This is an Accepted Manuscript of Edoardo Celeste et al, Data Protection and Digital Sovereignty Post-Brexit: An Introduction, in Edoardo Celeste, Roisin Costello, Edina Harbinja and Napoleon Xanthoulis (eds), Data Protection and Digital Sovereignty Post-Brexit (Hart 2023), 1-10, https://www.bloomsbury.com/uk/data-protection-and-digital-sovereignty-postbrexit-9781509966486/

1

Data Protection and Digital Sovereignty Post-Brexit: An Introduction

Edoardo Celeste, Róisín Á Costello, Edina Harbinja, Napoleon Xanthoulis

I. The legal context: the UK as a third country

The United Kingdom's decision to withdraw from the EU generated manifold disruptive effects in economic, social and legal terms, and on both sides of the Irish Sea as well as between these islands and mainland Europe.[1] Digital affairs have not been exempted from this disruption. With Brexit, the UK has left a group of states which is among the most advanced globally in protecting personal data, and which is currently at the forefront of legal innovation in regulating online content, services and disruptive digital technologies including artificial intelligence-based tools.[2]

The volume, and the contributions within it, speak to the embeddedness, and the prominence, of digital affairs - and data protection in particular, not only in relations between the European Union and third-party states but also in the constitutional architecture and regulatory thinking of the Union and its Member States. This emphasis on data protection as both a constitutional value and a right that influences external relations makes data protection particularly important in a post-Brexit landscape. Perhaps nowhere is this more clearly illustrated than in the relations between the United Kingdom and Ireland where data protection and the adequacy of the United Kingdom's data protection laws following Brexit have the potential not only to negatively impact intelligence sharing, trade and cross-border co-operation more generally but also compliance with the Good Friday Agreement itself. The result is that ensuring the adequacy of the UK's data protection (and privacy) laws post-Brexit is not only a legally complex and economically consequential matter – but also one which is politically charged.

Following Brexit, the UK has become a 'third country' from a data protection perspective, meaning that personal data cannot be freely transferred from the EU to the UK absent a specific

[1] For a comprehensive overview of the topic see Federico Fabbrini (ed), *The Law & Politics of Brexit* (Oxford University Press 2017); Federico Fabbrini (ed), *The Law & Politics of Brexit: Volume II: The Withdrawal Agreement* (1st edn, Oxford University Press 2020); Federico Fabbrini (ed), *The Law and Politics of Brexit. Volume III: The Framework of New EU-UK Relations* (First edition, Oxford University Press 2021); Federico Fabbrini, *The Law and Politics of Brexit. The Protocol on Ireland/Northern Ireland* (1st edn, Oxford University Press 2022).

[2] See Edoardo Celeste, 'Data Protection' in Federico Fabbrini, *The Law & Politics of Brexit: Volume III* (Oxford University Press 2021).

legal mechanism, in line with the requirements of the EU General Data Protection Regulation (GDPR). Indeed, the GDPR is directly applicable in all EU member states and in the three countries composing the European Economic Area (EEA), i.e. Iceland, Norway and Liechtenstein. Data transfers occurring among these countries are not subject to any type of restriction, while transfers to third countries, a group which now includes the UK, may occur if one of the conditions listed in Chapter 5 GDPR is met.[3] The most comprehensive mechanism allowing data transfers from the EU to a third country consists in the adoption of a decision by the EU Commission declaring that the legal framework of the third country offers an 'adequate' level of data protection. According to Article 45 GDPR and in line with the case law developed by the Court of Justice of the EU (CJEU), the assessment of the Commission should not be limited to the foreign country's legislation on data protection but should look at the legal framework in general, including areas that might have an impact on the protection of personal data, such the possibility of law enforcement authorities to access personal data transferred from the EU.[4]

In June 2021, the EU Commission adopted two decisions – one covering data transfers under the GDPR and one transfers under the Law Enforcement Directive – declaring that the UK data protection regime offers an adequate level of protection, thus allowing for the transfer of personal data from the EU to the UK.[5] This set of decisions prevented the possibility of a sudden stop to data transfers to the UK. Indeed, the exit of the UK from the EU – and thus its acquisition of the third country status – occurred on 31 January 2020. Until the end of December 2020, data transfers between the two jurisdictions were allowed as if Brexit did not occur in light of a legal arrangement during what was called the 'transition period'. The Trade and Cooperation Agreement (TCA) signed on 30 December 2020 introduced a further grace period of six months – ending on June 2021 – during which the UK could still be considered as an EU member state from a data protection perspective and the EU Commission could have the time to assess UK law with the perspective of adopting an adequacy decision.[6]

II. Towards a new UK data protection model?

Despite the UK's longstanding membership with the EU and the *de facto* alignment of UK data protection law with the EU GDPR at the time of Brexit, the EU Commission's decision to adopt an adequacy determination *vis-à-vis* the UK was vocally contested. Objectors pointed in particular to the architecture of UK national security law, which has been repeatedly judged both by national and European courts as failing to align with fundamental rights standards, as

[3] See Christopher Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5 International Data Privacy Law 235.

[4] See Maria Tzanou, 'European Union Regulation of Transatlantic Data Transfers and Online Surveillance' [2017] Human Rights Law Review <https://academic.oup.com/hrlr/article/3061949/European> accessed 30 March 2021; Maria Tzanou, 'Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights' in Federico Fabbrini, Edoardo Celeste and John Quinn (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart 2021); Federico Fabbrini, Edoardo Celeste and John Quinn (eds), *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart 2021).

[5] EU Commission, Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom; EU Commission, Commission Implementing Decision (EU) 2021/1773 of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom.

[6] For a more detailed reconstruction of the provisions of the TCA related to data protection, see Celeste, 'Data Protection' (n 2).

an issue of concern.[7] This circumstance alone would suffice to argue that there is a serious risk in terms of the sustainability of the newly adopted adequacy decision – a risk which now exceeds mere academic speculation following the recent case law of the Court of Justice of the EU that invalidated, for the second time, the EU Commission's adequacy decision adopted in relation to the United States.[8]

One might think, in these circumstances, that the precarious equilibrium created by the adequacy decision would cause the UK to desist from introducing new regulations in the digital field that could threaten its adequacy status vis-à-vis the EU, especially in light of the strategic and economic importance of data exchanges with EU member states. Yet, in September 2021 the UK Government published a consultation document that included the blueprint of a new model for data regulation, not accidentally entitled 'Data: a New Direction', in which the UK Government proposes its vision to emancipate UK law from the bureaucratic aspects of EU law, give new economic elan to the UK digital economy and lay the basis to make the UK a global champion in the tech sector.[9] The answers to the consultation later informed a new piece of legislation presented on 18th July 2022, the Data Protection and Digital Information Bill, whose parliamentary discussion has been momentarily suspended amidst the recent political turmoil in the UK.[10]

On the one hand, the departure from the EU offers to the UK the possibility to reacquire its legislative sovereignty in the digital field, as much advocated in the Brexit rhetoric. On the other hand, adopting a new regulatory model governing data protection – and digital technologies more broadly – pose new challenges both internally and from a cross-border cooperation perspective. Firstly, because departing from the EU data protection model concretely means challenging a framework to which the UK has so much contributed as a member state over the past three decades. Concepts, principles, and processes that are embedded in the UK data protection sector now risk being unilaterally changed for political purposes or in the name of revitalising the UK economy after Brexit. Will this restyling of UK data protection law succeed in its objective of making the UK more economically attractive as well as removing barriers to innovation?

Secondly, because the consequences of this choice are not limited to the UK context but contribute to exacerbate existing tensions between various countries' willingness to protect their digital sovereignty. The EU aims to continue to be a global standard setter in the data protection field. Protecting the EU digital sovereignty also means preserving the EU ideal of fundamental rights compliant development of technology.[11] The UK, by departing from the EU, seeks to compete on the international plane against superpowers in the tech sector such as

---

[7] See ibid; Edoardo Celeste, 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios' (2019) 15 European Constitutional Law Review 134. See also Santatzoglou and Tzanou in this volume.

[8] See *Facebook Ireland and Schrems* [2020] CJEU C-311/18, ECLI:EU:C:2020:559; Tzanou, 'Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights' (n 4).

[9] UK Department of Digital, Culture, Media and Sport, 'Data: A New Direction' (2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf>; UK Government, 'Data: A New Direction - Government Response to Consultation' <https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation> accessed 22 August 2022.

[10] UK Parliament, 'Data Protection and Digital Information Bill' <https://bills.parliament.uk/bills/3322> accessed 22 August 2022.

[11] See Edoardo Celeste, 'Digital Sovereignty in the EU: Challenges and Future Perspectives' in Federico Fabbrini, Edoardo Celeste and John Quinn (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart 2021).

the US and China, on the one hand, and against the EU, on the other hand. Yet, the UK is still linked to the EU from a data protection perspective by the adequacy decisions allowing data transfers between the two jurisdictions. This umbilical cord keeps the UK within the EU orbit as severing it would mean losing access to huge amount of EU personal data. Concretely speaking, the adequacy status prevents the UK from departing radically from EU data protection law for the fear of losing this special position.[12] And at the same time this means not being fully sovereign in the digital sector, always having to assess whether a reform would eventually lead to the loss of the adequacy status.

This edited volume aims to investigate the challenges and implications of the latest UK law and policy strategies in the data protection field – and in 'neighbouring' regulatory areas that have an impact on data protection, such as AI or online safety regulation. The book analyses the UK's data protection status after Brexit and reflects on the consequences of the emergence of a new data protection model in the UK. The volume also seeks to offer the reader an analysis which incorporates digital sovereignty concerns, examining emerging tensions both at national level and on an EU cross-border basis as they have been raised (or exacerbated by) Brexit. Beyond data protection and cross-border data transfers, the volume also considers broader questions of digital regulation, including digital sovereignty and the 'Brussels Effect' and the importation of regulatory and rights standards beyond the borders of the EU. In doing so, the authors analyse the data protection law reform proposals and other technology law reforms in the UK (namely online safety, AI regulation, human rights law reform), which, combined, may affect the UK data protection adequacy and the broader UK – EU political and economic relationship. Many authors thus exemplify and assess the legal, political and economic effects of regulatory convergence and divergence between the UK and EU. In all, the volume argues for a more robust and coordinated international cooperation on data protection and digital regulation more broadly, including the collaboration between various relevant digital and data protection regulators in the United Kingdom and the EU.

III. Building on the Cross-Border Data Protection Network project

This edited collection is the result of the 'Cross-Border Data Protection Network' project, which was jointly funded by the Irish Research Council and the UK Economic and Social Research Council and aimed to create a multistakeholder network investigating the challenges of vindicating data protection rights after Brexit. Over two years (2020-2022), the network organised five events bringing together prominent academics, civil society leaders, and public actors to engage with the challenges to data protection law caused by Brexit within the UK and on a cross-border basis between the UK, Ireland and, more broadly, the EU. The network involved three partner organisations, Dublin City University, the University of Southampton (formerly the University of Portsmouth) and Aston University, and two associate partners, King's College London and the Institute of Advanced Legal Studies.

The volume includes a selection of the scholarship generated by the network's members during this two-year process, collecting reflections on data protection law in a post-Brexit UK, the impacts on British legislative sovereignty of EU data protection law, the influence of Brexit on national privacy laws within the UK, and the broader socio-political and economic results of the changing data protection and technology regulation landscape between the UK and Ireland and the UK and EU.

[12] See Celeste, 'Data Protection' (n 2). See also Santatzoglou and Tzanou in this volume.

IV. Structure of the book

The book is divided into four parts. Part 1 critically assesses the potential directions of a new UK post-Brexit regulatory strategy in the digital field, starting with an analysis of Data Protection and Digital Information Bill. One of the core points examined by the contributors in this first part is whether and to what extent it will be possible for the UK to find an innovative way of regulating data without significantly departing from the existing EU regulatory model thus jeopardising its adequacy status. In Chapter 2, entitled 'Post-Brexit UK data protection – staying the course or charting a new direction?', Karen Mc Cullagh analyses how the planned Data Protection and Digital Information Bill would align with the requirements of the EU adequacy status. While the Bill aims to update and simplify the UK data protection framework in order to enable economic growth, McCullagh argues that multiple amendments proposed in the bill mean that the 'UK GDPR' would looks quite different to the EU version thus increasing the risk that the EU might question the 'adequacy' of the UK regime for the purposes of data transfers.

In Chapter 3, entitled 'Brexit and data protection law: A missed opportunity for innovative reform?', Henry Pearce shifts to consider how a departure from the European Union might offer the United Kingdom an opportunity to think differently about data protection and argues that personal data may not be the most suitable conceptual hub on which to base the regulation of contemporary data-handling activities. In light of this – Pearce argues – Brexit could be seen as an opportunity to locate a potential alternative approach to data protection law based on the notion of information harms. This approach – he argues – would result in a more granular way to regulating data processing activities as part of which the application of legal rules would be dependent on the contextual peculiarities of specific data uses. This would, in turn, allow for the law to move beyond the categories of personal data and anonymous data established in EU law and adopt a more responsive approach to data protection.

Part 2 of the book continues this analysis, focusing on the law enforcement and national security sectors. The contributions to this section map how data exchange regimes in the law enforcement context have changed post-Brexit and examine the extent to which current UK law regulating the use of data by law enforcement and national security agencies can still be considered to offer an adequate level of data protection. Paradoxically, when the UK was part of the EU, UK national security law fell largely outside the scope of EU law and consequently outside the scrutiny of the CJEU. However, as the contributors to this part note, the UK having acquired the status of a 'third country' from a data protection perspective, now confronts a situation in which the UK regime regulating access to and use of data by law enforcement and national security authorities is one of the core elements to be assessed when determining whether the UK offers an adequate level of data protection, in line with the requirements of the GDPR. The contributors highlight how, in light of the peculiarities of the UK national security and law enforcement regimes, the equilibrium of the recently adopted UK adequacy decision is precarious, drawing in particular on recent case law from the Court of Justice of the EU and the European Court of Human Rights.

In Chapter 4, 'Counter-terrorism, information sharing and law enforcement cooperation post-Brexit', Christine Andreeva explains that the EU counter-terrorism apparatus was being redesigned in light of security threats and political pressures within the Union while the UK began the process of exiting the EU. This circumstance made both negotiating parties even more aware of the mutual benefit of an EU-UK partnership in this field, and lead to very specific arrangements being negotiated between the parties. Andreeva particularly examines the Trade and Cooperation Agreement (TCA) in the area of law enforcement cooperation and information exchange, and, by comparing it to the previous EU instruments in this domain, it

reflects on the long-term consequences of Brexit on cross-border counter-terrorism cooperation between the EU and the UK. Andreeva stresses that this new arrangement is 'unprecedented with regard to a non-EU and non-Schengen third country'. As the TCA could never match the extent of law enforcement and judicial cooperation of the UK at the time of its EU membership, the new arrangements are considered as a step back when it comes to information-sharing.

Chapter 5, written by Sotirios Santatzoglou and Maria Tzanou, complements this analysis by focusing on UK internal national security laws. Their contribution, 'An (in)adequate data protection regime after Brexit? Bulk surveillance powers, national security and the future of EU-UK data transfers' opens with a historical analysis of the UK criminal policy that led to the consolidation of UK mass surveillance practices, in particular highlighting the influence of political strategies – from both sides of the political spectrum – in enhancing crime control through surveillance in the UK. The second part of the paper stresses how, paradoxically, after Brexit, national security matters have become the rationale for an increased EU review of the UK legal framework in the context of transborder data transfers. Regrettably – Santatzoglou and Tzanou argue – after the UK's departure from the EU, the UK will no longer have an explicit fundamental right to data protection in the UK and the Charter of Fundamental Rights of the EU will apply extraterritorially in the field of law enforcement and national security, but not in relation to all types of data processing. However, in light of its historico-political analysis the chapter concludes that bulk surveillance powers will not be removed and this thus represents one of the main vulnerabilities of the UK adequacy status.

Moving to the more quotidian deployment of surveillance in the name of national security, in Chapter 6, ''Serious and Systemic'? Live facial recognition technology in the United Kingdom and its impact on adequacy', Allison M Holmes examines how domestic regulation of facial recognition technology – and, in particular, live facial recognition (LFR) in the UK – could impact any adequacy decision. Ultimately, Holmes concludes that the arrangements governing LFR in the UK represent a clear divergence from EU standards governing the use of personal data and the vindication of fundamental rights.

Part 3 of the book turns to address the diverse manners in which data protection is affected through disparate pieces of legislation within the UK legal order. This part of the book is concerned, in particular, with two major areas of reform on which both the EU and the UK are actively, and heavily, engaged – namely, artificial intelligence and online safety. The contributions to this part explain how data protection law informs regulatory strategies in these two interlinked areas and analyse the extent to which new policies in the field of artificial intelligence and online safety are simultaneously shaping the evolution of data protection law. As the contributors examine, both the EU and the UK have declared their intention to become leaders in the field of artificial intelligence and prioritised online safety as an area of particular concern. This requires both a complex co-regulation strategy between regulators and private companies and a clear delimitation of the admissible use of artificial intelligence technology in particular. The result, the contributions argue, is a regulatory race between the EU and the UK, motivated by a mix of economic interests and fundamental rights protection justifications.

In Chapter 7, entitled 'Regulation vs innovation? A comparative analysis of EU and UK policy responses on Artificial Intelligence', Lilian Mitrou examines from a comparative perspective the current attempts to regulate artificial intelligence in the UK and the EU. In this context, the chapter contextualises this analysis within the cross-border data protection related concerns and challenges generated by Brexit and the recent proposals of the UK government to depart from the EU standards and establish a new data model. Mitrou's examination is based on the Proposal for an AI Act submitted by the European Commission on 21 April 2021 and the strategy and policy papers on AI published until August 2022 by the UK Government. Mitrou

analyses the need for regulating AI and discusses the advantages and challenges of transitioning from the ethical guidelines on AI to regulation. She highlights the difficulty to define what AI is in a sufficiently flexible and future proof manner, and compares the main regulatory priorities of EU and UK, examining the at first sight dichotomic couple of fundamental rights protection vs innovation. Finally, her chapter concludes reflecting upon the timing of the current regulatory proposals and on the role of AI regulation as tool for setting global standard and protecting digital sovereignty.

Chapter 8, by Edina Harbinja, expands the horizon of research, starting exploring the relationship between data protection regimes and other sectors of technology regulation. Her chapter, titled 'Regulatory divergence: The effects of UK technology law reforms on data protection and international transfers' examines examples of ongoing law reforms in technology law in the UK, discussing their effects on data protection and commercial data transfers. In particular, the chapter assesses implications of the regulation of online safety and AI in the UK, questioning their effect on the UK data protection regime and its adequacy status. The chapter challenges these reforms on the basis of their mutual divergence and inconsistency. It concludes that these proposals should be considered holistically. Otherwise, a piecemeal reform could lead to unintended and adverse consequences, not only on the enforceability of these proposals but also on the UK's data protection adequacy and, notably, data protection and privacy rights of individuals in the UK.

Part 4 contextualises the developments analysed in the first three parts of the book by adopting digital sovereignty as an interpretative lens. The contributions in this part explain how, on the one hand, EU data protection law aims to ensure an adequate level of protection both within the territory of the Union and in circumstances when data is transferred to a third country such as the UK. This implies that the UK, even after Brexit, will be subject to a significant Brussels effect in the digital field lest it risk losing its adequacy status. Equally, the UK has justified Brexit both prior to and following the public vote to effect its terms, by reference to a need for increased legislative sovereignty, as demonstrated by its recent reform proposals in the digital sector. The question remains, however, of whether the choice to depart from the EU data protection model is merely motivated by short-term economic interests (what contributors call digital 'sovereignism') but will, *de facto,* betray the United Kingdom's long-standing support for digital rights, as actively demonstrated in the past fifty years while it was an EU member state. The book will conclude with an analysis of the cross-border cooperation mechanisms that will help prevent future regulatory friction between the EU and the UK, and which may offer the basis for joint development of regulatory solutions in the digital field.

In Chapter 9, 'The Brussels Effect: Regulatory Standard-Setting and Constitutional Conflicts in Post-Brexit Privacy Law', Róisín Á Costello critically examines how EU values are exported through regulatory standards as part of the so-called 'Brussels effect.' The chapter argues that importing regulatory standards may now result in an unintended importation of rights standards, and, crucially, it may also mean that such a dual importation must take place to satisfy the requirements of the GDPR following the *Schrems II* case. As such, the UK, if it seeks to adopt a new data protection model that still meets the EU adequacy ruling, is required to critically examine the congruence of its own national constitutional tradition with European privacy values. Costello concludes by arguing that this raises particular challenges for the UK, given its progressive attempts following Brexit to shed or minimise the influence of EU law and the jurisprudence of the ECtHR.

Chapter 10, by Edoardo Celeste, builds on this analysis and specifically explores the implications of recent UK government announces concerning the reform of data protection from a digital sovereignty perspective. His contribution, 'Brexit and the risks of digital

sovereignism', recontextualises recent UK regulatory and policy moves as part of ongoing clashes concerning digital sovereignty between the EU and the UK. The chapter analyses the risks and limits of the digital sovereignty claims, questioning whether they are degenerating into a form of 'digital sovereignism', backed by economic protectionism instances and guided by economic interests. Celeste concludes on the core question of whether announced UK data policies denote a mere marketing strategy or rather provide evidence for a more serious constitutional value crisis. To avoid an economic war and 'a digital sovereignty arm-wrestling', Celeste argues that the solution is to foster international cooperation on data protection and digital regulation more broadly, to understand its core objectives and how they can be achieved while supporting the plurality of values and technical innovation.

Chapter 11 entitled 'Towards a successful cross-border regulatory cooperation', by Peter Hustinx, former EU data protection supervisor, concludes the volume by analysing the potential mechanisms to ensure effective regulatory cooperation on both sides of the English Channel. His contribution looks at the scope for institutional cooperation in the post-Brexit context by the authorities responsible for the supervision and enforcement of data protection laws in the UK and the EU. In doing so, it first sets out how the UK Information Commissioner's Office (ICO) has invested in developing a global framework for regulatory cooperation in the context of the Global Privacy Assembly and the results of these efforts so far. It then discusses a few alternative frameworks and their current practice, notably in the Council of Europe, the OECD and the European Union context. Against this background, the chapter examines how such regulatory cooperation between the UK and EU member states – at a regional scale or in bilateral settings – is currently or could be organised in the future, illustrating some critical conditions for success. Hustinx concludes by arguing that UK adequacy will continue to play a vital role, not only as a precondition for a successful cross-border regulatory cooperation but also in a much larger context.