

EU CYBER DIRECT RESEARCH SEMINAR

EU DIGITAL SOVEREIGNTY: FROM NARRATIVE TO POLICY?

Friday 18 March 2022, 13:00-17:45 CET
Leiden University (online)

The General Data Protection Regulation through the lens of digital sovereignty

Kristina Irion

This short contribution will present and discuss the European Union's (EU) General Data Protection Regulation (GDPR) through the lens of 'digital sovereignty'.¹ When high-ranking representatives of EU institutions endorsed digital sovereignty this has been interpreted as a signpost for a new-found assertiveness in EU digital policy.² However, digital sovereignty is conceptually fuzzy and is used to animate a wide spectrum of geopolitical, normative, and industrial ambitions.³ In the context of the GDPR it makes sense to operationalize digital sovereignty as the ability of rules to assert authority in a global and interdependent digital ecosystem. Conceived this way, I will reflect on how the GDPR wields transnational capacity by design: Firstly, the rules on transfers of personal data to third countries will be introduced and, secondly, the GDPR's revamped territorial scope of application will be considered. The concluding remarks will reflect on the GDPR's ability to wield transnational authority and its contribution to the EU's digital sovereignty goals.

Rules on transfer of personal data to third countries

EU data protection law sought to ensure that transfers of personal data to a third country cannot be used to undermine statutory protection of natural persons well before digital sovereignty has become valid currency in the EU. Already the GDPR's predecessor, the 1995 Data Protection Directive, contained special rules regulating the conditions under which an EU controller can lawfully transfer personal data to a recipient in a third country.⁴ The GDPR continues this

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L119, 6.

² See e.g.: The German Presidency of the EU Council. (2020). Together for Europe's recovery: Programme for Germany's Presidency of the Council of the European Union (1 July to 31 December 2020). Council of the European Union; European Commission. (2020d, September 16). State of the Union Address by President von der Leyen. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655.

³ See e.g. Tambiama Madiega, 'Digital Sovereignty for Europe' (2020) PE 651.992 <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)>; Kristina Irion and others, 'Governing "European Values" inside Data Flows: Interdisciplinary Perspectives' (2021) 10; Julia Pohle and Thorsten Thiel, 'Digital Sovereignty' (2020) 9 Internet Policy Review <<https://policyreview.info/concepts/digital-sovereignty>>.

⁴ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (no longer in force).

approach and requires that transfers of personal data to third countries adhere to the requirements set out in its Chapter V. It follows that such transfers can only take place:

1. On the basis of an adequacy decision of the European Commission;⁵
2. Subject to appropriate safeguards, notably standard data protection clauses;⁶ or
3. Pursuant to specific derogations that are subsidiary and circumstantial.⁷

Through its jurisprudence the Court of Justice of the European Union (CJEU) has substantially contributed to the interpretation of the GDPR transfer rules. In its judgments *Schrems I* and *II*, the CJEU invalidated twice an adequacy decision adopted by the European Commission that had been the basis for commercial data transfers to the United States.⁸ The Court affirms that the transfer rules are crucially preventing the circumvention of the protection afforded to individuals' personal data under EU law which must be read in the light of the Charter of Fundamental Rights of the European Union (Charter).⁹ The Court clarifies that where contractual safeguards do not suffice to ensure a level of protection that is essentially equivalent to the EU the controller is under an obligation to adopt supplementary measures in order to ensure compliance with that level of protection.¹⁰ As a consequence thereof the GDPR has its mechanisms against circumvention that would render it obsolete.

Territorial scope of the GDPR

The GDPR has chartered new terrain where it expands the territorial scope of application beyond the traditional principle of establishment according to which a controller or a processor must be in the Union. The regulation does also apply to organizations not established in the EU if their processing activities are related to the offering of goods or services to individuals who are in the Union or the monitoring of their behaviour.¹¹ The extraterritorial reach aims to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation.¹² Entities to which the GDPR applies by virtue of the extraterritorial reach are required to designate a representative in the Union.¹³ The revised territorial scope closed another loophole of the GDPR's application which follows yet another landmark ruling by the CJEU.¹⁴

Concluding remarks

In cross-border settings denial of authority that was frequently mounted on grounds of lacking jurisdiction or falling outside of its scope of application in relation to the GDPR rarely

⁵ Article 46(1) GDPR: A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.

⁶ Article 47(1) GDPR: ..., a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

⁷ Article 49 GDPR.

⁸ CJEU, Case C-362/14 (*Maximillian Schrems v Data Protection Commissioner*), ECLI:EU:C:2015:650; Case C-311/18 (*Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*), ECLI:EU:C:2020:559.

⁹ Case C-362/14, para. 73.

¹⁰ Case C-311/18, para. 132f.

¹¹ Article 3(2) GDPR.

¹² Recital 23 GDPR.

¹³ Article 27 GDPR.

¹⁴ CJEU, Case 131/12 (*Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*), ECLI:EU:C:2014:317.

succeed.¹⁵ This can be attributed to a novel regulatory design of the GDPR which is capable of transcending the confines of Westphalian jurisdiction; thereby rendering the regulation a better fit to the digital environment. The requirements for transfers of personal data and the extraterritorial reach are often criticised for their zeal and enforceability, being overly formalistic and even onerous.¹⁶ For the time being and absent of viable alternatives, the GDPR has neither become obsolete nor easy to ignore.

Quite to the contrary, EU approach to personal data protection makes for an idiosyncratic example of the ‘Brussels Effect’.¹⁷ Anu Bradford’s account of EU data protection law and practice finds both a de facto and a de jure Brussels effect.¹⁸ On the one hand, digital multinationals have adopted the EU data protection rules as a quasi-standard for their transnational operations. On the other hand, chores of countries emulate the EU approach to personal data protection in their domestic legal systems. Graham Greeleaf who eminently catalogues the global trend in data privacy laws identifies 145 laws worldwide which are inspired by the EU’s GDPR.¹⁹ Paul Schwartz and Karl-Nikolaus Peifer hold that “EU data protection has been stunningly influential: most of the rest of the world follows it.”²⁰ Arguably, this does not resolve in universal harmony but legal pluralism and contestation of what qualifies as data privacy-preserving flows.

As I argue elsewhere legal institutions are reactive to digital interdependence making legislators as well as courts recognise that domestic laws need to be better equipped for the transnational environment.²¹ Recent EU legislative initiatives appear crucially aware of their exposure to a global digital ecosystem and come piece and parcel with safeguards against inbound and/ or outbound circumvention. Not unlike the GDPR, also future AI regulation would apply to “providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country.”²² Likewise, the proposal for a European Data Governance Act foresees restrictions on cross-border data transfers of non-personal data to third countries that take inspiration from the GDPR.²³ The examples underscore that safeguarding the normative substance of EU regulation in a cross-border setting is a matter of digital sovereignty for the EU.

¹⁵ See for background Hannah L Buxbaum, ‘Territory, Territoriality, and the Resolution of Jurisdictional Conflict’ (2009) 57 *American Journal of Comparative Law* 631.

¹⁶ Svetlana Yakovleva and Kristina Irion, ‘Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade’ (2020) 10 *International Data Privacy Law* 201 <<https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipaa003/5813832>>.

¹⁷ To Anu Bradford the ‘Brussels Effect’ “refers to the EU’s unilateral ability to regulate the global marketplace.” Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2020) 1.

¹⁸ *ibid* 142f.

¹⁹ Greenleaf, Graham, *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance*. (2021) 169 *Privacy Laws and Business International Report*, 1, 3-5.

²⁰ Paul M Schwartz and Karl Nikolaus Peifer, ‘Transatlantic Data Privacy Law’ (2017) 106 *Georgetown Law Journal* 115, 122.

²¹ Kristina Irion, ‘Panta Rhei’ in Mira Burri (ed), *Big Data and Global Trade Law* (Cambridge University Press 2021) <https://www.cambridge.org/core/product/identifier/9781108919234/%23CN-bp-11/type/book_part>.

²² European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM/2021/206 final).

²³ European Commission, Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on European data governance (Data Governance Act), COM/2020/767 final.