European Parliament

Personal data transfers to China

Developments in online services and cloud computing mean the time has come to pay more attention to the protection afforded to EU citizens when transferring personal data to China.

Background

The European Data Protection Directive 95/46 (and the General Regulation that will replace it from 2018) state that data transfers outside the EU/EEA are allowed only if third countries ensure an **adequate** level of protection of individuals' personal data. When the European Commission finds that a third country respects this condition it adopts an 'adequacy decision' on the basis of all the circumstances surrounding a data transfer operation and the rules in force in the third country in question. As the EU Court of Justice clarified in its 2015 *Schrems* ruling, an adequate protection level must be understood as being essentially equivalent to that in the EU. The extraterritorial protection of EU citizens has shown its limitations in the face of widespread practices such as mass-surveillance in the US and elsewhere, where data can be transferred and stored on local servers. With increasing quantities of data flowing over the internet, and more so via **cloud computing**, ensuring effective data protection is becoming increasingly challenging. While the bulk of attention in Europe to date has been on data flows to the US, transfers to other big market players, such as China, have tended to be neglected, despite the increasing use of Chinese products (e.g. software and devices) and services (e.g. social networks and e-commerce websites) entailing a very large volume of data exchanges.

Data protection in China and EU requirements

The burgeoning economic, political and cultural relations between the EU and China in recent decades are reflected in greater flows of data. As the current literature widely reports, although sectoral data protection laws do exist in China and some legal remedies may theoretically apply to EU citizens, in reality, the legal order seems far from 'adequate' as prescribed by EU law: democratic conditions for the respect of human rights, such as independent courts, legal certainty and adequate means of enforcement cannot be guaranteed in China today. However, an outright prohibition of EU-China data flows would be impractical, as observed in a recent European Parliament study, given the growing use of online services and in particular of China-based cloud computing environments, involving vast data centres to which EU data may flow.

The role of the European Parliament

It seems clear, not least in view of the *Schrems* case, that efforts are needed to make solid deals with China on the protection of EU citizens' data. The European Parliament's Committee on Civil Liberties (LIBE) conducted a mission to China last November in part to discuss data protection issues with local authorities. LIBE used the opportunity to promote the adoption of an extensive personal data protection framework, including a common set of definitions. In its resolution on transatlantic data flows, the EP stressed that 'the Privacy Shield is part of a **broader dialogue** between the EU and third countries ... in relation to data privacy ... and objectives of shared interest', while underlining the need to define a general approach on data transfers to third countries. In the meantime binding corporate rules and standard contractual clauses remain the alternative tools (however, the legality of these tools is being challenged). International free trade agreements may also prove to be defining factors in the future of data privacy laws.

Following the LIBE mission to China, and in light of the broader concerns raised by the *Schrems* case as regards transfers to third countries other than the US, an oral question to the European Commission on how to ensure safe transfers to China will open a debate on the issue scheduled to take place at the June plenary. Next steps may include initiatives aimed at prompting negotiations with China along the lines of Privacy Shield or other arrangements, so as to increase legal certainty over how personal data should be transferred from the EU to China.

EPRS | European Parliamentary Research Service
Author: Shara Monteleone, **Members' Research Service**
PE 583.836