The "medieval" sovereignty on personal data. Considerations on the nature and scope of the EU regulatory model

Alessandro Mantelero, Polytechnic University of Turin

Like a sort of medieval town, the EU common framework on data protection has created a legal wall around the information concerning European citizens and only a few legal gateways give access to the valuable asset represented by personal data: standard contractual clauses, international bilateral agreements, foreign regulations that provide adequate levels of protection, binding corporate rules, ad hoc contractual clauses. In recent time, one of these gateways has been temporarily closed (Safe Harbour), since the judge of the "town" (the European Court of Justice) stated that it was not enough secure (weak enforcement of the Safe Harbour principles, lack of jurisdictional protection for EU citizens, potential risks due to the public/private surveillance partnership).

Without metaphors, the Schrems case apparently reaffirms the strength of the EU legal barrier to protect personal data, but actually unveils the frail nature of this regulatory wall: the ECJ judgment has pointed out the inadequacy and the limits of the different remedies available to legitimate trans-border data flows and, therefore, the frailness of the apparent EU supremacy in protecting personal data.

Against this background, the author discusses the limits of the EU-centric approach adopted by the Directive 95/46/EC and strengthened by the new regulation. On the one hand, binding corporate rules, standard contractual clauses and other solutions are based on the idea that data importers are able to provide an adequate level of protection to personal information. On the other hand, the provisions of third country regulations that have passed the adequacy test should provide an effective protection, which is essentially equivalent to that guaranteed within the European Union. Nevertheless, data importers may be forced by third country regulations to breach their contractual obligations and third country regulations may be overwhelmed by technological innovation or not adequately put into practice.

In the light of the above, the author concludes that the EU provisions on data flows, and on EU data sovereignty, have mainly a declaratory nature, as demonstrated by the more formal than real safeguard of personal data existing in many EU countries and by the lack of control on the enforcement of the contractual solutions for trans-border data transfers. This points out the political nature of the EU data protection regulation, that can be understood only in the broader context of the multi-stakeholder dimension of global data protection, which involves different economic areas (US, EU, China, etc.) and different organizations (COE, APEC, OECD, UN). From this perspective, this legal wall built around EU data, with its effects on international data flows, is the instrument to reinforce the EU leadership in drafting of a future global regulation of data protection, rather than a guarantee of an effective higher standard of protection. This leadership emphasises the protection of personal information as a fundamental right (ECJ, case C-362/14), which overrides the mere economic interests of data gatherers (ECJ, case C-131/12).