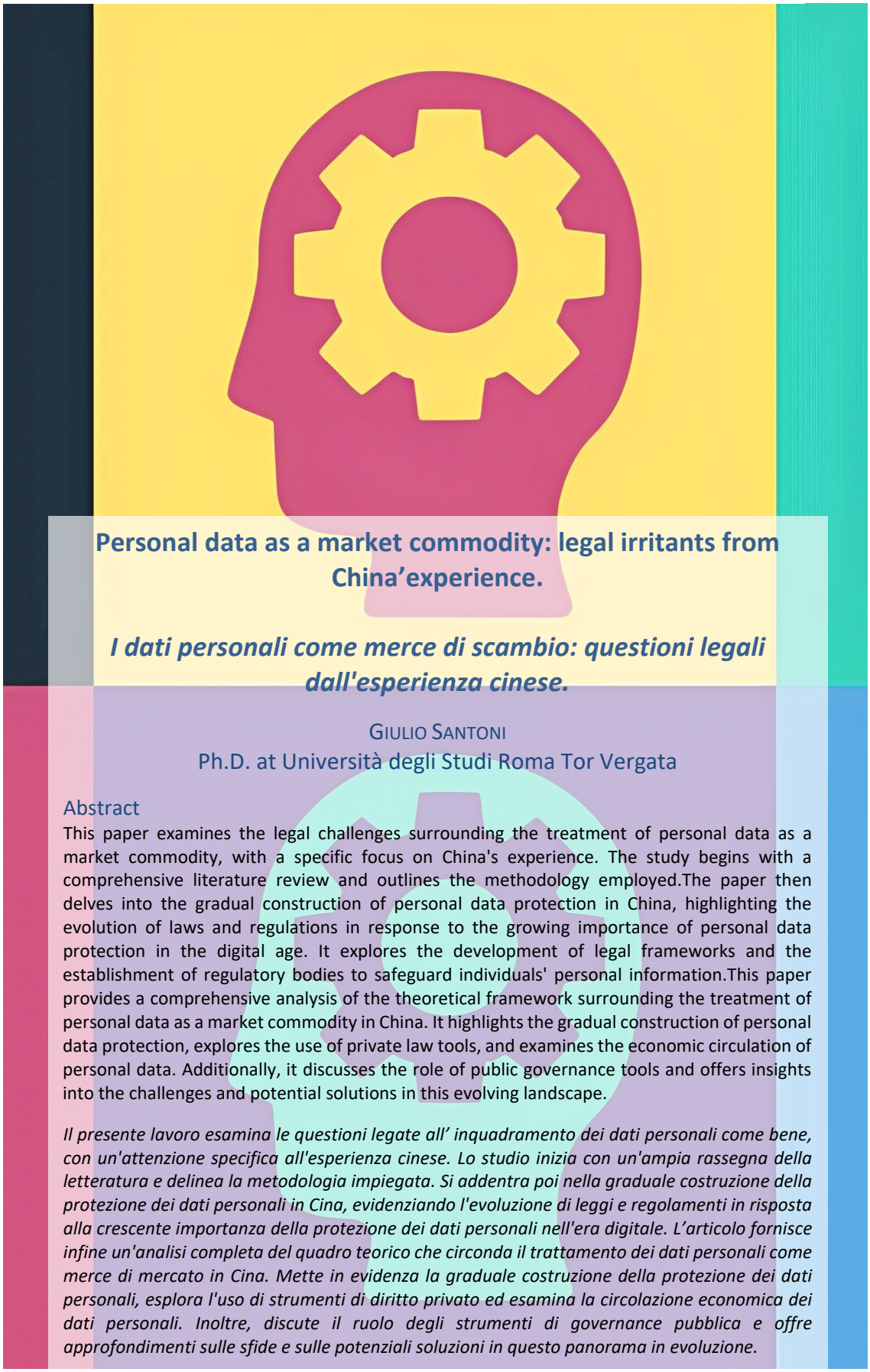
Santoni G, 'Personal data as a market commodity: legal irritants from China'experience' (2023) 1 EJPLT, 128-146.
DOI : https://doi.org/10.57230/EJPLT231GS

EJPLT
ISSN 2704-8012



Personal data as a market commodity: legal irritants from China'experience.

I dati personali come merce di scambio: questioni legali dall'esperienza cinese.

GIULIO SANTONI
Ph.D. at Università degli Studi Roma Tor Vergata

Abstract

This paper examines the legal challenges surrounding the treatment of personal data as a market commodity, with a specific focus on China's experience. The study begins with a comprehensive literature review and outlines the methodology employed.The paper then delves into the gradual construction of personal data protection in China, highlighting the evolution of laws and regulations in response to the growing importance of personal data protection in the digital age. It explores the development of legal frameworks and the establishment of regulatory bodies to safeguard individuals' personal information.This paper provides a comprehensive analysis of the theoretical framework surrounding the treatment of personal data as a market commodity in China. It highlights the gradual construction of personal data protection, explores the use of private law tools, and examines the economic circulation of personal data. Additionally, it discusses the role of public governance tools and offers insights into the challenges and potential solutions in this evolving landscape.

Il presente lavoro esamina le questioni legate all' inquadramento dei dati personali come bene, con un'attenzione specifica all'esperienza cinese. Lo studio inizia con un'ampia rassegna della letteratura e delinea la metodologia impiegata. Si addentra poi nella graduale costruzione della protezione dei dati personali in Cina, evidenziando l'evoluzione di leggi e regolamenti in risposta alla crescente importanza della protezione dei dati personali nell'era digitale. L'articolo fornisce infine un'analisi completa del quadro teorico che circonda il trattamento dei dati personali come merce di mercato in Cina. Mette in evidenza la graduale costruzione della protezione dei dati personali, esplora l'uso di strumenti di diritto privato ed esamina la circolazione economica dei dati personali. Inoltre, discute il ruolo degli strumenti di governance pubblica e offre approfondimenti sulle sfide e sulle potenziali soluzioni in questo panorama in evoluzione.

© The author(s) 2023, published by Suor Orsola Benincasa Università Editrice. This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: China; data protection; personal data; PIPL.

Summary: Introduction: Literature review and methodology. – 1. The gradual construction of personal data protection in China. – 2. Personal data protection through private law tools. – 3. Economic circulation of personal data circulation. – 4. Public governance tools for the protection of personal data and the data market. – Conclusions.

Introduction: Literature review and methodology.

The Chinese legal thinking has long been considered indifferent or at least less attentive to the protection of privacy, if compared to the Western one [1]. The promulgation of the Personal Information Protection Law (PIPL)[2], roughly comparable to the European GDPR, challenged this assumption[3]. The first Western reviews on the PIPL juxtaposed it with the GDPR, noting similarities and differences[4]. Others, while more attentive to the peculiarities of the Chinese legal system, and warning from an excessive methodological reliance on the similarity between the GDPR and the PIPL, did

[1] See. L Wang, B Xiong, 'Personality rights in China's New Civil Code: A Response to Increasing Awareness of Rights in an Era of Evolving Technology' (2021) 46, Mod. Chin., who argue that the concept of privacy, which was unknown in rural China, where "each peasant knew the number of eggs laid by his neighbor", found continuity in the legal system of socialist China. On the unfamiliarity of the concept of privacy in the Chinese legal system, see also G Zhu, 'The Right to Privacy: An Emerging Right in Chinese Law' (1997) 18, Stat. L. Rev, p. 208, noting that "shameful secrets" and "privacy" are homophonic words in Mandarin, both being spelled "*yinsi*". See also E Pernot-Leplay, 'China's Approach on Privacy Law: A third way between the U.S. Law and the EU?' (2020) 8, Penn S. J. of Law & Int. Aff., p. 66, who notes how, in fact, China's alleged cultural indifference to privacy is downsized by the fact that other jurisdictions rooted in traditional Chinese values, such as Hong Kong and Taiwan, actually offer more advanced forms of privacy protections and disciplines for personal data than most OECD countries. Some, as T Shtub, M Gal, 'The competitive effects of China's legal data regime', (2022) 18 [4] J. of Comp. and Econ., p. 3, contextualize the assumption of Chinas cultural indifference towards privacy protection, as they state that the Chinese legal culture is not indifferent to privacy per se, but that it does not fully conceive a right to privacy towards the State.

[2] The PIPL is denominated "个人信息保护法" in Chinese.

[3] Many sources translate 个人信息 (*geren xinxi*) as "personal information" in English translations and "personal information" in Italian. The term "information" is closer to the literal meaning of the Chinese expression, consisting of the words *geren* (personal) and *xinxi* (information). See, for example, Stanford University's DigiChina observatory https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, which is perhaps the most authoritative source of English translations of Chinese laws in topics related to the digital economy. The usage of the expression "personal information" however, is since the expression personal information, in the reference legislative text, which is the RGPD, is used in an a-technical sense, only in recital 6. Information "concerning an identified or identifiable natural person" is defined by Article 4 of the RGPD as "personal data" and not "personal information." As will be discussed more fully below, the *geren xinxi* referred to by the Chinese legislature was first defined by the 2018 Network Security Law and later more precisely by in the 2021 Personal Data Protection Law as "any kind of information (...) concerning identified or identifiable natural persons." The translation of *geren xinxi* as "personal data" therefore has the added merit of emphasizing the proximity to the RGPD. In the English language, the term "personal information" has sometimes been used to refer to personal data in North American legislations, such as in §312 of the Code of Federal Regulations, on the protection of minors' personal data online, and the Canadian Privacy Acy, which define "*personal information*" as "*individually identifiable information about an individual collected online.*" Since the definition of *geren xinxi*, is borrowed from the RGPD, the use of the expression personal data would also be preferable in English translations, to emphasize this difference. In any case, in English, the use of "*personal information*," which has been established as the official translation of *geren xinxi,* is not incorrect.

[4] See E Pernot-Leplay, 'China's Approach on Privacy Law', (n 1), p. 51, C Moriconi, 'Recent Evolution of the Personal Privacy Legal Protection in People's Republic of China' (2019) 9, NNJLSR, p. 248.

not deflect from the focus on the dichotomy between the two regulations[5]. Clementi, while centering his analysis on the comparison between the PIPL and the GDPR, also includes Civil Code provisions into the picture drawing a dual system[6]. He identifies two parallel sets of mechanisms for the protection of personal data and other personality rights. This allows to contextualize personal data protection, within a broader array of private law tools, while also enabling to interpret the Chinese legislator's stance on the issue of the abstract issue of whether personal data protection is a personality right. The author also sheds some light on a peculiar characteristic of the Chinese legal system that is the role of a supervisory body, the Cyberspace Administration of China. This has both regulatory and control prerogatives, which are unparalleled in the European legal system.

The tendency to overlap the GDPR and the PIPL was conclusively criticized by Creemers[7]. Indeed, the PIPL is only a brick in the complex structure of Chinese data regulations. Important provisions on personal data are included in the 2018 Cyber security Law (CSL)[8], the 2021 Data Security Law (DSL)[9], and the Civil Code, also entered in force in 2021. More importantly, the CSL and the DSL, while mentioning personal data, shift the main focus on other categories of data. The purposes of these laws are, respectively, the strategic security of China's Internet infrastructure and the promotion of a sustainable development of the data economy. As such, they deeply impact data handling activities, including those that rely on personal information.

Finally, some studies focus on the functional role of data regulations in China. Shtub and Gal make an argument for the competitiveness of China's data regulation, as it favors aggregation[10]. Chinese scholarship on the issue of data regulation is vast. Due to the difficulty in both translating material in Mandarin and also in retrieving Chinese legal documents from Europe, the reliance on Chinese sources must be limited. This study therefore focuses on such sources, understand three peculiar aspects of the Chinese market regime of data. These are the contextualization of personal data transaction within the framework for the protection of personality rights, the legal qualification of the aggregation of personal data and the unique role of the CAC. Particular emphasis is given to the scholarly debate on the systematization of personal data protection within Part IV of the Civil Code.

The purpose of this analysis is to contribute to the European debate, where the commodification of data is implied, even if data cannot be treated as any subject's

[5] See R Burkart and J Recha, 'Das neue chinesische Datenschutzrecht und die europäische DSGVO' (2022) 1, ZChinR, p. 19, while offering a comprehensive comparison between the German system, centered on the European RGPD, and the Chinese PIPL, argue that China does not possess a truly unified system of personal data protection laws. Even after the Personal Data Protection Law came into effect, China's system of laws continues to be fragmented. Cf A Geller, 'How comprehensive is Chinese Data Protection Law? A Sytematisation of Chinese Data Protection Law from a European Perspective' (2020) 69 [12] GRUR Inter., p. 1191, whose analysis predates the issuance of the PIPL and is therefore centered on the Civil Code, the Cybersecurity law and the Draft of the PIPL.

[6] See D Clementi, 'La legge cinese sulla protezione delle informazioni personali: un GDPR con caratteristiche cinesi?' (2022) 1, Rivista di diritti comparati, p. 194.

[7] See R Creemers, 'China's Emerging Data Protection Framework' (2022) 8 [1] J. of Cybersec., p. 1.

[8] The CSL is denominated "网络安全法" in Chinese.

[9] The DSL is denominated "数据安全法" in Chinese.

[10] See T Shtub, M Gal, 'The competitive effects of China's legal data regime', (n 1), p. 7.

property[11]. Article 1 of the GDPR states that the regulation couples the need to protect natural persons with the need to enable the free movement of personal data. Free movement of data within the Union, similar to other commodities, cannot be restricted or prohibited for reasons connected with the protection of personal data. At the same time, the legal nature of data movement is not agreed upon.

This essay does not aim to mirror the juxtaposition between the PIPL and the GDPR, by claiming that the European legal system can transplant Chinese categories into its own[12]. However, it is grounded on the idea that the same way European civil law has long represented a legal irritant in the Chinese experience, European scholars may benefit from being exposed to data regulation in China, even though the Chinese institutes may not be directly transplanted in the European legal system. While doing so, the essay also aims to offer a deeper understanding of the market of information and digital services in China, whose characterization as a mere tool to "crackdown" on enterprises challenging the absolute power of the Chinese Communist Party (CCP) has already been effectively contested[13], but it regrettably keeps captivating Western observers.

A last methodological note is that this essay does not take into account policy documents. In this sense, the Author disassociates from all other major contributions by Western scholars. Chinese policy documents have been consistently quoted, either in order to provide a comprehensive understanding of Chinese law or to empirically fill in the many gaps that Chinese regulations on the ever-evolving platform economy inevitably leave open. A number of reasons suggests however to reject this choice. Firstly, unlike laws, the hierarchy of policy documents and programmatic declarations is unclear and its understanding would go beyond the purposes of this article. Secondly, the final purpose of this article is to provide insights to European lawyers, through the tools of comparative law. While Chinese policy documents can often provide insights in how to interpret the law, they usually have a generic and programmatic tone and do not explicitly refer to legal remedies and tools. Third, also Chinese laws are often described as, and criticized for, their generic and programmatic provisions. Indeed, most Chinese policy strategies can be tracked down in the laws, especially in the CSL and the DSL, which are characterized by a large number of programmatic provisions[14]. Finally, and perhaps most importantly, come terminological issues. The pillar on which comparative law relies is legal terminology. Difficulties in legal translation are not to be understated, starting from the very concept of personal data/ personal information (个人信息), in Chinese law. However, referring to policy documents would open new issues, related to

[11] See V Ricciuto, *L'equivoco della privacy, persona vs. dato personale*, ESI, 2022, p. 62.

[12] For the perils of legal transplants see A Watson, *Legal Transplants: An Approach to Comparative Literature* (2nd edition), The University of Georgia Press, 1997, p. 21.

[13] For a broad perspective on the efficiency of the Chinese data market, refer to T Shtub, M Gal, 'The competitive effects of China's legal data regime', (n 1), pp. 7 - 9. R. Creemers et al., 'Is China's Tech 'Crackdown' or 'Rectification' Over?', (2023), Digichina, available at: https://digichina.stanford.edu/work/is-chinas-tech-crackdown-or-rectification-over/, (last access on 16 June, 2023), openly contests the usage of the expression crackdown to describe China's approach to the platform economy, noting that: "Rather, regulators see the sector as so important that the excesses that had built up around it could no longer be tolerated".

[14] See R Creemers, 'China's Emerging Data Protection Framework' (n 7), pp. 9, who notices how all Chinese laws (PIPL, DSL and CSL) are indeed vague and required integration through implementing provisions released by the CAC.

the usage of concepts that can have radically different political implications in the two systems, such as cyber sovereignty[15].

1. The gradual construction of personal data protection in China.

The constitutional protection of the individual right to privacy in China is weak[16]. Article 38 of the 1982 Constitution enshrines the right to personal dignity of citizens of the People's Republic of China, which translates, in essence, into the protection of reputation[17]. Articles 39 and 40 of the Constitution, on the other hand, provide for the inviolability of home and correspondence, respectively[18]. These constitutional principles have long remained unimplemented and deprived of effective protections. From 1982 to 2010, the protection of personality rights was limited to the few provisions contained in the 1986 General Principles of Civil Law. Here, included in the list of personal rights were the right to a name (Art. 99), the right to image (Art. 100), the right to reputation (Art. 101), as well as the right to honor (102)[19].

With reference to continental European legal systems, scholarship noted a shift in the objective of the protection of privacy rights. In the 1960s-70s, it was aimed at tempering the risk of surveillance by public authorities. Subsequently, after the commercialization of digital technologies enabled a data economy, it focused on the problem of the circulation of personal data in a free market of information[20]. In China, where subjective rights suffer from a serious deficit of protection when the infringer is an agent of the public authority, a discipline to protect personal data was formed only after the establishment of an information market raised issues related to the usage of

[15] For a thorough comparison of AI policies in China and the USA, refer to E Hine, L Floridi, 'Artificial Intelligence with American Values and Chinese Characteristics: A Comparative Analysis of American and Chinese Governmental AI Policies', [2022] AI & Soc., pp. 2 - 5.

[16] See R Cavalieri, *Il diritto nella Cina socialista e postsocialista,* in M Scarpari (ed.), *La Cina*, vol. III, Einaudi, 2009, p. 465, which points out that Chinese citizens are guaranteed, in addition to equality and dignity, a number of political rights (voting, freedom of expression, press, assembly, association), personal rights (inviolability of the person and his dignity, domicile and correspondence), social and economic rights (work, religious freedom, retirement, education and material assistance). It should be added, however, that the practical scope of the listed rights is significantly compressed both by the fact that their free exercise is subordinated by Article 51 of the Constitution to state interest and by the fact that their regulation is generic and often lacking tools for implementation.

[17] Article 38 of the Constitution of the People's Republic of China: The personal dignity of citizens of the People's Republic of China is inviolable. Insult, defamation, false accusation or false incrimination against citizens by any means is prohibited.

[18] Article 39 of the Constitution of the People's Republic of China: The residence of citizens of the People's Republic of China is inviolable. Illegal search or intrusion into the residence of citizens is prohibited.
Article 40 of the Constitution of the People's Republic of China: The freedom and secrecy of correspondence of citizens of the People's Republic of China, shall be protected by law. No organization or individual may, for any reason whatsoever, infringe upon the freedom of citizens and the secrecy of correspondence, except in cases where, in order to meet the needs of state security or criminal investigation, public security organs and public prosecutors' offices are permitted to censor correspondence, subject to procedures prescribed by law.

[19] The 1986 General Principles contained only general provisions on torts, which was only comprehensively regulated in 2010 through the Law on Torts. In 2021, it was replaced by the relevant rules of the Civil Code, Book VII of which is devoted to torts.

[20] See V Ricciuto, *Circolazione e scambio di dati personali*, in V Ricciuto, C Solinas (ed.) *Forniture di servizi digitali e pagamento con la prestazione dei dati personali*, Milan, 2022, p. 8 -12.

personal data for commercial purposes[21].

Chinese scholars divide the path regulation of digital platforms in China into two phases, characterized by different macroscopic trends. The first runs from 1994 to 2012 and the second from 2012 to the present[22]. According to this historical reconstruction, *online* content regulation activity initially focused on censoring politically controversial material. This would have led to the exclusion of most foreign enterprises, thus resulting in a form of protectionism that allowed Chinese network operators to thrive in an outwardly closed but internally highly deregulated market internally. Against this backdrop of encouraging the creation of a domestic digital industry, personal data was not specifically regulated until 2012.

While the second phase was characterized by a greater reliance on legislation, in the years prior to 2012, network regulation was often contained in directives, decisions, decrees, administrative measures, and even "opinions" and "circulars". Moreover, these referred to a large number of ministries, formally coordinated by the Ministry of Industry and Information Technology (MIIT), but in reality reporting to conflicting interests of different branches of the state[23].

The evolution of Chinese legislation on personal data protection is complex, but it allows for better understanding the choices made by the legislature[24]. Besides being

[21] On the deficit of protection of individual rights vis-à-vis public authority in China, see F Spagnoli, 'The revision of the Chinese Constitution: an analysis of the 2018 constitutional amendment and its major features', in DPCE Online, (2019) 38 [1], available at https://www.dpceonline.it/index.php/dpceonline/article/view/647, who notes how not only in China, but in all constitutions referring to Marxist-Leninist ideologies, the protection of individual rights is conceived as instrumental to the long-term objectives of the system. The realization of social rights is preferred over liberal political and civil rights (seen as necessarily influenced by the underlying economic power relations (pp. 132). Nonetheless, it would be unfair to dismiss such protections as merely formal recognition. The Chinese state, however subservient to the principle of the democratic dictatorship of the proletariat, established by the Prologue of the Constitution, recognizes the protection of individual rights as having a dual function. On the one hand, the protection of subjective rights is directed toward other private subjects, but mainly toward the territorial and peripheral articulations of the state. See also Y Su, (苏永钦) '私法自治中的国家强制 --**从功能法的角度看民事**规范的类', (State Coercion in Private Law Autonomy - A Class of Civil Norms from a Functional Law Perspective) [2001] **中外法学** (Peking University Law Journal), available at https://www.legal-theory.org/?mod=info&act=view&id=17895, in which civil law is also considered as a regulatory tool by which the central state can ensure that peripheral State bodies comply with the law. The Chinese Constitution finds its fundamental principles in the primacy of the Communist Party, the provision of political lines to guide its action, the democratic dictatorship of the people, and adherence to the socialist way. A constitution based on such principles can only repudiate the idea of separation of powers, F Spagnoli, *Ibid.* (p. 134) and thus resolves itself "(in)The lack of constitutionality review of laws by a body other than the legislature means that in China more than "constitutional justice" one can speak of "constitutional supervision".

[22] See W Miao, M Jiang. Y Pang, 'Historicizing Internet Regulation in China: A Meta-Analysis of Chinese Internet Policies', (2021) 15, Int. J. of Comm., pp. 2015-2016.

[23] See W Miao, M Jiang. Y Pang, *Ibid* pp. 2005 - 2007, who use the Chinese proverb "too many cooks in the kitchen" to describe the fragmented situation that justified the creation of the CAC, placed under the direct control of the Chinese Communist Party Politburo Standing Committee. Since than, secondary legislation has been made more rational and coherent, partly through the establishment of a centralized Internet governing body, the Cyberspace Administration China. See also W Miao, M Jiang, Policy review: the Cyberspace Administration of China, [2016] Global Media and Communication.

[24] For a more comprehensive listing of the complex system of secondary sources that preceded the post-2012 reform season, see E Pernot-Leplay, China's Approach on Privacy Law (n 4), pp. 64 ff. See also, for a detailed review of the evolution of Chinese regulations, in Italian language, E Toti, 'Dalla Decisione per il rafforzamento della protezione delle informazioni su internet alla Legge sulla tutela delle informazioni personali della RPC con caratteristiche cinesi', in Media Laws, pp. 213, ff.

consistent with the overall trend of having improved in quality after 2012[25], China's creation of a legal framework on personal data can be appreciated under two distinct perspectives. On one hand, a right to personal data protection was gradually carved out, from a set of public Internet governance tools, implemented through administrative means, which emerged from the need to ensure State governance over online activities. On the other hand, the notion that personal data protection emerged is projection of an individual right to privacy also progressively emerged. In this latter perspective, personal data protection is framed within a broader toolset of personality rights, which can be protected through online intermediary liability provisions contained in the Civil Code.

The so-called Telecommunications Regulations, No. 291/2000, adopted by the State Council in 2000, while reaffirming the objective of ensuring telecommunications and information security, did not contain any provisions on the protection of personal data[26]. This is not to say that the law was blind to the problem of the growing circulation of information about Chinese citizens in digital format. Article 6 of the Regulations prohibited the use of telecommunications to disseminate information that harmed state security, public and social interests and the legitimate rights and interests "of others"[27].

The protection mechanisms provided by the Regulations were based on public law instruments. They relied, in particular, on a licensing system, which, in the case of telecommunication service providers required 51 percent state participation[28].

The first regulations specifically dedicated to the phenomenon of data circulation were contained in the "Decision of the National People's Congress on Strengthening Information Protection," dated Dec. 28, 2012. Like the 2000 Regulations, the 2012 Decision continued to respond to the need for the affirmation of public interest objectives, which, in this case, was to realize national sovereignty over cyberspace[29]. The preamble of the Dec. 28, 2012 Decision continued to identify the primary objectives in network security, the protection of national security and social order, relegating only to the last position the legitimate rights and interests of citizens and legal persons.

Nevertheless, the decision, which straddles the two phases of network regulation identified by Chinese doctrine, had the merit of ending the legislature's apparent blindness to the phenomenon of personal data processing. The very notion of "personal data," 个人信息, appears for the first time in the 2012 Decision, in Article 2[30] . Although lacking a definition, the notion of personal data could be reconstructed from Article 1 of the 2012 Decision, which actually contained a programmatic rule: "the State shall protect electronic information that can identify the personal identity of citizens and affects their privacy." This provision revealed a conception in which the planes of the

[25] See E Toti, *Ibid* p. 214.

[26] Art. 1 of the 2000 Regulation, which is known in Chinese as 电信条例.

[27] Article 6 of Regulation No. 291/2000 used the expression "他人," literally "other persons," to identify the holders of those other rights and legitimate interests that the regulation deemed worthy of protections of an indefinite nature.

[28] Article 10(1) of Regulation No. 291 of 2000 speaks of 经营基础电信业务, an expression that can be traced back to the notion of basic telecommunication services proper to U.S. law.

[29] **全国人民代表大会常**务委员会关于加强网络信息保护的决定.

[30] The first definition of the concept of personal data was introduced into Chinese law only in 2018, with the Cybersecurity Law (see *below*).

regulation of personal data protection as a public interest and privacy protection were still confused, and which, as will be discussed, was overcome with the 2021 reforms[31].

The 2012 Decision also provided for a primitive framework for the processing of personal data: it provided for principles of "lawfulness, legitimacy, necessity, and determinacy of the purposes of the processing of personal data," but these were entirely lacking in definition. The legitimacy of processing was conditional on the consent of the individuals involved, without including this provision in a broader regulation of the legal bases of processing.

The protection of protected personal data was limited to those belonging to Chinese citizens. Some Western scholars questioned, based on this latter element, whether Chinese regulations shifted from the U.S. model of data protection, characterized by the fact that data protection is reserved for citizens and lawful residents of the United States, towards the European model, which instead guarantees the personal data of individuals as such[32].

The object of protection, personal data, was defined as information through which Chinese citizens were identified or identifiable, as well as all information involving the confidentiality of Chinese citizens (Article 1 of the 2012 decision). The mention of the right to privacy of citizens betrays a conceptual overlap of the subject of the circulation of personal data with that of privacy. It is interesting to note as of now that in the definitions of personal data in the most recent laws, which replaced the one just quoted, the reference to confidentiality has disappeared (see *below*, § 3). The document did not indicate whether there were categories of sensitive data, nor, more generally, did it address whether there were types of data deserving of reinforced protection. In terms of the protections themselves, there were also no particular obligations placed on the data controller. Article 8 of the decision allowed Chinese citizens to have their data erased, but only when the information violated their rights, or resulted in telephone harassment[33]. In conclusion, the 2012 Decision was but an intermediate step, where the extreme vagueness of the provisions was obviated by a multitude of lower-ranking sources[34].

---

[31] Previously, the Ministry of Public Security's Coordinated Regulation No. 43 of 2007, titled "Management Measures for the Protection of the Degree of Information Security," included an interesting provision in Article 23(2). It imposed certain obligations on qualified entities such as "the organizations engaged in the determination of security systems" to respect, in addition to state secrets and trade secrets, individual confidentiality.

[32] See E Pernot-Leplay, 'China's Approach on Privacy Law: A third way between the U.S. and the EU?' (n 4). p. 65.

[33] The 2012 decision contains numerous provisions aimed at preventing aggressive marketing practices through telephone calls.

[34] The extremely vague tenor of the provisions contained in the 2012 decision was partly obviated by the Ministry of Industry and Information Technology's (MIIT) Guideline, "On Telecommunications and the Protection of Personal Data of Internet Users," dated September 1, 2013 (电信和互联网用户个人信息保护规定.) The Guideline strongly incentivized the adoption of certain technical standards, which, while not mandatory, clarified numerous principles set forth in the legislative provisions reviewed thus far. Interestingly, the MIIT did not merely specify the vague provisions contained in the law, but on the contrary went so far as to introduce new institutions and categories that did not exist in the latter. In particular, it introduced a distinction between personal data and sensitive data. In terms of discipline, the approach provided by the decision has already been superseded in 2014, with the enactment of the Consumer Protection Act. This law, while limited to the aspects of data circulation related to consumer contracts, affirms in Article 14 that consumers have the right, and no longer a mere legitimate interest, that their personal data be protected, as well as providing in Article 29 a more detailed regulation of the circulation of personal information collected in the context of consumer contracts. Coeval with the Consumer Protection Act is the important

2. Personal data protection through private law tools.

The regulation of personal data is currently contained in the PIPL, which has a similar structure to the RGPD and adopts several solutions borrowed from the European regulation. However, it operates against a backdrop of other important laws, which manifest the continuing existence of multiple legislative goals. The Chinese Civil Code, which also came into effect in 2021, outlines the relationship between personal data protection and privacy protection. The CSL responds to strategic needs, such as "ensuring network security, safeguarding national sovereignty over cyberspace, national security, and social and public interests." Since it came into effect three years earlier than the other laws, it also contained some generic provisions on personal data, which, in some cases have been superseded in the 2021 PIPL[35]. The DSL, also implemented in 2021, imposes numerous technical measures on data controllers and takes into account several categories of data. The CSL and the DSL also take into account the protection of personal data, but they do so in the angle of protecting the State interest to the security of citizen's data[36]. The definition of personal data (个人信息) was first introduced in art. 76 (5) of the 2018 Cyber security law, before being restated in art. 4 of the 2021 PIPL and in the Civil Code (art. 1033)[37]. All the definitions are slightly different, but overall similar to the GDPR. Personal data is defined as data that enables the identification of a natural person[38]. Nevertheless, the remedies that the two laws offer are centered on

---

interpretation of Supreme People's Court No. 11/2014 on injuries to personality rights through the web(审理利用信息网络侵害人身权益民事纠纷案件).

[35] Please refer to E Pernot-Leplay, 'China's Approach on Privacy Law: A third way between the U.S. and the EU?' (n 4). p. 74, and T Shtub, M Gal, 'The competitive effects of China's legal data regime', (n 1), p. 13, who agree that data protection discipline contained in the 2018 Network Security Law was intended to maintain some freedom of interpretation in the early stages of reform.

[36] Article 1 of the CSL defines the purposes of the law, stating that: "This Law is formulated in order to: ensure cyber security; safeguard cyberspace sovereignty and national security, and social and public interests; protect the lawful rights and interests of citizens, legal persons, and other organizations; and promote the healthy development of the informatization of the economy and society".

[37]Article 76 (5), unlike PIPL, includes a non-exhaustive list of personal data "including name, date of birth, ID card number, personal biometric information, address, telephone number, and so on." The Supreme People's Court has recently had to clarify that the use of camera images for the purpose of identifying subjects in public places such as hotels, shopping malls, stations, airports, and recreational or sports facilities is a form of personal data processing, see the Supreme People's Court's Forecasts on Various Issues Concerning the Application of the Law in Civil Law Cases Concerning the Processing of Personal Data through Facial Recognition Technologies of July 27, 2021.

[38] The 2012 decision, in Article 1, also referred to information that made the subjects of the processing identified or identifiable, but with two important differences. The first is that, in the decision, "information involving the confidentiality of the same" was also taken into account. The reference to confidentiality was thus removed from the definition, perhaps coherently with the more general trend, which, as will be discussed below, the Chinese Civil Code enshrines, of separating the regulation of personal data from the regulation of confidentiality. The second novelty is that not only data referable to Chinese citizens are subject to protection, but to all natural persons. As mentioned above, part of the doctrine has seen this as evidence of the Chinese legislature's decision to abandon the North American model of data protection in favor of the European model. The Privacy Act, 5 U.S.C. § 552a(a)(2) clarifies that: "the term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence." The shift from the former to the latter would also be evidenced by the decision to adopt a personal data regulation based on a general data law, PIPL. Indeed, the regulation of data protection in the U.S. system is based only on sector-specific rules, such as those contained in 15 U.S.C, § 41 et seq. which may in fact have been the inspiration for the earlier Chinese legislature, in the consumer protection provisions recalled *supra* in paragraph 1. An innovation made by the PIPL, and perhaps borrowed from the GDPR, concerns the introduction of the notion of a personal data controller, rendered in Chinese as 个人信息处理者. Earlier laws, including the Network Security Act,

the supervisory role of public organs[39].

Book IV of the Chinese Civil Code addresses the issue of the relationship between personal data protection and the right to privacy. Article 990 enumerates personality rights. They include the right to life, the right to physical integrity, the right to health, the right to a name, the right to reputation, the right to honor, and the right to privacy (隐私权). The list is not exhaustive, as Article 990 concludes with the phrase "and other rights." The second paragraph of Article 990 adds, "in addition to the rights listed, the individual shall enjoy all other rights and interests of personality derived from personal freedom and human dignity." A further list of rights, headed as "civil rights," is included in Article 110. It overlaps with the list in Article 990, from which it differentiates only in the addition of the right to spousal autonomy, that is, the right of the individual to freely choose his or her spouse[40]. The protection of personal data is again excluded from the list. However, they appear in the subsequent Article 111, which states that personal data are subject to protection by law, without openly stating the existence of an individual right to the protection of personal data.

The exclusion of the protection of personal data from the list of subjective rights, has led Chinese jurists to wonder about the nature of the subjective legal situation in the hands of the person affected by the processing and the possible practical consequences of denying the nature of subjective right to personal data[41].

In the Civil Code, the right to privacy is defined as the right to the undisturbed conduct of private life and the protection of the intimate sphere of natural persons, its private activities and its private information[42], which it does not want to be disclosed to others

---

had used the concept of network service provider, 网络**运**营者 or 网络服务提供者, borrowed from the discipline, strongly marked by public elements, of the liability of network service providers.

[39] See H Zhao (赵宏), "《民法典》时代个人信息权的国家保护义务" (The Nation's duty to protect the right to personal information in the era of the Civil Code), Vol. 1 /2021, 经贸法律评论 (Economic and Trade Law Review), pp. 6 - 8, draws a dual system of data protection, where public law and private law tools coexist.

[40] The right to decide on one's own spouse aims to solve the practice of arranged marriages, which is still extremely widespread in the country.

[41] See L Wang, (王利明), '论《个人信息保护法》与《民法典》的适用关系', (On the relation of the application of the "Personal Information Protection Law" and the "Civil Code"), (2021) 中国民商法律网, (China Civil and Commercial Law), available from https://mp.weixin.qq.com/s/BTEYEWcNfLPFyxzmJgv3Pw. Wang Limin is one of the most influential proponents of the argument that personal data are also protected through private remedies. According to the A., the fact that personal data are subject to public protection does not exclude their civil law nature. See also H Zhao, The Nation's duty to protect the right to personal information in the era of the Civil Code (n 39), reaffirms that the Civil Code purposefully does not define data protection as an individual right. Incidentally, the author also points out that the expression used by Art. 111 of the Civil Code, which obligates "any organization or entity that has a need to obtain data of others," also includes the Chinese government, against whose data collection activities civil remedies would thus be available. [41] The very placement of personality rights in an autonomous book of the Civil Code, precisely the fourth, has been sharply criticized by German doctrine, on the grounds that it entails a departure from the scheme of the BGB, not justified by the addition of forms of protection other than compensation for non-contractual damage [41]. Moreover, the use of compensation actions is also recognized by Chinese jurisprudence to protect legal situations falling under the category of civil legitimate interests, see H. von Senger, 'Vom Code Napoleons zum Zivilgesetzbuchs Xi Jinpings' (2020) 2, ZChR, p. 144, who points out that Book IV of the Code is essentially declaratory in nature, since it adds no practical remedies to those provided in the other books, and in particular in Book VII on the protection of torts.

[42] The concept of private information is the result of a semantic choice by the Chinese legislature, on which it is appropriate to dwell. The expression used by article 1032 is 私密信息, the translation of which is particularly problematic. The literal translation of the concept is "private information," a translation, however, that does not

(Art. 1032, c. 2). Acts detrimental to privacy, are listed in Art. 1032 and are the investigation, intrusion, disclosure, publicizing and handling of private information (私密信息 – *simi xinxi*).

The notion of private information is of pivotal importance, because it establishes the boundary between tools for the protection of privacy and personal data protection. Its boundaries, however, are blurred. They do not overlap with the concept of sensitive personal data (敏感个人信息), which is defined in Article 28 of the PIPL, as the information which, if illegally used or leaked, could cause harm to the dignity of natural persons or harm their personal security or property[43].

The concept of private information is more blurred. The code qualifies it as information that the individual does not want to disclose to others, but without further elaborating[44]. Article 1033 of the civil code lists some conduct that infringes on the right to privacy, including the "handling of other people's private information."[45] . Since the handling of others' private information is in itself an infringement of the individual's right to privacy, it is to be understood as an activity that is substantially restricted. It is in this sense that Chinese doctrine has warned interpreters against confusing private information with sensitive data, clarifying that "since the concept of private information is very broad, (...) it also risks weakening the foundation for the development of big data

capture the closeness of the expression to the categories proper to personal data protection. "Data," as noted above, is rendered in Chinese as 数据, - *shuju* -, but personal data is referred to as 个人信息 - *geren xinxi*, literally "personal information." The term used by the code to denote private information is *simi xinxi, which* precisely uses the same word, *xinxi*, by which personal information is denoted. Some authors have therefore translated the concept of *simi xinxi* as "sensitive data". This is a solution that cannot be accepted. Detailed regulation of sensitive data was introduced only with the Data Protection Act of November 1, 2021, which followed the Code by a few months (which came into effect on January 1, 2021). Here, sensitive data is referred to as 敏感个人信息 or *mingan geren xinxi*, literally sensitive personal information. The concept of *mingan geren xinxi*, unlike the more problematic expression used by the code, *simi xinxi,* is immediately relatable to the category of personal data, with respect to which it is in a species to *genus* relationship. Consistently, Article 28 of the Personal Data Protection Law defines sensitive data as those personal data that, if disclosed or improperly processed, may harm the dignity or security of the person or property of the person concerned. The standard includes an illustrative list of sensitive data, which are biometric data, religious beliefs, special identity (特定身份), health data, financial data, and geolocation data. All personal data referable to individuals under the age of 14 are also considered sensitive. The mandatory standard GBT35273, released in 2017 and updated in 2020, also refers to personal information. It is worth adding that the definition of sensitive information therein is partially different from that in Article 29 of the Personal Information Protection Act. Paragraph 3.2. of the Standard defines sensitive data as data whose loss, disclosure in ways contrary to law, or misuse, could endanger the personal or financial security of the data subjects or result in damage to reputation, physical and mental health, or discrimination against the data subject.

[43] Article 28 includes also a list of information which represent sensitive data: “information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14”.

[44] The definition is undoubtedly insufficient, as the right holder cannot be allowed to define its scope. X Cheng, (程啸), ‘我国民法典对隐私权和个人信息的保护‘ (Protection of privacy and personal information in our Civil Code) [2020] China Court, available at: https://www.chinacourt.org/article/detail/2020/07/id/5383094.shtml,. Moreover, the term "private data" also appears in Article 45 of the Network Security Act, where it also lacks a definition.

[45] The provision by prohibiting "intruding into a person's private life through phone calls, sending text messages, using instant messaging tools, sending e-mails and flyers and the like"; "taking photographs or spying on the intimate parts of another person's body" and others, helps to define the content of the tortious activities mentioned in Article 1032 (investigation, intrusion, disclosure, publicizing).

and artificial intelligence."[46] .

The boundary between the regulation of personal data, which can be legitimately controlled within the scope of the exercise of an economic activity, and that of private information, which falls within the scope of the right to confidentiality, subject to the protection of personality rights, is clarified by Article 1034 of the Civil Code[47]. The rule states that "to those personal data that represent private information the rules on the protection of confidentiality, or, failing that, those on the protection of personal data, shall apply."[48] . Personal data can thus be private information, when, for example, a combination of personal data reveals private information[49]. In this case, the plans for protection overlap and priority should be given to the instruments for protecting private information[50].

Civil Code provisions on private information, despite the uncertainties of the terminological and systematic framework, have the merit of placing the regulation of data circulation in the broader context of the protection of personality rights and of separating with some clarity the sphere in which the protections of the right to privacy operate from the regulation of personal data.

The difference is relevant not only in terms of protection, but also in terms of economic exploitation, which are limited for personality rights, and allowed for personal data, albeit within the contours established by the PIPL of 2021[51]. The regulation of personal data is characterized by the fact that the profiles focused on protection are accompanied by the provision of numerous principles dedicated to the processing of the same, that is, on a form of economic exploitation. It is in terms of the economic exploitation of personal data that Article 1 of the Personal Data Protection Act, which supplements and expands the codicil principles (Art. 1, see, *amplius, infra*)[52]. The practical effect of denying that personal data fall within the scope of personal rights is

---

[46] Along these lines, K Ran, (冉克平), '论《民法典》视野下个人隐私信息的保护与利用', (On the protection and usage of private information in the Civil Code) [2021], Soc. Sci. J., pp. 103 - 111, who argues that: "由于隐私信息的范围非常广泛，《民法典》第 1034 条第 3 款为隐私信息提供单一的权利优先保护模式，不仅难以为不同类型的个人隐私信息提供差异化保护，而且会削弱大数据和人工智能创新发展的基础".

[47] Cf. with X. Cheng, (程啸), '个人信息保护中的敏感信息与私密信息', (Sensitive and Private Information in Personal Information Protection), [2022] Zhengzhou Intermediate People's Court Webpage, available at http://zzfy.hncourt.gov.cn/public/detail.php?id=27359.

[48] See K Ran, 'On the protection and usage of of private information in the Civil Code' (n 46) who also considers the provision in Article 1034, c. 3, too vague to be able to reconstruct how the privacy provisions concretely apply to private data, considers, for example, that nude photos and photos depicting the individual in the course of sexual relations are personal information and therefore cannot be legitimately collected and used by third parties.

[49] See X Cheng, 'Protection of privacy and personal information in our Civil Code' (n 44).

[50] See Z Gu, (**谷兆阳**), '**民法典中**隐私权与个人信息保护的关系', (The relationship between privacy and personal data protection in the civil code) [2021] Supreme People's Procuratorate Webpage, available at: https://www.spp.gov.cn/spp/llyj/202108/t20210825_527513.shtml, who clarifies that these are limited hypotheses, such as the case where a combination of personal data allows it to be traced back to the fact that a person has contracted AIDS.

[51] See L Wang, B Xiong, "Personality rights in China's New Civil Code", (n 1). p. 712 who point out that limited forms of exploitation of personality rights are allowed in the Civil Code. This distinguishes them from the right to bodily integrity, which is completely excluded from the individual's autonomy.

[52] The code also devotes some provisions to negotiated acts involving the exploitation of the right to the name (Art. 1013) and image (Arts. 1021, 1022). However, these are not accompanied by detailed rules or principles governing the use of the name and image.

to exclude their qualification as absolute rights and insusceptible to economic exploitation by third parties[53].

3. Economic circulation of data circulation in China.

The main goal of personal data protection, to which both the GDPR and the PIPL respond, is a consequence of the fact that personal data have now become a key economic resource[54]. The provisions on the processing of personal data and the individual rights that have been listed above respond to the need to ensure that economic activities involving personal data are carried out in deference to the principle of limited negotiability of personality rights. A further problem is that of the circulation of rights of economic exploitation of personal data.

In European law, that an economic regulation of the circulation of personal data accompanies privacy reflections of the regulation is now a widely held view in doctrine and accepted in case law[55]. Article 1 of the GDPR not only states, in paragraph 3, that "the free movement of personal data in the Union may not be restricted or prohibited on grounds relating to the protection of natural persons with regard to the processing of personal data," but also provides that the regulation shall lay down rules relating to the free movement of personal data (Art. 1, c.1). Moreover, the original core of the recognition of the proprietary nature of personal data was already contained in Directive No. 95/46 EC[56].

In China, the Personal Data Protection Law in Article 1 "promotes the rational exploitation of personal data"[57]. Earlier laws, while not expressly mentioning the economic exploitation of personal data, seem to assume such lawfulness. For example, the E-Commerce Act of 2018 prohibits acts of disposition involving the personal data of others, but only when a public official is selling it (Article 85). Moreover, the same law seems to implicitly admit the existence of a market for personal data when regulating the use of personal data collected by e-commerce platforms for promotional

[53] See X Cheng, (程啸), '民法典编纂视野下的个人信息保护', (Protection of personal information in the perspective of civil code codification.) in 中国法学 (China Law), 2021.

[54] Not surprisingly, the doctrine has been reported to find that the main purpose of the current generation of regulations is to define the private relationships that exist between the person identified by personal data and the economic operator who makes a profit from it, V Ricciuto, Circolazione e scambio di dati personali *cit.*, p. 8.

[55] See V Ricciuto, *Circolazione e scambio di dati personali, cit.*, p. 12; G Resta, *I dati personali oggetto del contratto*, in V Ricciuto, C Solinas (ed.) *Forniture di servizi digitali e pagamento con la prestazione dei dati personali*, CEDAM, (2022), p. 56.

[56] On the progressive recognition of the patrimonial nature in EU law, and the resistance of Italian legal science, V Ricciuto, 'La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno', [2018], in Il diritto dell'informazione, pp. 689, ff.

[57] Article 1 Personal Data Protection Law: "This law is adopted in implementation of the Constitution, in order to protect rights and interests over personal data, standardize personal data processing activities, and promote rational exploitation of personal data. Note that the term 利用 presents a certain degree of ambiguity. The most authoritative translation of the Data Protection Act currently available (from Chinese to 'English), by R Creemers, available at https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, translates *liyong*, as "use."

purposes[58].

In this essay, we avoid to delve into the web of proclamations by political figures and policy documents, which are often redundant and lack the immediate force of law. But even from a rapid and non exhaustive overview, it is clear that the Chinese policy-makers acknowledge the existence of a data market and admit its lawfulness. The document entitled *Outline of Operations to Stimulate the Development of Big Data*, adopted by China's State Council on August 31, 2015 is dedicated to the purpose of encouraging greater use of *big data* by private industry, as well as complementing public market regulation activities through *big data*[59] . The importance of big data is emphasized also in the *Opinions to Build a More Improved Production Factor Allocation System-Guiding Factors in Advanced Production Forces*, published by the State Council on April 10, 2020. The Opinions do not only focus on digitization, but on perfecting China's data economy toward a market economy. Here data, understood not as personal data but generically as *shuju*, is taken into account as a factor in industrial production, an assessment that entered formal law through Article 7 of the 2021 Data Security Law.

All the sources mentioned mainly refer to big data, that is, aggregated and often anonymous data. Explicit references to the circulation of personal data in the market are lacking. More generally, neither the title nor the contract according to which economic exploitation rights over individuals' personal data may be assigned or transferred to third parties is clear[60].

In the Chinese context, the multitude of policy documents emphasizing the importance of the *data economy* is contrasted with the uncertainty of the law on the legal basis that enables contractual circulation of personal data[61]. Article 23 of the PIPL merely confirms the validity of transfers (the provision uses the verb 提供 - *tigong*, which means supply or offer) of data by a data controller to another data controller, conditioning them on a mere obligation to notify the data subject[62] . Interestingly, the same term, *tigong*, appears in Article 111 of the Code, which in establishing that personal data are subject to protection by law, prohibits organizations that process personal data from "buying, selling, or supplying (*tigong*) it in a manner contrary to law".

PIPL, art. 23, makes it clear that not only does the data subject have the right to be

---

[58] The use of individual information for profiling to reconstruct individual-consumer preferences is one of the most important and lucrative commercial uses of personal data. See A Acquisti, C Taylor, L Wagman, The Economics of Privacy (2015) 54 [2] Journal of Economic Literature, pp. 443, ff.

[59]国务院关于印发促进大数据发展. GF No. 50/2015. In this policy document, in Chapter 2, with reference to the government's use of big data to accelerate industrial development, the Chinese government uses the phrase "stimulate the creation of market services using big data technologies."

[60] See C Peng, (彭诚信), '论个人信息的双重法律属性', (On the two sorts of legal qualification of personal data*)* [2021], Tsinghua Law Journal, p. 79.

[61] See A Fei (费安玲), '论买卖合同标的物规则的形成理念——以人格尊严和无体物为分析视角', in 环球法律评, (On the Concept of the Formation of the Subject Matter Rule for Sale and Purchase Contracts - An Analytical Perspective on Human Dignity and Incorporeality), [2022], 环球法律评论, (Global law review), pp. 117, who makes an extensive critique of the code's provision, noting how the Chinese legislature misrepresented the content historically given to contracts of sale and purchase in Roman law systems, in which the distinction between res *corporales* and *res incorporales* was central.

[62] More explicit is Article 7 of the DSL, which, however, does not refer to personal data, but to data in general. In fact, the provision states that the state "shall protect the data-related rights and interests of natural and legal persons (...), ensure a free flow of data, and promote the digital economy with data as a key factor."

informed of the transfer, but that the new processing may not exceed the purpose of the original one. The literal sense of Article 23 would seem to open up the possibility that personal data can be the subject of acts of disposition. Chinese doctrine has clarified in this sense that buying and selling represents the archetypal contractual scheme of rights transfer[63]. At the same time, article 595 of the Civil Code provides that the object of purchase and sale is a tangible object (物). It is uncertain, whether the Chinese legislature's choice to limit the object of sale and purchase to the "thing" makes the provisions on sale and purchase contracts that could be adapted radically inapplicable to the circulation of personal data. The Supreme People's Court indirectly touched on the issue in the aforementioned Case No. 9 in its April 11, 2022 interpretation, titled "large-scale buying and selling of personal information violates personality rights and social public interests." The use of the term, implies that transfers of personal data are sale contracts, which in the present case are held to be unlawful not because they are being sold, but because they were originally acquired without the consent of the data subjects.

Even allowing for a broad interpretation of Article 595, that is, an interpretation that understands the term 物 as “good” and not as “physical thing”, does not solve the additional problem of whether personal data qualify as a good.

Buying and selling is expressly prohibited only if it diminishes the person's physical integrity (Art. 1017, Civil Code). The sale of parts of the human body is prohibited even when it does not involve a permanent injury or otherwise a relinquishment of the integrity of the body itself, but by the very fact that the thing being bought and sold is composed of human tissue[64].

Personality rights are excluded from the prohibition just reported. From comparison with common law systems, Chinese jurists have observed how, in Chinese law, personality rights can be only subject to very limited economic exploitation[65].

Although a piece of information may be stored in an electronic data, it is not embedded in it and remains an intangible asset, can be copied and is not consumable, indeed its value increases by virtue of repeated use[66] . The same information can be collected and processed in the form of electronic data by more than one party, without being the subject of an exclusive right by any of them. Starting from this consideration,

---

[63] See A Fei, ‘On the Concept of the Formation of the Subject Matter Rule for Sale and Purchase Contracts’ (n 61).

[64] See L Wang, B Xiong, ‘Personality rights in China's New Civil Code’, (n 1) p. 712 claim that womb surrogacy is a widely debated issue in China. This is partly because of the respect that legal traditions from ancient times enjoy in the Chinese legal culture. In ancient China, as indeed in contemporary Greece and Rome, maternal surrogacy, in the form of wife rental, was permitted. This legal institute, known in classical Chinese law as 借腹生子 (literally "renting a belly to give birth to a child"), is described, in the version adopted in Sparta, by Plutarch: "if an honored man admired a prolific woman married to another he could, with the consent of her husband join her, so as to sow fertile ground, and procure valiant sons, who would be brothers and blood relatives of valiant men" (Lyc, 15:11-13). Cf. also A Fei, “On the Concept of the Formation of the Subject Matter Rule for Sale and Purchase Contracts - An Analytical Perspective on Human Dignity and Incorporeality” (n 61), according to whom there were more than 500 trials related to the buying and selling of human tissue in China in 2022. This bleak picture also emerges from the pages of Chinese novelist Yu Hua, who in his collection of short stories titled "China in Ten Words" describes how in the 1990s, during China's economic boom, there were underground blood exchanges.

[65] See J Xue (薛军), ‘人的保护: 中国民法典编撰的价值基础’, (The protection of human beings: the value basis of the Chinese civil code) [2006] 中国社会科学 (Chinese Social Sciences), p. 122.

[66] See C Peng, ‘On the two sorts of legal qualification of personal data’, (n 60), p. 80.

it has been noted, that if from the "raw" personal data, through processing, more elaborate information about the individual is derived (and susceptible to more lucrative commercial uses), the data may acquire a new nature as a finished good, susceptible to forms of exclusive ownership referable to the data controller, without prejudice to the personality rights attached to them[67] .

The issue of the nature of property rights, the subject of lively doctrinal debate, has only been touched upon in case law. It is therefore appropriate to merely mention the case of *Weibo v. Maimai*, although it predates the promulgation of recent data protection laws, as it has had some resonance in China. Weibo is a service that blends some features of Facebook with some of Twitter. It allows its users, whether individuals or companies, to create profiles, through which they can interact. Maimai is a service roughly equivalent to LinkedIn, which also operated through Weibo. Cooperation between the parties was governed by meticulous agreements, which Maimai violated through the collection of data regarding education and professional experience, as well as Weibo users' most frequently used profile photos, names, and *tags*. On Maimai's defense, which argued that Weibo cannot prevent third parties from using its users' data, which moreover is visible to any user, the appellate court noted that the data was not acquired by virtue of an autonomous algorithm, but by cross-referencing users' personal data, such as phone numbers, with those registered on Weibo. In condemning Maimai, censuring its conduct, however, the Beijing court applied unfair competition rules. The Weibo v. Maimai case, which dates precisely from 2016, demonstrates that, in fact, data controllers' property rights were protected in China even before the enactment of the main laws on the subject, which came into effect between 2017 and 2021[68].

4. Public governance tools for the protection of personal data and the data market.

The PIPL, while maintaining several Chinese characteristics is based on a foreign law, which of course is the GDPR. The CSL and DSL, on the other hand, are distinctly Chinese. They create a legal regime applicable to all data, regardless of whether they are personal, important or sensitive. Unlike the PIPL, these two laws use a programmatic language and objectives. Indeed, it could be argued that the impact of the GDPR on the PIPL is not only its content, but also the legislative methodology[69].

The first major law to enter in force after the creation of the CAC was the

[67] See C Peng, *Ibid* p. 83.

[68] Others have noted an opposing tendency of Chinese judicial authorities to thwart monopolistic attitudes on the part of major market players, C Boullenois, 'China's data strategy' [2021] in ISS Europa, available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_21_2021.pdf, p. 4. This trend is about to find express legislative recognition in Article 9 of the Law Against Monopolies, which will go into effect on August 24, 2022 and provides: Operators shall not use data and algorithms, technologies, capitalization advantages, and rules to engage in monopolistic conduct prohibited by this law.

[69] See R Creemers, (n 7) p. 8, who, in comparing the PIPL and GDPR, claims that "While this model resembles, and hasderived ample inspiration from, the GDPR, it misses the generalityof the European approach: where China has recreated the consumerprotection aspect of the GDPR to a significant degree, it has not emulatedthe European foundational principle that privacy is a fundamentalright. Most importantly, the PIPL largely leaves the powerof government bodies untouched, as it does not impose any meaningfulconstraints on their ability to collect and process data".

Cybersecurity law (2017), which forms the true cornerstone of the Chinese data protection regime. The CSL encompasses different elements, ranging from content control to the protection of strategic infrastructures, to security of network products.

The storage of important and personal data in Chinese territory is a major concern of the legislator, which is also reflected in the detailed and restrictive regulation regarding the transfer of data out of China[70]. The CSL, which is overall vague and imprecise, did not provide for a detailed regime on data localization requirements, which were later introduced by the CAC through regulations. Most importantly, data localization requirements were further specified through the PIPL.

The CSL regulates not only data processing activities, but network operators more in general. The regulation of network access service providers in China requires them to exclude intermediary peripheral service providers identified by the government. This exclusion primarily affects numerous Western newspapers, and more generally websites that depict the Chinese government's actions as human rights violations[71]. But censorship limited to measures to remove specific websites or content would be bound to be ineffective. The sheer volume of material disseminated through the Internet imposes can only be filtered through the control of vital nodes of the network, i.e., Internet sites, such as search engines, social platforms, etc., that are instrumental to the operation of other sites, as well as to cooperation between subjects[72].

Chinese scholars described how the blocking of Google, Facebook, Amazon and several other vital nodes in the Western information system has opened up market space for Chinese Internet industry players[73]. The exclusion of major Western platforms allowed the Chinese industry to fill the void left by the censorship of Western online service providers[74]. As a result, numerous alternative platforms, Chinese intermediaries offering online services parallel to those offered by Western counterparts, have emerged.

The dynamics of expansion and contraction of the freedom of private economic initiative in China are particularly evident precisely in the field of offering network intermediation services[75]. The CSL further identifies some categories of data holders

---

[70] See D Clementi, 'La legge cinese sulla protezione delle informazioni personali: un GDPR con caratteristiche cinesi?' (n 6).

[71] See H Zheng, 'Regulating the Internet: China's law and practice' (2013) 4 [1] Beijing L. Rev., p. 1.

[72] A significant citation from the people's newspaper, the renmin ribao is made by J A Lee and C.Y. Liu 'Forbidden City enclosed by the great firewall: the law and power of internet filtering in China' [2012] Minn. J. of L., Sci.. & Tech., p. 144: "*As long as we use more ways of properly looking at the Internet, we can make use of the best parts, we go for the good and stay away from the bad and we use it for our purposes, then we can turn it around on them . . . [W]e won't be defeated in this huge Internet war by the various intranational and international reactionary ideological trends in the various areas.*" The Authors go on to comment that "*In sum, the Chinese government praises efforts to benefit from digital technology's advantages, but declares that use of digital technology must not undermine state control.*"

[73] This aspect is frequently stressed by Chinese doctrine, see, for example, W Miao, M Jiang, Y Pang 'Historicizing Internet Regulation in China' (n 22), p. 2022.

[74] For a careful reconstruction of Chinese industrial policies implemented for the purpose of closing the gap with Western competitors, see C Foster, S Azmeh, 'Latecomer Economies and National Digital Policy: An Industrial Policy Perspective', [2020] The Journal of Development Studies, pp. 1247-1262.

[75] A well-known case is that of the *online shadow banking* sector in China. As mentioned earlier, China's banking sector is dominated by the presence of the so-called big *four*, large state-owned banks whose main function is to direct savings toward the financing of strategic enterprises, that is, those instrumental in achieving the government's policy goals, see S Sen, 'Finance in China after the WTO' [2005] Economic and Political Weekly p. 565. Cf. D Elliott, A

that are defined as critical information infrastructure. According to the definition provided for in relevant administrative regulations, such infrastructure includes, but is not limited to important network infrastructure. Important industries in critical sectors, such as energy, transportation and finance are also included[76]. Such industries are subject to strengthened security measures, clarified in the Regulations.

The DSL and CSL also provide for a categorization of data based on their relevance for China's strategic and economic interests. It is parallel to private law classifications, adopted by the PIPL and the Civil Code, which is instrumental to modulate data protection on its impact on personality rights. The CSL mentions personal data, but not sensitive data, nor private information. On the other hand, it speaks of "important data", which are data that are not necessarily related to a physical person, but cannot be stored abroad without the CAC's approval. However, because the draft of the CSL talked about important business data and the final version of important data, the legislator likely wanted to include data that are important in a strategic perspective. The DSL also includes another category of data, which are "core national data". These are data related to "national security, the lifelines of the national economy, important aspects of people's livelihoods, major public interests, etc".

Kroeber, Q Yu, 'Shadow banking in China: a primer, in, Economic Studies' , [2015] The Brookings-Tsinghua Center, p. 1, who point out that the dynamic just described has prevented the Chinese banking system from operating in the market and reduced its ability to finance the growth of private firms. The Chinese government has thus allowed the *shadow* banking system, so-called *shadow banking*, to flourish in the form of financial intermediation services offered through the network and highly deregulated. . These consisted largely of *matchmaking* mechanisms that allowed savers to view credit applications submitted by companies. In a few years they evolved into full-fledged institutions dedicated to credit collection, to which, however, the onerous rules of Chinese banking law were not applied. Even broader exceptions, however, have been granted to *crowfunding* platforms, which in fact often end up engaging in the business of offering financial products to the public, as defined by Article 15 of the Financial Products Law, an activity which, according to Interpretation 18/2010, if carried out without the permission of the competent authority, the CRSC, constitutes the crime of misappropriation of savings of the public, as defined in Article 176 of the Criminal Law. *Crowdfunding* companies have put in place measures to prevent the activity carried out from falling under the definition in Article 15. These are merely cosmetic measures, such as the creation of membership lists. The turning point in both the regulation of online financial services and the market dynamics of the same came with the Guidelines of the National Bureau of Information through the Internet (Yin Fa 2015 - No. 221) on promoting the healthy development of Internet finance. The Guidelines enshrined the principle that the development of the industry would benefit from greater involvement of authorities and more centralization in the hands of a small number of large (and therefore more reliable) companies. It should be emphasized that the Guidelines aimed not only to improve the security of the fintech market, but to increase its economic and innovative potential. They thus introduced a wide range of new legislation and enforcement practices. In fact, they ordered (a) banks and other institutional entities, to invest more in the sector and to fund internet platforms that complied with progressive legal requirements; (b) market regulators, to encourage mergers or other forms of cooperation among Chinese fintech companies (c) administrative departments for industry and market to encourage the registration of de facto entities operating in the sector; (d) to apply taxation regulations to companies active in the sector; (e) to establish physical infrastructure, such as databases, to support the expansion of the sector; and (f) to banks to put in place agreements with payment service intermediaries in order to enable networked payments and to stand as guarantors of the legitimate development of such payment systems.

They also divided the *online* lending system between P2P loans, i.e., between individuals and thus subject to the lending rules contained in the Contracts Act (now absorbed into the Civil Code that went into effect on January 1, 2021), and loans that took place through aggregate networks of creditors and debtors, which were instead subject to supervision by financial market regulators.

[76] Article 2 of Regulation No. 745/2021, issued by the State Council, Critical Information Infrastructure Security Protection Regulations, translation available at: https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/.

Conclusions.

The personal data protection system erected by the PIPL resembles, in many aspects, the GDPR. It was pointed out that the main difference between the PIPL and the GDPR is that the Chinese personal data protection regime is clearer about the distinction between data protection and privacy. This is indeed confirmed by the Civil Code provisions, which frame data protection as a matter parallel, but not overlapping privacy and other personal rights. Such a comparison could convoy the idea that overall the Chinese data protection regime is lacking, if compared to the European one.

On the other hand, the Chinese PIPL is framed in a broader data regulation, which takes into account both the handling of personal information that affects the individual, as well as the regulation of data in the perspective of the protection of national security and economic interests.