# Book Reviews

The Book Reviews section will introduce you to the latest and most interesting books on a wide range of topics pertaining to the law and policy of data protection. For further information on the submission of reviews please contact the Book Reviews Editor Gloria González Fuster at Gloria.Gonzalez.Fuster@vub.be.

*Data Protection, Migration and Border Control: The GDPR, the Law Enforcement Directive and Beyond*
By Teresa Quintel
Hart Publishing 2022, 288 pp.
£85.00; Hardback

*Niovi Vavoula**

Research on the establishment, operation and reconfiguration of European Union (EU) large-scale IT systems for third-country nationals (SIS, VIS, Eurodac, EES, ETIAS and ECRIS-TCN) has heightened in recent years due to increased legislative activity in this area. Though typically developed within specific subfields of EU immigration law -and to an extent EU criminal law-, such as asylum (Eurodac) or visas, the growing convergence of the rules governing their operationalisation and interoperability, have elevated IT systems to a policy field of their own. Despite their inherently technical nature, large-scale IT systems processing data of third-country nationals pose a series of challenges to the fundamental rights to privacy and protection of personal data, as enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights (Charter), as we all as other rights such as the right to effective remedies, rights of the child, and the right to human dignity.

So far, the limited number of monographs that have been published in this field have focused on the right to effective remedies[1] and the rights to privacy and protection of personal data.[2] With the exception of my monograph, these systems have been primarily viewed in isolation.[3] What literature has been missing though is a more data protection focused exercise to understand and position the rules on large-scale IT systems within the broader data protection framework, and assist in determining the applicability of different sets of rules laid down in the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED) and the EU Data Protection Regulation (EUDPR). Teresa Quintel's first monograph aims to fill in this particular gap in the literature, and does so in an excellent manner. The monograph is based on the author's doctoral thesis, which won the Excellent Thesis award in Law from the University of Luxembourg, as well as the 2022 Stefano Rodotà Award[4] of the Council of Europe.

The monograph comprises four chapters, an introduction, and a conclusion. Chapter 1 provides an overview of the developments in the Area of Freedom, Security and Justice (AFSJ) with regard to the right to personal data protection. It maps the struggle between privacy and security in an era when internal border controls have been abolished and the powers of the EU in the field of migration gradually emerged and expanded. The chapter sets the scene by looking into various legal developments, both in the field of data protection and in the field of databases, and the growth in agencies' powers. These involve the data protection reform – after all, the LED is a development building on the Schengen *acquis*. The reform took place amidst the so-called 'refugee

DOI: 10.21552/edpl/2024/1/19

* Niovi Vavoula is a Senior Lecturer at Queen Mary University of London, UK. For correspondence: <n.vavoula@qmul.ac.uk>.

1 See Evelien Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (Martinus Nijhoff 2008); Simona Demkova, *Automated Decision-Making and Effective Remedies: The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice* (Edward Elgar, forthcoming 2023).

2 For a holistic approach to the compatibility of all EU IT systems with the right to respect for private life, see Niovi Vavoula, *Immigration and Privacy in the Law of the EU: The Case of Information Systems* (Briull 2022). With regard to SIS see Stephen Kabera Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation* (Martinus Nijhoff 2008).

3 See Georgios Glouftsios, *Engineering Digitised Borders - Designing and Managing the Visa Information System* (Springer 2021).

4 Council of Europe, '2022 Rodotà Award' <https://www.coe.int/en/web/data-protection/2022-rodota-award> accessed 15 March 2024.

crisis', and the increase in terrorist events in EU Member States which had a catalysing effect in the proliferation of databases: the family of SIS, VIS and Eurodac has doubled to welcome EES, ETIAS and ECRIS-TCN – which are to become interoperable. The author manages to set out the main components of these developments in a concise and easy to understand manner.

Chapter 2 is devoted to understanding the implications of interoperability. The IT systems were initially set up in a compartmentalised manner to respect the separate purposes for which each system had been developed. Quintel explains the four interoperability components – the European Search Portal (ESP), the shared Biometric Matching Service (sBMS), the Multiple Identity Detector (MID) and the Common Identity Repository (CIR), and rightly argues that interoperability challenges the purpose limitation principle. Interoperability 'broadens and then merges originally separated purposes', she states, noting that it facilitates law enforcement access to the databases by allowing it to be a routine process even though the Court of Justice of the EU has argued that law enforcement access is an ancillary purpose. Furthermore, the author dives deeper into the functions of the CIR, which streamlines law enforcement access and allows police authorities for (potentially discriminatory) checks on third-country nationals on national territory. Quintel also explains how the MID, which will store links between different records (for example, when an individual uses multiple identities, or when their data are stored in more than one database for legitimate reasons) expands access to SIRENE Bureaux, despite one of the flagship arguments of the European Commission, according to which interoperability would not affect existing access rights to the underlying systems. Overall, the chapter analyses various challenges to data protection, from purpose limitation to data quality and supervision of the systems.

Chapter 3 provides a scoping exercise of the LED to demonstrate its overly broad scope. This is an important point to make considering that the LED constitutes *lex generalis* for the law enforcement use of IT systems, therefore the contours of its scope determine which data processing activities fall within that scope. In that respect, the chapter first provides an outline of the LED and explains how certain competent authorities under its provisions, such as police authorities or border guards, may be subject to both the GDPR and the LED, thus creating challenges for potential misuse of data protection rules. The purpose of the processing is essential; the purposes for which personal data may be processed may be interpreted at the national level expansively so that the LED would apply instead of the GDPR. The convergence between immigration and law enforcement certainly does not help the case of IT systems, but, as the author states, 'processing carried out in the context of migration management, asylum and border control should generally be governed by the [...] GDPR, as the processing operations [...] are innately of administrative nature'. The chapter proceeds with a more detailed overview on the provisions of the LED to demonstrate the differences from the GDPR: because of these differences, the wrongful application of the LED instead of the GDPR could potentially have negative effects on individuals, such as third-country nationals. Through this analysis the monograph becomes a useful source for data protection scholars who are interested in the scope of protection provided by the LED irrespective of their interest in IT systems.

The final chapter of the monograph is devoted to the processing of personal data in IT systems by EU agencies, primarily Europol, the European Border and Coast (EBCG) Agency, and Eurojust. Chapter 1 already explained how different AFSJ agencies, particularly Europol and the EBCG Agency, can process the personal data stored in interoperable IT systems, for example in the context of hotspots to support Member States in identifying third-country nationals or (in the case of Europol) for law enforcement purposes. Both agencies share a common characteristic: their powers hover in-between migration and law enforcement. Though Europol is a law enforcement agency, its mandate includes the crimes of human smuggling and trafficking in human beings, both of which have a distinct migration flavour. In turn, the EBCG Agency is a quasi-law enforcement agency, which exchanges operational personal data with other EU agencies and national law enforcement agencies. The author analyses the applicable data protection rules, and explores potential loopholes. For example, in the case of the EBCG Agency, the applicable legal framework is the EUDPR, which however contains gaps in respect of the processing of operational personal data in its Chapter IX (eg on transfers and supervision). The Chapter also explores gaps in data protection in respect of the pro-

cessing by Europol (eg with respect to biometric data, an issue that only the latest Europol reform addressed).

Overall, as a scholar whose research interests lie in both immigration and data protection law, I really enjoyed reading this book. It brings to the fore fundamental questions about the nature of IT systems and the effect of making them interoperable. It also demonstrates how the blurring of the boundaries between immigration and law enforcement has a distinct collateral effect on the application of different sets of data protection rules. Ultimately, the book could be seen not only as a critique on the fragmentation of the EU data protection framework, exemplified through the case of IT systems for migration, asylum and border management, but more broadly as a warning to the Member States and the EU Agencies implementing the legal framework on IT systems and their interoperability, as well as the supervisory authorities entrusted with oversight tasks. As demonstrated in the previous paragraphs, the monograph will be of interest to both data protection scholars who are broadly interested in the processing of personal data in the law enforcement context and to migration scholars who are interested in getting acquainted with the IT systems. The book does not aspire to provide a comprehensive account on the systems, but it does manage to make the reader think about the potential data protection breaches due to the complex legal framework of the IT systems and the general data protection legal framework. Ultimately, the monograph serves as a reminder of what the European Data Protection Supervisor (EDPS) has pointed out: that so long as migration continues to be treated as a 'problem', the rights to privacy and data protection enjoyed by third-country nationals will continue to be suspended at EU borders.[5]

5 Wojciech Wiewiórowski, 'Privacy and data protection too often suspended at EU borders' (*Euractiv*, 27 January 2023) <https://www.euractiv.com/section/data-privacy/opinion/it-is-time-to-tear-down-this-wall/> accessed 15 March 2024.

DOI: 10.21552/edpl/2024/1/20

* Dr Diana Sancho is Associate Professor of Law, University of Westminster, London. For correspondence: <D.Sancho1@westminster.ac.uk>.

## *Delimitación del derecho aplicable en el Reglamento 2016/679: Tutela jurídico privada de la protección de datos*

by Elena Rodríguez Pineau and Elisa C. Torralba Mendiola
Tirant Lo Blanch 2023, 350 pp.
€35.00.

*Diana Sancho**

In addressing the regulatory needs of our intricate digital and data-driven economy, data protection laws increasingly rely on private remedies to attain public objectives. The General Data Protection Regulation (GDPR), which constitutes the overarching standard for regulating the processing of personal data and whose solutions inspire data protection regulations beyond Europe, is no exception.

In Chapter I of the book *Delimitación del derecho aplicable en el Reglamento 2016/679: Tutela jurídico privada de la protección de datos* ('Delimiting applicable law in Regulation (EU) 2016/679: Private enforcement of data protection'),[1] Professors Elena Rodríguez Pineau and Elisa Torralba Mendiola, distinguished experts in private international law, meticulously examine the hybrid nature of the GDPR. While this hybrid nature contributes to the success of the GDPR, it also poses challenges to the Regulation in achieving its goals: ensuring a high level of protection for the fundamental right to data protection as outlined in Article 8 of the Charter of Human Rights and in Article 16 of the Treaty on the Functioning of the European Union (TFEU), as well as facilitating the free movement of personal data within the European Union.

The book focuses on choice-of-law conflicts arising in data protection law, when the GDPR rules apply to regulating cross-border data processing relationships simultaneously with rules from other sources. To deal with these conflicts, including the gaps in regulation arising from the GDPR, the authors have recourse to the mechanisms and tools available in private international law, which they employ to evaluate how much they contribute to meeting the GDPR objectives. This leads to a book that addresses a crucial gap in the literature and makes a substantial and meaningful contribution to advancing knowledge in this area through innovative and creative proposals.

The authors use the following criteria to guide their analysis. Firstly, the choice-of-law conflict is cat-

1 Elena Rodríguez Pineau abd Elisa C. Torralba Mendiola, *Delimitación del derecho aplicable en el Reglamento 2016/679: Tutela jurídico privada de la protección de datos* (Tirant Lo Blanch 2023).

egorised as either intra-European or extra-European. The former occurs because the opening clauses of the GDPR delegate the regulation of aspects of the data protection relationship to Member State law. The latter situation arises when elements of a data protection relationship are regulated by the GDPR, which applies extraterritorially, and the laws of third countries. Extra-european conflicts can also happen when a dispute in Europe falls outside the scope of the GDPR. Secondly, the authors consider the nature of the protection delivered, whether administered by data protection authorities or not. Lastly, the book thoroughly analyses choice-of-law conflicts of a private law nature that may arise in data protection relationships between relevant actors (data subjects, controllers and processors).

This results in five chapters structuring the book: Chapter I serves as an introduction; Chapter II explores dimensions of the choice-of-law conflicts between data protection authorities; Chapters III and IV analyse choice-of-law conflicts arising in data protection relationships of private law nature; and finally, Chapter V recapitulates and concludes.

In Chapter II, intra-European conflicts are evaluated first. The authors argue that the cooperation mechanisms among authorities outlined in the Regulation only sometimes provide sufficient legal certainty in identifying the relevant authority or applicable law. For this reason, they propose, as a more suitable solution, the application of the law of the establishment of the data controller in the European Union (or, if the controller does not have an establishment in the Union, the law of the Member State where the goods and services are offered, or where the monitoring of behaviour takes place under the conditions in Article 3.2 GDPR). In the event of extra-European conflicts, when the dispute at issue falls outside the scope of the GDPR, the solution that the authors recommend consists of relying on the relevant provisions of national law adopted by the Member states to complement the GDPR. However, they also acknowledge the difficulties this proposal presents if the territorial scope of application of the national law at issue merely aligns with that of the GDPR. This is the case of the national data protection law in Spain. For this reason, they advocate amending the choice-of-law rule in this national instrument to incorporate an additional connecting factor, such as the residence of the data subject in Spain.

Concerning the intra-European conflicts between the laws of different Member States, Chapter III innovates by proposing the application of the law of the Member State where the centre of the data subject's interests is located. The authors' proposal unfolds in two stages: firstly, in section II, they argue for the necessity of a choice-of-law rule tailored to data protection law, rejecting the use of the general solutions in Regulations Rome I and Rome II on the applicable law to contractual and non-contractual obligations. Subsequently, in section III, the authors justify the existence of an implied choice-of-law rule in the GDPR that supports the law of the Member State of the centre of the data subject's interests. The authors welcome the application of this law, which was adopted by the CJEU in cases C-509/09 and C-161/10 *eDate & Martinez*, as a well-suited solution to meet the needs of the GDPR. This solution has its challenges, though. As the authors acknowledge, difficulties may arise, such as the mosaic effect that this rule creates when the centre of interests cannot be determined.

Chapter III also deals with the conflicts arising when a data protection dispute of a private law nature in Europe falls outside the scope of the GDPR. In this instance, the authors propose applying the law of the country where the controller is established as a coherent solution aligned with the GDPR's rationale and the interests at stake. In evaluating contractual mechanisms for the international transfer of personal data to countries that lack equivalent protection to that of the GDPR, the authors explore the option of applying the GDPR as a mandatory rule. This approach aims to safeguard the rights of data subjects under the GDPR, including, for instance, the right to compensation in its Article 82. This proposal contributes to ensuring data subjects a high level of protection, but it presents challenges. As the authors acknowledge, enforcing European data protection rights may be complex in foreign States. After all, despite their influential position, the standards of the GDPR do not apply globally.

Private law aspects of the relationships between controllers and processors, on the one hand, and individuals and data processing actors (controllers and processors), on the other hand, are further analysed in Chapter IV. Particularly interesting are the determinations concerning the application of the right to compensation in Article 82 to choice-of-law conflicts within the EU. Here, the authors advocate for apply-

ing the law of the centre of the interests of the data subject, though they also acknowledge the difficulties concerning implementing this rule in collective actions.

To conclude, Professors Elena Rodríguez Pineau and Elisa Torralba Mendiola's work presents a variety of captivating proposals, contributing significantly to advancing our understanding of this complex topic. It demonstrates how the reliance on mechanisms in private international law, despite the differing legal rationales informing their solutions compared to those inspiring European data protection law, can contribute to achieving GDPR goals. More than anything, the book emphasises the necessity to build bridges across disciplines to meet the challenges of our digital society, a need that the adoption of the Artificial Intelligence Act has further exacerbated. This, in fact, offers an opportunity to explore such multidimensional facets of knowledge further to create better regulatory responses.