WORK AND DIGITALISATION 09.12.2021 | Timo Daum

A Chinese law made in Europe

Inspired by the EU's GDPR, China has introduced a law to protect individuals' personal data. It's another move to rein it the power of Big Tech

On 1 November 2021, the Chinese government introduced a new law that attempts for the first time to comprehensively regulate the storage, transfer, and processing of personal data. The Personal Information Protection Law (PIPL) enshrines the principle of consent for the use and transmission of personal data, impact assessments for the private sphere and security, and the handling of data protection violations. Article 2 states: 'The personal information of natural persons receives legal protection; no organization or individual may infringe upon natural persons' personal information rights and interests'.

Why has the Chinese government decided to take this step now? To date, China has had no comprehensive protection of personal data. The new law closes this gap and thus represents – similar to the European General Data Protection Regulation (GDPR) of 2018 – an important step towards the standardisation, updating, and formalisation of data protection principles.

A number of substantial changes were incorporated in the final version of the law. These range from a ban on algorithmic price discrimination, to a new requirement of data portability and new approaches to cross-border data transfer and processing of the data of minors below 14 years of age. The vigorous debate is far from over, however, because the legislation rather represents a framework – with concrete details remaining to be filled in.

From US regulation to GDPR

At first it seemed that China would take the comparatively minimalistic US regulation as a model in developing its own legislative framework. In the United States, digital regulation is largely a patchwork. 'Historically, in the US we have a bunch of disparate federal [and state] laws', according to data protection expert Amie Stepanovich. Soon, however,

there was a shift towards the European GDPR. The final text, now available in English translation, confirms this trajectory, as broad swathes in the text exhibit similar concepts and even virtually identical formulations.

'This law is actually inspired very much by GDPR', explains Han Xinhua, law professor and member of the cybersecurity committee of Communication University of China. "'The rules are very similar in many ways, such as the definition of personal information, sensitive information processing rules, ..., the obligation to take security measures, preservation (storage) Time limit, personal information protection impact assessment, DPO/personal information protection responsibility system, etc.'

Discussions in China have been going on for years on the necessity and design of user rights in the digital domain.

Because the new law applies to all data collected in China it also concerns foreign firms and institutions active in China. Most companies have already informally oriented themselves to the GDPR standard, according to expert Yiming Hu. But now 'they all need to take a closer look'.

The rejection of the US model and the extensive adoption of the GDPR in the world's most populous country represents something of an export coup for the European Union in the digital economy.

Common prosperity

Discussions in China have been going on for years on the necessity and design of user rights in the digital domain. These debates have taken place in a context in which corruption, arbitrariness, and a lack of rule-of-law structures have been seen as an obstacle to Chinese development. This finds expression in the current 'principal contradiction' in Chinese society. The Chinese Communist Party (CCP) considers this to be between 'unbalanced and unsatisfactory development and people's constantly growing need for a better life'. The 'common prosperity movement' launched by the Party is thus aimed at fostering better governance and a more balanced economy.

This campaign is a response to the gulf that has opened up in recent years between rich and poor, the emergence of a new urban middle class and, not least, the rise of powerful domestic digital companies and rampant corruption in state and Party. The era of Xi Jinping, after all, is characterised by an 'severe and far-reaching anti-corruption campaign', according to sinologists Daniel Fuchs and Frido Wenten.

In recent years the emergence of big digital corporations as 'processors of personal data' has jeopardised social equilibrium. This has complicated relations between the Chinese government and the big firms considerably. Their increasing power has been closely monitored and, when necessary, reined in. For example, in late 2020 the government temporarily halted the initial public offering of the Ant Financial Services Group, an affiliate of the Chinese Alibaba Group.

A range of new digital laws

Han Xinhua explains that a 'three-pillar model' has been created: 'The dual structure of public power-private rights in an industrial society is replaced by a triangle structure of public power-private power-private rights instead. According to her, this development has changed the balance of power in the digital world. She emphasises that in the new power triangle it is important to strengthen individual rights vis-à-vis the other two poles. The new law then also aims to promote these rights. Xinhua emphasises that the law was passed primarily because of 'China's internal pressure', and not because of efforts to accommodate foreign countries or to conform to Western standards.

China's new law inspired by the EU's GDPR really does strengthen individual rights against big digital corporations.

The new law must be seen within the context of a whole series of other laws adopted in recent years in an effort to reframe digital legal space. For example, the Law on Cyber Security came into force on mainland China on 1 June 2017. On 1 September 2021 the Data Protection Law came into force, covering the use, collection, and protection of data in the People's Republic of China.

Zhenbin Zuo, expert on Chinese law at the University of Cambridge, sees both the Cyber Security Law and the Data Protection Law in the context of national security legislation. President Xi Jinping has also emphasised this connection: 'Without cybersecurity there is no national security.'

Article 58 of the PIPL contains a so-called 'gatekeeper provision', which makes platform operators responsible for all practices of third-party providers on their platform. According to Zuo, this forces operators 'self-regulate their third-party suppliers and maintain a good ecosystem of online Apps. This is similar to FTC's requirements on Facebook after the Cambridge Analytica incident.'

The CCP's goals

By contrast, according to Zuo, the recently adopted PIPL is more concerned with protection of individual rights and interests. 'But as explained in the legislative notes for PIPL 2021, it is also largely about promoting corporate interest and growing a national digital economy.'

China's new law inspired by the EU's GDPR really does strengthen individual rights against big digital corporations. For the Party and state leadership, however, it also serves two other purposes: first, it is one element of the campaign against corruption and abuses, and thus is likely to strengthen public trust in institutions; and second, it belongs in the context of a policy of regulating, restricting, and even reining in the digital corporations.

Reinforcing individual data protection rights and curbing the power and data collection frenzy of private and state entities is intended to ensure the frictionless operation of China's digital economy going forward. Within the framework of combating hyper-capitalist excesses, the state is siding with ordinary people, the millions-strong army of digital platform users. In this way, it is killing two birds with one stone: it is reining in the power of the big corporations and positioning itself as the advocate of the new digitally savvy Chinese middle class.



Timo Daum
Berlin

Timo Daum has been a fellow of the research group 'Digital Mobility and Social Differentiation' at the Social Science Research Center Berlin since 2020. He is also a writer and university lecturer in the field of business informatics and digital transformation.