmental stakeholders, such as civil society and social entrepreneurs/activists, closer to new data flows and smart governance systems. This bridging task could be reliant on key higher education institutions, in the context of PIPL and Shenzhen data regulation implementations.

4.4. Civil Society

Citizens nowadays have awareness of the privacy issue and are sensitive about r news related to this topic. For instance, an influential social media company, WeChat, recently exposed a privacy leakage issue in which the company software read users' albums automatically, drawing a great deal of attention from citizens due to its popularity [119]. Even though the official response was claimed immediately, many online users presented their concerns about the exposure of their personal information. Hence, PIPL attempts to guarantee the basic rights of citizens, including rights to information, access, correction, erasure, and so on (PIPL Chapter 4). Under such conditions, citizens in Shenzhen might benefit from the new regulations because PIPL offers additional individual rights for citizens.

The key guiding principles underpinning Shenzhen's 2018 Smart City Plan are data unification and integration. However, Shenzhen's smart governance model is highly centralized for data collection, management, and application, which may result in clear difficulties when engaging with communities and citizens. In this sense, as stated in Section 2.1. it could be interesting to explore blockchain-driven implementations, including citizens and communities by using DAOs. PIPL and Shenzhen data regulations could provide an interesting future framework by which to leverage data sovereignty. It goes without saying that the significant existing gap between big data ambitions and local realities in Shenzhen due to major technopolitical hurdles embedded in local data practices, are likely to pose potential future difficulties until they are gradually amended.

4.5. Social Entrepreneurs/Activists

Basically, there is evidence of this type of stakeholder in the fifth helix, referring to the social entrepreneurs in Shenzhen [120]. Regarding the huge damage caused by the pandemic, social entrepreneurs offer a positive response to the disaster. For example, as a social enterprise, Shenzhen link accessibility increased information accessibility for visually impaired persons during the outbreak of COVID-19 [52,121]. It may seem then that PIPL could leverage the potential of social entrepreneurs by transforming communities. The recent lockdown in early September 2022 will demonstrate the quality of the entrepreneurial fabric of the city. During the pandemic, a communitarian fabric of assistance was established to sort out these kinds of issues.

Therefore, generally speaking, PIPL can bring a positive influence on multi-stakeholders in Shenzhen. Although it is hard to adapt PIPL at the beginning especially for the private companies [53], it can bring us a relatively favorable direction on personal data protection.

5. Conclusions

This article posed a research question in two parts: (i) how will PIPL affect the data privacy of Chinese citizens, and broadly, consequently, (ii) how will PIPL influence the global digital order, particularly by paralleling the existing GDPR and CCPA?

In response to these research questions, the article has broadly described the recent PIPL regulation comparatively amid the GDPR and the CCPA.

First, despite being too early for an in-depth judgement and examination of the implications for Chinese citizens, PIPL will clearly benefit the control of data by the Chinese government and will allow for a relevant gateway for international multilateral rules through cross-border data governance [37], particularly as seen in the case of Shenzhen, given its privileged technopolitical and geostrategic localization. The aim of the article was to provide a state-of-the-art review of PIPL considering the current development in the field of data privacy. More prospectively though and with a vision for future work, we can state that this new regulation will clearly help to feed SCS and to improve it. In addition, as formulated in Section 2.1., the Chinese government aims to establish sectoral data ecosystems at the city-regional level to deploy data devolution [33]. It goes without saying that PIPL aims to rein in the previously unchecked growth of its tech giants, including the WeChat operator Tencent, and ByteDance, the company behind TikTok and Douyin. PIPL is focusing on protecting individuals, society, and particularly national security. As such, if the GDPR is grounded in fundamental rights and the CCPA is grounded in consumer protection, PIPL is closely aligned with national security. Hence, PIPL is clearly affecting data privacy of citizens and related stakeholders as this article has shown with the case of Shenzhen.

Secondly, PIPL suggests a step forward toward data sovereignty in China. The consequences of such regulation in the international digital order remain to be seen. What is clear is that PIPL, the GDPR, and the CCPA are already influencing digital policies and practices worldwide. Whereas PIPL is likely to encourage Chinese domestic companies to improve how they handle data, it will also have an impact on broader data rules worldwide. Actually, countries in Asia, namely India and Vietnam, may follow the Chinese approach of having those data localization measures in their privacy laws.

This article acknowledges some limitations given the recent regulation and the lack of evidence from the stakeholders in the case of Shenzhen. Thus, future research avenues could explore in depth how stakeholders are coping with PIPL through interviews and discuss which data governance models are emerging out of this regulation. The vision of the future work could be deployed as follows. Given the direct influence of PIPL alongside the GDPR and the CCPA in the global digital order, this article could articulate the vision of the future work around data privacy in relation to the increasingly vast activity around DAOs as presented in Section 2.1. During the Stanford DAO Workshop [73], the author of this article could witness the influence that these new digital architectures, driven by blockchain and framed through crypto-politics, will present for data privacy regulations and, generally speaking, for cross-border data flows among citizens. This article aimed at providing a preliminary state-of-the-art review to initiate this new line of research inquiry on data privacy, potentially being the point of departure for further data developments around emerging research fields including blockchain and DAOs.

Funding: This research was funded by Fulbright Scholar-In-Residence (S-I-R) Award 2022-23, Grant Number PS00334379 by US-UK Fulbright Commission and IIE, U.S. Department of State in California State University, Bakersfield and by the Economic and Social Research Council (ESRC), Grant Number ES/S012435/1 WISERD Civil Society: Changing Perspectives on Civic Stratification and Civil Repair.

Institutional Review Board Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Calzada, I. *Smart City Citizenship*; Elsevier Science Publishing Co Inc.: Cambridge, MA, USA, 2021. https://doi.org/10.1016/C2017-0-02973-7.
2. Sadowski, J.; Viljoen, S.; Whittaker, M. Everyone should decide how their digital data are used—not just tech companies. *Nature* **2021**, *595*, 169–171. https://doi.org/10.1038/d41586-021-01812-3.
3. Breuer, J.; Pierson, J. The right to the city and data protection for developing citizen-centric digital cities. *Inf. Commun. Soc.* **2021**, *24*, 797–812. https://doi.org/10.1080/1369118X.2021.1909095.
4. Löfgren, K.; Webster, C.W.R. The value of Big Data in government: The case of 'smart cities'. *Big Data Soc.* **2020**, *7*, 2053951720912775. https://doi.org/10.1177/2053951720912775.
5. Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*; Profile: London, UK, 2019.
6. Calzada, I. Data Co-operatives through Data Sovereignty. *Smart Cities* **2021**, *4*, 1158–1172. https://doi.org/10.3390/smartcities4030062. Special Issue "Feature Papers for Smart Cities".
7. Calzada, I. (Smart) citizens from data providers to decision-makers? The case study of Barcelona. *Sustainability* **2018**, *10*, 3252. https://doi.org/10.3390/su10093252.
8. Calzada, I.; Almirall, E. Data ecosystems for protecting European citizens' digital rights. *Transform. Gov. People Process Policy* **2020**, *14*, 133–147. https://doi.org/10.1108/TG-03-2020-0047.
9. Veliz, C. *Privacy is Power: Why and How You Should Take Back Control of Your Data*; Corgi: London, UK, 2020**.**
10. Pelteret, M.; Ophoff, J. A Review of Information Privacy and Its Importance to Consumers and Organizations. *Inf. Sci. Int. J. Emerg. Transdiscipl.* **2016**, *19*, 277–301. https://doi.org/10.28945/3573.
11. GDPR (General Data Protection Regulation). Available online: www.gdpr-info.eu (accessed on 8 August 2021).
12. CCPA (California Consumer Privacy Act). CCPA and GDPR Comparison Chart. Available online: https://iapp.org/resources/article/ccpa-and-gdpr-comparison-chart/ (accessed on 8 August 2021).
13. Gamvros, A.; Wang, L PIPL: A Game Changer for Companies in China. Available online: https://www.dataprotectionreport.com/2021/08/pipl-a-game-changer-for-companies-in-china/ (accessed on 29 August 2021).
14. Kostka, G.; Antoine, L. Fostering model citizenship: Behavioral responses to China's emerging social credit systems. *Policy Internet* **2020**, *12*, 256–289. https://doi.org/10.1002/poi3.213.
15. Reijers, W.; Orgad, L.; De Filippi, P. The rise of cybernetic citizenship. *Citizsh. Stud.* **2022**. https://doi.org/10.1080/13621025.2022.2077567.
16. Calzada, I. *Emerging Digital Citizenship Regimes: Postpandemic Technopolitical Democracies*; Emerald: Bingley, UK, 2022**.**
17. Calzada, I. The right to have digital rights in smart cities. *Sustainability* **2021**, *13*, 11438. https://doi.org/10.3390/su132011438. Special Issue "Social Innovation in Sustainable Urban Development".
18. Calzada, I.; Pérez-Batlle, M.; Batlle-Montserrat, J. People-Centered Smart Cities: An exploratory action research on the Cities' Coalition for Digital Rights. *J. Urban Aff.* **2021**, *43*, 1–26. https://doi.org/10.1080/07352166.2021.1994861.
19. Keith, M.; Lash, S.; Arnoldi, J.; Rooker, R. *China Constructing Capitalism*; Routledge: London, UK, 2014**.**
20. Jingchun, C. Protecting the right to privacy in China. *Vic. Univ. Wellingt. Law Rev.* **2005**, *36*, 645. https://doi.org/10.26686/vuwlr.v36i3.5610.
21. Zhou, H.H. Parallel or Intersection: The Relationship between Personal Information Protection and Right to Privacy in China. *Peking Univ. Law J.* **2021**, *33*, 1167–1187.
22. Liz, F. Survey: Over 60% of China's Online Shoppers Research Products Online Before Purchase. Available online: https://jingdaily.com/chinese-online-shoppers-research-online-before-purchase/ (accessed on 7 October 2021).
23. Emiliano, T.; Zizheng, Y. The Evolution and Power of Online Consumer Activism: Illustrating the Hybrid Dynamics of "Consumer Video Activism" in China through Two Case Studies. *J. Broadcasting Electron. Media* **2021**, *65*, 761–785. https://doi.org/10.1080/08838151.2021.1965143.
24. Gillis, T.B.; Spiess, J.L. Big Data and Discrimination. *Univ. Chic. Law Rev.* **2019**, *86*, 459–487.
25. Liu, C.; Graham, R. Making sense of algorithms: Relational perception of contact tracing and risk assessment during COVID-19. *Big Data Soc.* **2021**, *8*, 2053951721995218. https://doi.org/10.1177/2053951721995218.
26. The China Personal Information Protection Law (PIPL). Available online: https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law.html (accessed on 30 September 2021).
27. Zheng, G. Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S., and China. *Comput. Law Secur. Rev.* **2021**, *43*, 105610. https://doi.org/10.1016/j.clsr.2021.105610.

28. Chen, J.; Sun, J. Understanding the Chinese Data Security Law. *Int. Cybersecur. Law Rev.* **2021**, *2*, 209–221. https://doi.org/10.1365/s43439-021-00038-3.
29. Hummel, P.; Braun, M.; Tretter, M.; Dabrock, P. Data sovereignty: A review. *Big Data Soc.* **2021**, *8*, 1–17. https://doi.org/10.1177/2053951720982012.
30. De Filippi, P.; McCarthy, S. Cloud computing: Centralisation and data sovereignty. *Eur. J. Law Technol.* **2012**, *3*, 1–18.
31. Esposito, C.; Castiglione, A.; Frattini, F. On data sovereignty in cloud-based computation offloading for smart cities applications. *IEEE Internet Things J.* **2019**, *6*, 4251–4535.
32. Floridi, L. The flight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philos. Technol.* **2020**, *33*, 369–378. https://doi.org/10.1007/s13347-020-00423-6.
33. Calzada, I. Chapter 6—DEVOLVING smart city citizenship: Smart city-regions, data devolution, and technological sovereignty, Editor: Igor Calzada. In *Smart City Citizenship*; Elsevier Science Publishing Co Inc.: Cambridge, MA, USA, 2021; pp. 219–234. ISBN 9780128153000. https://doi.org/10.1016/B978-0-12-815300-0.00005-8.
34. Couture, S.; Toupin, S. What does the notion of 'sovereignty' mean when referring to the digital? *New Media Soc.* **2019**, *21*, 2305–2322.
35. Digital Cooperative Research. You're Data. You're Control. You're Profit. Available online: https://medium.com/digital-cooperative-research/youre-data-you-re-control-you-re-profit-5a181948011 (accessed on 8 August 2021).
36. Loukissas, Y.A. *All Data Are Local: Thinking Critically in a Data-Driven Society*; MIT Press: Cambridge, MA, USA, 2019.
37. Yanqing, H. *"Game of Laws": Cross-Border Data Access for Law Enforcement Purposes: Models in the United States, Europe, and China*; Beijing Institute of Technology School of Law: Yale, MI, USA, 2022; pp. 1–16.
38. Calzada, I. Replicating smart cities: The city-to-city learning programme in the Replicate EC-H2020-SCC project. *Smart Cities* **2020**, *3*, 978–1003. https://doi.org/10.3390/smartcities3030049.
39. Calzada, I. Democratising smart cities? Penta helix multistakeholder social innovation framework. *Smart Cities* **2020**, *3*, 1145–1172. https://doi.org/10.3390/smartcities3040057.
40. Lytras, M.; Visvizi, A.; Kwok, T.C. (Eds.) 'Big data research for social sciences and social impact' Special Issue. *Sustainability* **2020**, *12*, 180.
41. Barns, Sarah. Re-engineering the city: Platform ecosystems and the capture of urban big data. *Front. Sustain. Cities* **2020**, *2*, 32. https://doi.org/10.3389/frcs.2020.00032.
42. OECD. *Data in the Digital Age*; OECD: Paris, France, 2019.
43. United Nations. *Report of the Secretary General: Roadmap for Digital Cooperation*; UN: Nairobi, Kenya, 2020.
44. Masso, A.; Kasapoglu, T.; Tammpuu, P.; Calzada, I. Constructing digital deep borders through datafied selection: Estonian E-residency as 'Citizenship by Connection' [Forthcoming]. *Gov. Inf. Q.* **2022**.
45. Blume, P. Data protection and privacy—Basic concepts in a changing world. *Scand. Stud. Law* **2010**, *56*, 151–164.
46. What is Data Privacy? Available online: https://www.snia.org/education/what-is-data-privacy (accessed on 30 September 2021).
47. Westin, A.F. Privacy and freedom. *Wash. Lee Law Rev.* **1968**, *25*, 166–170.
48. Pötzsch, S. Privacy awareness: A means to solve the privacy paradox? *Future Identity Inf. Soc.* **2009**, 226–236. https://doi.org/10.1007/978-3-642-03315-5_17.
49. Yao-Huai, L. Privacy and data privacy issues in contemporary China. *Ethics Inf. Technol.* **2005**, *7*, 7–15. https://doi.org/10.1007/s10676-005-0456-y.
50. Data Privacy Guide: Definitions, Explanations and Legislation. Available online: https://www.varonis.com/blog/data-privacy/ (accessed on 30 September 2021).
51. Seubert, S.; Becker, C. The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Provacy Protection. *Ger. Law J.* **2021**, *22*, 31–44. https://doi.org/10.1017/glj.2020.101.
52. Changkun, S. How Chinese Social Entrepreneurs Stepped Up to Respond to COVID-19. Available online: https://skoll.org/2020/05/04/how-chinese-social-entrepreneurs-stepped-up-to-respond-to-covid-19/ (accessed on 12 October 2021).
53. Almirall, E. Què Está Passant a La Xina Amb Les Technològiques? Available online: https://www.elnacional.cat/ca/opinio/esteve-almirall-passant-xina-tecnologiques_639014_102.html (accessed on 12 October 2021).
54. Ioannou, A.; Tussyadiah, I. Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. *Technol. Soc.* **2021**, *67*, 101774. https://doi.org/10.1016/j.techsoc.2021.101774.
55. Wang, R. Personal Information Protection Law: Five Significant Meanings. Available online: https://mp.weixin.qq.com/s?__biz=MjM5OTE0ODA2MQ==&mid=2650943534&idx=1&sn=960bcb4bdea2b355454128fde19c0ee7&chksm=bcc97f5c8bbef64ac4779c10c78938afa5e3d3e20090496d87033363fe357764232e92e04079&mpshare=1&scene=24&srcid=0821TamppJEwbhUQbCoKBxze&sharer_sharetime=1629511080107&sharer_shareid=1a4fd694135664b5058f5b88f41fc22b&exportkey=A5Fy9gBaqnCjUazer8OY8VI%3D&pass_ticket=mek7pUcvKTWxlt60yhtlaAVThiMlup-GJF0vSBo1lUWxnUlkzS%2FdvD8jyZRV0%2F8W3&wx_header=0#rd (accessed on 7 October 2021).
56. Cobb, S. Data privacy and data protection: US law and legislation. ESET White Paper 2016, 1–15. Available online: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjn3vC63IP6AhUzmYQIH-RFuDT4QFnoECBkQAQ&url=https%3A%2F%2Fwww.welivesecurity.com%2Fwp-content%2Fuploads%2F2018%2F01%2FUS-data-privacy-legislation-white-paper.pdf&usg=AOvVaw1lYtt_VABfuVYTTWIuQpXy (accessed on 12 October 2021)

57. History of Privacy Timeline. Available online: https://safecomputing.umich.edu/privacy/history-of-privacy-timeline (accessed on 30 September 2021).
58. European Data Protection Board (EDPB-EDPS). *Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance Act*; EDPB: Brussels, Belgium, 2021.
59. European Commission. *A European Strategy for Data*; European Commission: Brussels, Belgium, 2020.
60. European Commission. Proposal Regulation: European Data Governance Act. Available online: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-data-governance-data-governance-act (accessed on 8 August 2021).
61. Craglia, M.; Scholten, H.; Micheli, M.; Hradec, J.; Calzada, I.; Luitjens, S.; Ponti, M.; Boter, J. *Digitranscope: The Governance of Digitally-Transformed Society*; EUR 30590 EN.; Publications Office of the European Union: Luxembourg, 2021; ISBN 978-92-76-30229-2. https://doi.org/10.2760/503546, JRC 123362. Available online: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digitranscope-governance-digitally-transformed-society (accessed on 1 September 2022).
62. Kigsing, M. *The Political Economy of Digital Ecosystems: Scenario Planning for Alternative Futures*; Routledge: Oxford, UK, 2022.
63. Calzada, I. The techno-politics of data and smart devolution in city-regions: Comparing Glasgow, Bristol, Barcelona, and Bilbao. *Systems* **2017**, *5*, 18. https://doi.org/10.3390/systems5010018.
64. Peng, Z.; Xu, C.; Wang, H.; Huang, J.; Xu, J.; Chu, X. P2B-Trace: Privacy-preserving blockchain-based contact tracing to combat pandemics. In Proceedings of the SIGMOD '21: 2021 International Conference on Management of Data, Virtual Event, China, 20–25 June 2021; Association for Computing Machinery: New York, NY, USA, 2022; pp. 2389–2393.
65. Monsees, L. *Crypto-Politics: Encryption and Democratic Practices in the Digital Era*; Routledge: Oxford, UK, 2019.
66. Nabben, K. A Political History of DAOs. Available online: https://www.fwb.help/wip/cypherpunks-to-social-daos (accessed on 1 September 2022).
67. Chen, D.; Zhao, H. Data Security and Privacy Protection Issues in Cloud Computing. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; pp. 647–651. https://doi.org/10.1109/ICCSEE.2012.193.
68. Peng, Z.; Xu, J.; Hu, H.; Chen, L. BlockShare: A Blockchain empowered system for privacy-preserving verifiable data sharing. *Bull. IEEE Comput. Soc. Tech. Comm. Data Eng.* **2022**, 14–24. http://sites.computer.org/debull/A22june/p14.pdf
69. Tavani, H.T.; Moor, J.H. Privacy protection, control of information, and privacy-enhancing technologies. *SIGCAS Comput. Soc.* **2001**, *31*, 6–11. https://doi.org/10.1145/572277.572278.
70. Gao, S.; Peng, Z.; Tan, F.; Zheng, Y.; Xiao, B. SymmeProof: Compact zero-knowledge argument for blockchain confidential transactions. *IEEE Trans. Dependable Secur. Comput.* **2022**, 1–14. https://doi.org/10.1109/TDSC.2022.3179913.
71. Wang, D.; Zhao, J.; Yingjie, W. A survey on privacy protection of Blockchain: The technology and application. *IEEE Access* **2020**, *8*, 108766–108781. https://doi.org/10.1109/ACCESS.2020.2994294.
72. Peng, Z.; Huang, J.; Wang, H.; Wang, S.; Chu, X.; Zhang, X.; Chen, L.; Huang, X.; Fu, X.; Guo, Y.; et al. BU-Trace: A permissionless mobile system for privacy-preserving intelligent contact tracing. Database Systems for Advanced Applications. In *Proceedings of the DASFAA 2021 International Workshops: BDQM, GDMA, MLDLDSA, MobiSocial, and MUST, Taipei, Taiwan, 11–14 April 2021*; Springer: Taipei, Taiwan, 2021; pp. 381–397. https://doi.org/10.1007/978-3-030-73216-5_26.
73. Stanford DAO Workshop 2022. Frances C. Arrillaga Alumni Center at Stanford University. DAO Research Collective, Megagov, Smart Contract Research Forum, and Stanford Center for Blockchain Research. Available online: https://docs.google.com/document/d/1x4I_2JpYGVM3F_B7itGYLCIzkFYxCqPR-tTtpfhU9Gg/edit#heading=h.e49ioc2rm0zd (accessed on 1 January 2020).
74. Rennie, E.; Zargham, M.; Tan, J.; Miller, L.; Abbott, J.; Nabben, K.; De Filippi, P. Towards a participatory digital ethnography of blockchain governance. *Qual. Inq.* **2022**, *28*, 837–847. https://doi.org/10.1177/10778004221097056.
75. The Personal Information Protection Law in China: A Legal Analysis. Available online: https://www.china-briefing.com/news/the-personal-information-protection-law-in-china-a-legal-analysis/ (accessed on 30 September 2021).
76. Creemers, R.; Webster, G. Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021). Available online: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021 (accessed on 7 October 2021).
77. PIPL (Personal Information Protection Law). Available online: https://m.thepaper.cn/baijiahao_14154156 (accessed on 7 October 2021).
78. Calzada, I.; Cowie, P. Beyond smart and data-driven city-region? Rethinking stakeholder-helixes strategies. *Reg. Mag.* **2017**, *308*, 25–28. https://doi.org/10.1080/13673882.2017.11958675.
79. Cooper, Z.G.T. Of dog kennels, magnets, and hard drives: Dealing with Big data peripheries. *Big Data Soc.* **2021**, *8*, 20539517211015430. https://doi.org/10.1177/20539517211015430.
80. Van Dijck, J. Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveill. Soc.* **2014**, *12*, 197–208. https://doi.org/10.24908/ss.v12i2.4778.
81. Van Dijck, J.; Hacker, K. The digital divide as a complex and dynamic phenomenon. *Inf. Soc.* **2003**, *19*, 315–326. https://doi.org/10.1080/01972240309487.
82. Sadowski, J. When data is capital: Datafication, accumulation, and extraction. *Big Data Soc.* **2019**, *6*, 1–12. https://doi.org/10.1177/2053951718820549.
83. Ada Lovelace Institute. *Exploring Legal Mechanisms for Data Stewardship*; Ada Lovelace Institute: London, UK, 2021.
84. Liu, J.; Zhao, H. Privacy lost: Appropriating surveillance technology in China's fight against COVID-19. *Bus. Horiz.* **2021**, *64*, 743–756. https://doi.org/10.1016/j.bushor.2021.07.004.

85. Calzada, I. Chapter 7—PROTECTING smart city citizenship: Citizens' digital rights and AI-driven algorithmic disruption. In *Smart City Citizenship*; Calzada, I., Ed.; Elsevier Science Publishing Co Inc.: Cambridge, MA, USA, 2021, pp. 219–234. ISBN 9780128153000. https://doi.org/10.1016/B978-0-12-815300-0.00007-1.
86. Kitchin, R. Civil liberties or public health, or public liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. *Space Polity* **2020**, *24*, 362–381. https://doi.org/10.1080/13562576.2020.1770587.
87. Li, H.; Wang, S. The role of cognitive distortion in online game addiction among Chinese adolescents. *Child. Youth Serv. Rev.* **2013**, *35*, 1468–1475. https://doi.org/10.1016/j.childyouth.2013.05.021.
88. Micheli, M.; Ponti, M.; Craglia, M.; Suman, A.B. Emerging models of data governance in the age of datafication. *Big Data Soc.* **2020**, *7*, 1–15. https://doi.org/10.1177/2053951720948087.
89. Caragliu, A.; Del Bo, C.F. Smart cities and urban inequality. *Reg. Stud.* **2021**, *56*, 1097–1112. https://doi.org/10.1080/00343404.2021.1984421.
90. Calzada, I.; Cobo, C. Unplugging: Deconstructing the Smart City. *J. Urban Technol.* **2015**, *22*, 23–43. https://doi.org/10.1080/10630732.2014.971535.
91. Ernst & Young. The California Consumer Privacy Act: Overview and Comparison to the EU GDPR. Available online: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-the-california-consumer-privacy-act.pdf (accessed on 7 October 2021).
92. Chin, Y.-C.; Zhao, J. Governing cross-border data flows: International trade agreements and their limits. *Laws* **2022**, *11*, 63. https://doi.org/10.3390/laws11040063.
93. Voss, W.G. Cross-Border Data Flows, the GDPR, and Data Goverrance. *Wash. Int. Law J.* **2020**, *29*, 485–532.
94. Data Localization—Advantages & Challenges. Available online: https://tidesacademy.com/data-localization-advantages-challenges/ (accessed on 7 October 2021).
95. Luca, B. EU Countries Green Light New Data Governance Framework. Available online: https://www.euractiv.com/section/data-protection/news/eu-counties-green-light-new-data-governance-framework/ (accessed on 12 October 2021).
96. Cheng, H.; Lai, Y.; De, T. Decoding the decision-making in the new wave of urban redevelopment in China: A case study of a bottom-up industrial land redevelopment in Shenzhen. *Land Use Policy* **2021**, *111*, 105774. https://doi.org/10.1016/j.landusepol.2021.105774.
97. Shenzhen Special Zone News. The total GDP of Shenzhen in 2020: 2.77 trillion yuan. Available online: http://www.sz.gov.cn/szzt2010/yqfk2020/szzxd/content/post_8534669.html (accessed on 12 October 2021).
98. Greater Bay Area. Outline Development Plan for the Guangdong-Hong Kong-Macao Greater Bay Area. 2019. Available online: https://www.bayarea.gov.hk/filemanager/en/share/pdf/Outline_Development_Plan.pdf (accessed on 5 September 2022).
99. Will, K. Shenzhen SEZ, China. Available online: https://www.investopedia.com/terms/s/shenzhen-sez-china.asp (accessed on 12 October 2021).
100. Tencent. Available online: https://www.tencent.com/en-us/ (accessed on 12 October 2021).
101. Huawei. Available online: https://www.huawei.com/en/ (accessed on 12 October 2021).
102. DJI. Available online: https://www.dji.com/cn (accessed on 12 October 2021).
103. OnePlus. Available online: https://www.oneplus.com/cn (accessed on 12 October 2021).
104. SF Express. Available online: https://www.sf-express.com/cn/en/ (accessed on 12 October 2021).
105. BBC. Amazon Hit with $886m Fine for Alleged Data Law Breach. Available online: https://www.bbc.com/news/business-58024116 (accessed on 12 October 2021).
106. Sohu. China Has Initiated a Cybersecurity Review on the Direct Employment of DIDI, BOSS. Available online: https://www.sohu.com/a/494313644_114778 (accessed on 12 October 2021).
107. Sina. Ministry of Industry and Information Technology Rectifies Internet Privacy Issues. Available online: https://t.cj.sina.com.cn/articles/view/6327900155/1792c17fb00101489b (accessed on 12 October 2021).
108. Shenzhen Evening News. Shenzhen's enterprises keep data security for users. Available online: https://k.sina.com.cn/article_1913382117_720be4e501901909p.html (accessed on 12 October 2021).
109. The Paper. Liang Zhenying: Cross-Border Circulation of Data has Become a New Subject of Urban Integration in the Greater Bay Area. Available online: https://finance.sina.com.cn/tech/2021-09-26/doc-iktzqtyt8253796.shtml (accessed on 12 October 2021).
110. Shenzhen Municipal Service Data Administration. Shenzhen Special Economic Zone Data Regulations officially announced. Available online: www.sz.gov.cn/szzsj/gkmlpt/content/8/8935/post_8935483.html#19236 (accessed on 12 October 2021).
111. Shenzhen Municipal Government Data Open Platform. Available online: Opendata.sz.gov.cn (accessed on 12 October 2021).
112. Glibal Open Data Application Innovation Competition. Available online: https://www.sodic.com.cn/ (accessed on 12 October 2021).
113. Shenzhen Special Zone News. Shenzhen Implements "Red, Yellow And green" Color Separated Electronic Health Code. Available online: http://www.sz.gov.cn/cn/xxgk/zfxxgj/zwdt/content/post_6991757.html (accessed on 12 October 2021).
114. GroBe-Bley, J.; Kostka, G. Big Data dreams and reality in Shenzhen: An investigation of smart city implementation in China. *Big Data Soc.* **2021**, *8*, 20539517211045171. https://doi.org/10.1177/20539517211045171.
115. Shenzhen University. Available online: https://en.szu.edu.cn/ (accessed on 12 October 2021).
116. The Chinese University of Hong Kong, Shenzhen. Available online: https://www.cuhk.edu.cn/en (accessed on 12 October 2021).

117. Southern University of Science and Technology. Available online: https://www.sustech.edu.cn/en/ (accessed on 12 October 2021).
118. Jiang, K. Shenzhen University: Data security protection starts from data classification. *China Educ. Netw.* **2021**, *Z1*, 73–75.
119. Cotter, K.; Medeiros, M.; Pak, C.; Thorson, K. "Reach the right people": The politics of "interests" in Facebook's classification system for ad targeting. *Big Data Soc.* **2021**, *8*, 2053951721996046. https://doi.org/10.1177/2053951721996046.
120. Larry, Y. The emergence of social entrepreneurs in China. *J. Int. Counc. Small Bus.* **2020**, *1*, 32–35. https://doi.org/10.1080/26437015.2020.1714359.
121. South China Morning Post. Wider Lockdowns in Shenzhen Trigger Exodus of Travellers as China's Tech Hub Comes to a Standstill. Available online: https://www.scmp.com/tech/policy/article/3191031/wider-lockdowns-shenzhen-trigger-exodus-travellers-chinas-tech-hub (accessed on 2 September 2022).