Can Chinese legislation on informational privacy benefit from European experience?

Zhang, K.

Summary

Summary of: Can Chinese Legislation on Informational Privacy Benefit from European Experience?

This thesis is concerned with data protection legislation in China. The primary objective is to examine the advisability of cloning European data protection law and transplant it into China. In order to address the issue, I explored it from several perspectives.

In Chapter 2, using documentary evidence and interview results, I compared the material laws over data protection of the European general system with the Chinese credit reporting system, and provided a positivist assessment of the data protection levels in the two regions. In doing so I employed a set of measure sticks that I derived from the 2013 version of the OECD guidelines. I focused on the differences (not on the matches) between the two jurisdictions. These differences are marked. Generally, the comparison reveals that European data protection laws cover the principles of informational privacy as embedded in OECD 2013 far more complete than Chinese data-protection laws do (when available at all). Considering the Chinese credit reporting database CRC in Chapter 2 thus provides evidence that this database, were it operational in Europe, would be in danger of being deemed illegal. I pointed out that the CRC's operations violate three types of privacy guarantees, valid under European data protection law.

The first violation type concerns the data subject's rights. Two elements in the OECD 2013 are recognized by both regions. Yet, the right to object, which can be considered a species of the right to challenge is a peculiarity of European data protection law and is not observed in Chinese laws. The second type of violations concerns the data controllers' obligations. The Directive recognizes all

OECD principles on the data controllers' obligations, while Chinese Credit Reporting Laws miss the collection limitation principle, the use limitation principle, the openness principle and the accountability principles. These omissions are serious indeed. The third violation type concerns the procedural issues. Implementation principles are largely recognized by European data protection law, except the national strategy, which was only incorporated into the OECD guidelines in 2013. Yet, China misses most of the procedural core issues. Only three principles are found in China's system, including "reasonable means for the individual to exercise their rights, adequate sanctions and complementary measures." Again, Chinese positive laws on data protection for credit reporting lag seriously behind Directive 95/46/EC when looked at through the lens of OECD 2013. Therefore, under China's legal arrangements Chinese CRC database use might very well be considered legal. Yet under European law the very same database use would clearly be illegal.

Based on the above comparison, I conclude that if China's policymakers introduce European data protection law, it can upgrade China's legal arrangements, considered from a positivist perspective. Consequently, and assuming the "all other things being equal" assumption, European data protection law can serve as a point of departure for improving China's legal arrangements. But since we know that all other things are not equal between Europe and China, I submit that further investigations are needed. They may suggest improvements to the plan to directly clone and transplant legal texts from Europe into China.

In Chapter 3, I investigated the evolution of privacy and informational privacy in Europe and China as these evolutionary paths have certainly unwound under different conditions. I began the Chapter by showing some considerations on the analogies between languages, cultures and legal systems: like languages, legal systems evolve under the pressures of the cultures they serve and are part of - consequently, by looking at the developments in their cultural environments, how the differences between legal systems may be better understood - both in the book (the positivist perspective) and in action (the realist perspective). Based on the analysis I conclude that differences in culture helped shape differences in data protection law. As the discussion of European data protection law in the Chapter demonstrates, it has

emerged from the (functional) roots of European privacy conceptions that came to flourish under the pressures of contingencies in the environment. These functional roots are there first, and are soon followed by the emergence of the first legal forms of privacy protection by law. Privacy functions and laws kept on co-evolving in Europe and culminated after World War II not only in elaborate functional (and thus instrumental) legislation, but also in the rather Kantian idea of privacy as an intrinsically individualist human value (as expressed in art. 12 of the UDHR). In China, the current legal arrangement over data protection issues grows directly out of China's collectivist culture, which only rewards the instrumental-goods aspect of privacy. The findings in this Chapter suggest that China's policymakers should realize that European data protection law is being transplanted neither from, nor to jurisdictions with culturally blank or neutral slates. Instead, both Europe and China have pre-existing sets of data protection laws and privacy- related cultural norms. The cultures that embed privacy practices are complicated and have far-reaching implications for the ways that data protection laws are and will be understood, and on how they will be received, upheld and enforced. Therefore, I suggest that China will adopt a cautious approach to the realization of the legal transplantation plan.

At the end of Chapter 3, I have established differences between two positive law arrangements and between the two cultures involved. There is a lot that at first sight seems a valid candidate for importation from the EU to China. Yet, there are risks. For instance, both technical innovation and the uptake of social media services are highly dynamic and tend to make adequate legislation difficult. So in order to make an informed choice about what to import and what not to import, it is useful to analyze how the legal systems under discussion support (or undermine) the recipient legal system's resilience in a changing environment.

This very issue is my motivation for Chapter 4's excursion into Incomplete Law theory. In order to impose an interpretation on the phenomenon in question, I deployed the theory of Incomplete Law, created by Xu and Pistor, for the analysis. It showed that European data protection laws, as represented by Directive 95/46/EC, are incomplete. The reasons can be categorized in three ways. First, the generality of the Directive makes it difficult to provide rules that are

specific enough; second, technology, that strongly influences data protection law's subject matter, changes at high speed and therefore renders the Directive more incomplete as it lags further behind; and finally, lawmakers are unable to foresee all future contingencies, also those contingencies that emerge through mass adoption of innovative services. Particularly, technology's changes strongly challenge even the short-term "fit" of the Directive. The Directive 95/46/EC was designed to regulate the data processing technologies a couple of decades ago and thus focused on "old" problems while digital technologies have experienced radical revolutions. New advanced digital technologies were being introduced into public communications networks and in the community. Access to digital mobile networks has become available and affordable for the public at large. These digital networks have huge opportunities for processing personal data. All these changes, thus, required frequent adaptations of the law for it to remain effective. This led to problems with the law's focus and mechanisms to remain connected to reality.

How does Europe arrange to face the resulting incompleteness? European policymakers created a new role, the data protection authority who assumes residual LMLEP (law making and law enforcing powers), in order to make interventions possible for mitigating the problems of incompleteness. In Chapter 4, I focused on the Article 29. Working Party and the national data-protection authorities that take significant roles in regulating and law enforcement for reducing incompleteness. The investigation confirmed that the emergence of data authorities responded to the problem of under-enforcement caused by highly incomplete law. Data authorities are more flexible than legislative agencies on adapting the law to a changed technical environment (although the scope of their lawmaking rights is limited), since their swift reaction time allows them to better keep up with the fast pace of technology. And Data authorities are more proactive than courts, since they can initiate actions to enforce data protection law in situations where courts, by design, have to wait for a file to be suit.

Consequently, the findings in Chapter 4 reject the assumption (which China's policymakers nurse) that European data protection law is complete, and that the transplantation scheme can be confined to material, positive data protection laws. I show that, beyond their expectations, issues of dynamics in technology and in mass use of social media are not trivial and require measures that safeguard the availability of a highly informed and highly responsive authority that has sufficient residual LMLEP to guard the law's incompleteness will not become intolerable. I conclude that legal transplantation as envisaged will not ensue effective consequences unless a competent regulatory authority is in place.

As a follow up to this conclusion, I analyzed in Chapter 5 what gaps between the law in the books and the law in action the EU data authorities have to face when they regulate American Facebook or its Chinese sibling (RenRen). It is clear from the discussion that RenRen's current practices are neither in compliance with European Data Protection principles, nor with EU data protection laws. Consequently, if RenRen would open its EU headquarters in any member state in Europe, the firm may receive multiple complaints about its data protection practices. Regarding Facebook, I conclude that, even though its current practices seem to comply with EU data protection law, they do not fully comply with European Data Protection principles. This leads to the insight that what is acceptable to EU privacy laws needs not be acceptable through the lens of the Working Party's principles. On the one hand, this means that the level of data subjects' protection may increase substantially to a higher level, dependent of the data regulators' performance (as such regulators populate the Working Party). On the other hand, the same finding shows that it is difficult to enforce the law rigorously in order to influence the data protection behavior of a world-leading Social Network Service player like Facebook. In other words, the efficacy of the law in action is complex, and difficult to anticipate by looking at the law and its enforcing officials in isolation.

In China, the tension between the efficacy of law in action and the optimal standard of legal design is mounting, at least at the outset of the data protection transplantation plan. The incompleteness of data protection law in China is more severe than in Europe, as many of such laws simply are not there at all and most of such laws that exist have been enacted recently. The incompleteness is also more severe in China than in Europe, because law enforcement agencies simply lack the experience that accompanies the adjudication in a substantial number and variety of cases. This is particularly relevant to the MIIT's performance. Under such conditions, mechanisms of

law enforcement cannot be expected to work effectively, at least not during the early period of the data protection institution's development. Thus, Chinese legislators face a predicament: they really need to develop a European type of data protection system, and yet they lack the instruments to do so. Worse yet, recipes for law enforcement that have historically worked elsewhere may not help in the short-to-medium term in China.

Now, I can answer my main research question: "Is China's transplantation plan advisable?" My approach concludes that it is not feasible to solely transplant EU data protection law (as China's transplantation proposal suggests), unless an equivalent to the EU data authorities is included. Chinese Data protection law is less strong than EU privacy law (Chapter 2). However, cultural differences (Chapter 3) and inherent incompleteness of the EU law (Chapter 4), coupled with the fact that institutional arrangements in the EU that reduce incompleteness will not work in China (Chapter 5) make me conclude that of the effectiveness of the an imported European data protection law cannot be expected too much.

In the Second Part of my research project I explore what additional opportunities can be discerned when adopting the perspective offered by complexity theory, and when considering the subject matter of data-protection regulation to be a complex adaptive system (hereinafter CAS). This change of perspective is because the phenomena that I encountered in Chapters 3-5 and that characterize the subject matter for personal-data protection can be summarized with six characteristics: they are networked/connected, they lead to emergent interdependencies, now and then showing path dependent, dynamic, complex and adaptive behavior.

In this Second Part, I first identified the subject matter of data protection law to be a Personal Data Community (PDC). Then, I investigated, through 4 combining the PDC with the knowledge and experiences from different classes of CAS, whether data protection law's subject matter, as a network of data users, exhibits the characteristics of a CAS and what these imply for the future of data protection law. Through using some key CAS-properties and relating them to our PDC and its ecology, we are "informed" that these characteristics apply to the PDC and that thus the PDC can be understood as a CAS. From the CAS perspective, the human-created PDC is a large

and dynamic system of interacting data users networked in a particular pattern of organization from which arises the ability to adapt to internal and external changes by self-organization, emergence and co-evolution/learning.

My findings brought challenges to legal arrangements over data protection issues, since these try to tame a CAS. Evidence taken from case studies published in this book as well as other sources suggested that data protection law's subject matter is (possibly) quite different from other law's subject matters. It faces critical transitions all the time in practice. Thus - as we continuously have to regulate situations that the legislature could (and did) not imagine when framing the law - the purposes of data protection law, the reasons for its existence and the modalities of its regulation are requiring methods quite different from those that focus on the interpretation of material laws.

I suggest that future data protection law may fruitfully build on CAS- theory's recommendations: as Ruhl (1997) minded us, the problems presented in a CAS only can be addressed unless you think like a complex adaptive system. Thus, the problem needing attention is to adjust data protection law to tally with its subject matter. But how?

Multidisciplinary CAS-theory can help legal scholarship to better inform the legislature on expected risks and outcomes of legislative interventions that address CAS-"dots." In this Second Part, I suggested some strategies that can be adopted to help legal researchers capture complex adaptive phenomena in the PDC when arranging or regulatory frameworks. These strategies include: (i) the evaluation of expected benefit of legal intervention, (ii) understanding the environment, (iii) the special functionalities of hubs, (iv) understanding agents' incentives and (v) considering the forces of incentives vs learned behavior. I think that legal scholarship needs to establish and protect its own identity boundaries in multidisciplinary settings by explicitly defending its proper position as addressing autonomous behavior by responsible agents. Where social scientists are on the look-out for knowledge that will nudge such agents into behaving in a way that they want, often unconsciously, legal scholars are interested in knowledge that will support responsible agents to make autonomous behavioral choices, while aware of legal and cultural norms -- of knowledge that can be learned. A legislator will presumably be best informed, I think, when both types of knowledge and their inter-

actions can be made available in a coherent framework. Complexity theory is a serious candidate for providing it.

The picture of the data protection law's subject matter as a CAS is an ongoing rather than completed construction. Notwithstanding that our understandings on CAS theory is in a state of evolution, our efforts thus far have already served to deepen our understanding of many problems that troubled data protection law. And they have operated as checks against some of the mistakes of current data protection laws. It is against this background that I expect that regulation over data-protection issues stand to benefit from being informed through the lens of CAS theory.