This is an Accepted Manuscript of Edoardo Celeste, Brexit and the risks of digital sovereignism, in Edoardo Celeste, Roisin Costello, Edina Harbinja and Napoleon Xanthoulis (eds), Data Protection and Digital Sovereignty Post-Brexit (Hart 2023), 181-198, https://www.bloomsbury.com/uk/data-protection-and-digital-sovereignty-postbrexit-9781509966486/

Brexit and the risks of digital sovereignism

EDOARDO CELESTE*

I. Introduction

Regaining sovereignty from the EU was a mantra of the Brexit campaign.[1] The Eurosceptic slogan 'let's take back control' referred to an alleged erosion of sovereignty and supremacy of the powers of the UK Parliament by EU institutions.[2] Before the Brexit referendum, in a last attempt to reconcile UK sovereignty claims and its status as an EU member state, UK Prime Minister David Cameron even proposed the idea of a 'Parliamentary Sovereignty Act', a plan that was soon dismissed as only a definitive departure from the EU would have achieved its objectives.[3] The EU, its laws and institutions were perceived as hampering the socio-economic development of an independent and sovereign UK, which relied on a century-long democratic tradition. However, it was clear that to regain that coveted independence a polite handshaking between former partners would not have sufficed. Especially in light of the complexity of the issues to be solved, plugging off the cable from the EU family could not be an overnight change.[4] As expected, the Brexit process resulted to be more akin a suffered divorce.

The post-Brexit restructuring of UK law in the digital field did not attain the headlines amid even more challenging legal issues to face. One can argue that, in a first phase, the UK limited itself to an ordinary, or consequential, reordering of its digital law following the departure from the EU. Ordinary in the sense that no extraordinary amendment to UK law was introduced in

* Assistant Professor in Law, Technology and Innovation and Programme Chair of the European Master in Law, Data and AI (EMILDAI), School of Law and Government, Dublin City University, Ireland.

[1] See Keith Ewing, 'Brexit and Parliamentary Sovereignty' (2017) 80 The Modern Law Review 711; Graham Gee, 'Regaining Sovereignty? Brexit, the UK Parliament and the Common Law' [2016] European Public Law 131; Michael Gordon, 'The UK's Sovereignty Situation: Brexit, Bewilderment and Beyond …' (2016) 27 King's Law Journal 333.

[2] Juliette Ringeisen-Biardeaud, '"Let's Take Back Control": Brexit and the Debate on Sovereignty' (2017) 22 Revue française de civilisation britannique <http://journals.openedition.org/rfcb/1319>.

[3] See Gordon (n 1); Ben Wellings and Emma Vines, 'Populism and Sovereignty: The EU Act and the In-Out Referendum, 2010–2015' (2016) 69 Parliamentary Affairs 309.

[4] 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).

the digital field following the Brexit referendum. All changes were dictated as a necessary consequence of the loss of legal force of EU law following Brexit and as the exercise of national regulatory prerogatives delegated by EU law itself. For example, through the introduction of the European Union (Withdrawal) Act 2018, the EU GDPR was retained into UK law through a mere relabelling, now being known in domestic law as the UK GDPR.[5]

Despite a series of pre-existing structural issues in the British legal system,[6] the substantial maintenance of the integrity of UK law in the data protection field led to the adoption by the EU Commission of a decision determining the adequacy status of the UK data protection regime.[7] Such a recognition has allowed for the continued flow of personal data across the English Channel after the UK's departure from the EU, and more precisely after the end of the transition period agreed by both parties in the Trade and Cooperation Agreement (TCA), and finishing in June 2022.[8] However, after the seminal *Schrems I* case decided by the Court of Justice of the European Union (CJEU) in 2015, adequacy decisions are not determinations regarded to be set in stone but are conversely subject to regular monitoring to verify the subsistence of the conditions allowing for a safe transfer of personal data to the third state concerned.[9] Consequently, it was not expected that the UK would have introduced significant changes in its data protection regime lest it loose an adequacy status which is functional to a multi-billion pound industry in the UK.[10]

Yet, the month of September 2021, only a few months after the adoption of the UK adequacy decision, marked the beginning of what could be defined as a second, distinct phase of the process of development of UK digital law post-Brexit. After an initial, consequential, legal reordering, the UK government, amid a general surprise, especially from the EU partners, announced its intention to reform UK data protection law in order to purge it from the burdensome box-ticking obligations deriving from a bureaucratic EU data protection law and make it more business and innovation friendly.[11] After collecting feedback through a public

[5] See Edoardo Celeste, 'Data Protection' in Federico Fabbrini, *The Law & Politics of Brexit: Volume III* (Oxford University Press 2021).
[6] See Celeste, 'Data Protection' (n 5).
[7] EU Commission, *Commission implementig decision of 28.6.2021 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*, <https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf>.
[8] For a more detailed explanation of the clauses of the TCA related to data protection, see Celeste, 'Data Protection' (n 5).
[9] *Schrems* [2015] ECJ C-362/14, ECLI:EU:C:2015:650; See Tuomas Ojanen, 'Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter: ECJ 6 October 2015, Case C-362/14, Maximillian Schrems v Data Protection Commissioner' (2016) 12 European Constitutional Law Review 318.
[10] See Oliver Patel, Duncan McCann, and Javier Ruiz, 'The Cost of Data Inadequacy: The Economic Impacts of the UK Failing to Secure an EU Data Adequacy Decision' (UCL European Institute report with the New Economics Foundation 2020) <https://www.ucl.ac.uk/european-institute/sites/european-institute/files/ucl_nef_data-inadequacy.pdf>.
[11] 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>.

consultation that run for ten weeks from September 2021, in July 2022, an outgoing government introduced the Data Protection and Digital Information Bill.[12]

In the public consultation and the documents accompanying the bill, the government explicitly states its objective of regaining UK sovereignty in the digital field by adopting an innovative legislation that would help the UK become a digital champion.[13] However, as experienced in other fields, the actual emancipation from the legal rules developed over decades with the other EU member states for an integrated EU economy is a complex process, generating a plurality of tensions, not least from a digital sovereignty perspective. Indeed, the UK's attempt to introduce a new autonomous data protection model enters into conflict, in an integrated digital economy where data are freely transferred, with the EU's recent attempts to protect its digital sovereignty by preserving fundamental rights guarantees over its data.

This chapter reconstructs and interprets the recent UK's policy moves in the data protection field using a digital sovereignty lens. It will be argued that, while the UK data protection reform is in line with the promises of Brexit of regaining national parliamentary sovereignty, it represents the first example worldwide of a nation deviating rather than approaching the EU data protection model (II). From a digital sovereignty perspective, European nations have understood that to compete with foreign superpowers like the US and China it is necessary to advance a group strategy. In contrast with this trend, the UK data reform presents itself as an isolationist attempt to regain national digital sovereignty. UK digital sovereignty policies, if re-contextualised from a global perspective, particularly looking at their relationship with the EU, might be frustrated by the relatively small economic and regulatory relevance of the UK on the international plane (III). Introducing a data protection reform without fully assessing its potential legal and economic impact and longer-term consequences at a societal level risks to represent a short-sighted form of digital sovereignism (IV). A potential solution to this sovereignist deviation is certainly not imposing to remain legislatively inert and subject to the inherited EU law. Room for change is available but the UK should carefully assess the consequences of losing its EU adequacy status, interrogate itself on the democratic support of this policy move, and explore its potential role in fostering a transnational conversation to develop cross-border synergies in the development of data protection, and more broadly, digital law (V).

II. Regaining digital sovereignty: the promises of Brexit

The Data Protection and Digital Information Bill, introduced in July 2022, carries forward most of the proposed reforms announced by the UK's Department for Digital, Culture, Media and Sport (DCMS) in the public consultation launched in September 2021. In a nutshell, the bill reforms the GDPR's accountability framework by removing the requirement for Data

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

[13] 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>.

Protection Impact Assessments (DPIA), for records of processing, and for the Data Protection Officer (DPO), replacing the latter with a 'senior responsible individual'. Organisations will be able to refuse 'vexatious', and not only 'manifestly unfounded', subject access requests or alternatively they will be able to charge a 'reasonable fee'. The bill transforms the Information Commissioner's Office, the UK national data protection authority, in an Information Commission composed of up to 14 commissioners. The Commission will be subject to 'strategic priorities' defined at ministerial level and in enforcing data protection law the new institution will have to pay regard to new objectives, such as the 'the desirability of promoting' competition and innovation, the importance of preventing crimes and the need to preserve the security of the State. The scope of Article 22 of the UK GDPR, which currently includes, in line with the EU GDPR, a ban of decisions relying on solely automated means which have a legal effect on the individual as well as a right to human intervention in those circumstances where such decisions are allowed, is reduced. The bill removes the ban and grants a right to human intervention only in case of 'significant' automated decisions producing an 'adverse legal effect' on the individual. Lastly, but not certainly least, the bill reforms the UK's adequacy mechanism for data transfers by replacing the criterion of adequacy with the requirement that the foreign data protection regime does not offer a 'materially lower' standard of protection.[14]

As affirmed by the DMCS when publishing the open consultation, with the reform the British Government wants to affirm the UK as a 'science superpower' at the forefront of digital innovation, especially in the field of Artificial Intelligence (AI).[15] In short, boosting innovation and acquiring a leading position in the teach sector globally are the key objectives of the executive. In the consultation outcome document published on 23 June 2022, the DMCS reiterates the aspiration of transforming the UK in the 'most attractive global data marketplace'.[16] According to the Government, this might be achieved by exploiting the legislative sovereignty that the UK has reacquired following Brexit. Reading the Foreword from the UK Digital Secretary to the public consultation launched in September 2021 the sense of frustration vis-à-vis EU law is tangible.[17] The set of EU law regulating data is perceived as potentially hampering the development of the UK economy because of its 'complexity' and 'vagueness'. The UK wants to remain a world-leading regulator, excel in the AI field as well as to continue to attract technology companies. To do so, according to the UK government, new, different and more 'agile' legislation is needed. Hence, the proposal of launching a public consultation, significantly entitled 'Data: A new direction'.

By departing from the GDPR's accountability framework, organisations will have more capability to benefit from the personal data in their possession and therefore innovate, while at the same time maintaining a 'responsible' use of the data in their possession. Bureaucratic obligations imposed by the GDPR, such as DPIAs, mandatory reporting, the duty to appoint an independent Data Protection Officer (DPO), are eliminated in the name of increased innovation and global competitiveness. In order to acquire a competitive advantage on the EU and more

[14] Data Protection and Digital Information Bill, Section 45B.
[15] UK Department of Digital, Culture, Media and Sport (n 13) 2.
[16] 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, Introduction.
[17] UK Department of Digital, Culture, Media and Sport (n 13).

broadly on a global scale, the UK government attempts to eliminate all legal obligations considered to be burdensome or formal box-ticking exercises for organisations processing data. In this scenario, the role of the Information Commission necessarily changes, becoming a promoter of innovation with more 'effective powers' to monitor and steer the development of the UK digital economy.

From a transnational perspective, one can regard this recent policy move by the UK government with surprise. Indeed, only a few months before launching the public consultation on the data protection reform, the UK secured an adequacy decision from the EU Commission. And this occurred at the very last minute, a couple of days before the end of the transition period after which data transfers from the EU to the UK would not have been possible in the absence of a specific legal mechanism. As mentioned in the introduction, the case law of the CJEU has clarified that adequacy determinations must rely on a holistic assessment of the law of third country in question. After Brexit, the UK has become a third country from a data protection point of view, thus requiring a positive analysis of its data protection framework from the EU Commission in order to secure a continued free flow of personal data from the EU. The adequacy decision obtained in June 2021 already relied on unstable bases, given the existence of regulatory provisions in the UK which have been deemed to be contrary to EU fundamental rights, such as extensive mass surveillance and data retention powers in the field of national security and the restriction of data subject rights in case of data processing for immigration purposes.[18] The proposed data protection reform adds a further layer of instability, potentially increasing, if approved, the degree of divergence between EU and UK law, and thus making a suspension of the adequacy decision from the EU even more likely.

Yet, if one analyses the decision of the UK government from a national perspective, looking in particular at its positioning within the Brexit process, the recent move of the British executive is far less surprising. The proposed reform fully subscribes the political agenda of Brexit, its rhetoric, and in particular the claim that Brexit would eventually allow the UK to reacquire its lost sovereignty. Indeed, first of all, it generates from the assumption that EU law imposes unnecessary requirements, is bureaucratic and does not support innovation.[19] Hence, the need to get rid of EU norms in order to reacquire full independence in the nation's sovereign choices and finally incentivise a flourishing economy. Interestingly, one can notice that the recent data protection reform is fully in line with this chain of arguments, and is the last of many fields that have been instrumentalised to pursue the Brexit agenda, even in absence of clear socio-economic evidence that this policy move will be successful from a general perspective.[20]

---

[18] See Celeste, 'Data Protection' (n 5). See also European Parliament resolution of 12 February 2020 on the proposed mandate for negotiations for a new partnership with the United Kingdom of Great Britain and Northern Ireland (2020/2557(RSP), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/2557(RSP).

[19] See Department for Exiting the European Union, 'Benefits of Brexit: How the UK Is Taking Advantage of Leaving the EU.' (2022) <https://www.gov.uk/government/publications/the-future-relationship-between-the-united-kingdom-and-the-european-union>.

[20] See Orla Lynskey, 'EU-UK Data Flows: Does the "New Direction" Lead to "Essentially Equivalent" Protection?' (22 September 2021) <https://dcubrexitinstitute.eu/2021/09/eu-uk-data-new-direction/>, who argues that the UK may use data protection to pursue its political agenda. Cf. also Oliver Patel, Duncan McCann, and Javier Ruiz, 'The Cost of Data Inadequacy: The Economic Impacts of the UK Failing to Secure an EU Data Adequacy Decision' (UCL European Institute report with the New Economics Foundation 2020)

Indeed, as will be highlighted in section IV, this reform risks to push the EU Commission towards the unavoidable choice of suspending the UK adequacy decision, with a series of significant economic and compliance costs in the short to medium term.[21] Conversely, on the other end, the proposed reform, apart from the opinions shared in the public consultation, does not rely on solid empirical research demonstrating the advantages of the change from a business and innovation perspective. On the contrary, various answers to the public consultation highlight how some of the proposed changes – in particular the removal of Article 22 on automated decision making and the lightening of some accountability requirements – might lead to a lower level of public trust in public and private institutions processing data in the UK as well as an increased diffidence from international partners wishing to transfer data to the UK.[22]

III. Digital sovereignty clashes: the UK reform in the EU context

In the field of data protection, the recent UK policy move represents a unicum. Over the past few years, multiple countries have adopted data protection legislation drawing significant inspiration from the EU model or have been forced to bring their laws in line with EU standards, in what the scholarship has called the 'Brussels effect'.[23] The UK's decision of emancipating itself from EU data protection law, creating a new model drawing inspiration from different data protection regimes[24], establishing new objectives for the activities of its national data protection authority, such as promoting innovation and global competition, as well as identifying new criteria and partnerships to create a new UK data protection galaxy of international data transfers is unprecedented. The EU, so far, has played a central role as a global standard setter in the digital field, partially because of its economic relevance and partially because its focus on fundamental rights, values that, at least in principle, are regarded as reference points in modern democratic states.

However, apart from the direction that this policy move is taking, the UK's idea itself of definitely severing its ties from the EU, regaining its legislative sovereignty and creating a new, independent regulatory dimension might be seen as an illusion. Indeed, the hyper-connected digital society where we live, and even more in a transnational trade context, such as the one linking the EU and the UK, which was previously a single common market, the concept of rigid regulatory boundaries linked to sovereign physical territories does not correspond to reality. In the infosphere – as Floridi calls it – nation states struggle to apply the Westphalian notion of sovereignty as it is not necessarily true that, for instance, data physically located in

<https://www.ucl.ac.uk/european-institute/sites/european-institute/files/ucl_nef_data-inadequacy.pdf>, who illustrates the economic impact of the failure to obtain an adequacy status from the EU Commission. Indeed, the announced data protection reform could lead to the similar situation of losing the adequacy status.

[21] Cf Oliver Patel, Duncan McCann, and Javier Ruiz (n 10).

[22] Cf. Competition & Marketing Authority, 'CMA response to consultation on Data: A new direction' (2021) para 9; The Faculty of Advocates, 'Response from the Faculty of Advocates to The Consultation on Data: A New Direction' (20 December 2021).

[23] See Costello in this volume; see Federico Fabbrini, Edoardo Celeste and John Quinn (eds), *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart 2021).

[24] See Bridget Treacy, 'Expert Comment' (2021) 22 Privacy & Data Protection 2.

one jurisdiction are exclusively subject to the laws of that country.[25] EU data protection law offers one of the clearest examples of extraterritorial effect, the GDPR itself explicitly having an extraterritorial scope of application.[26]

This phenomenon can be explained by the contemporary need of nation states to protect their digital sovereignty. The notion of 'digital sovereignty' has not received a univocal definition, as it would be hard to find consensus on the concept of 'sovereignty' itself.[27] Indeed, sovereignty is a historical concept that has evolved over the centuries from denoting a relative pre-eminence in a specific subject matter – as the medieval bishops had in all religious issues notwithstanding the temporal power governing the territory where they were located – to an absolute capability to regulate the legal ordering within the physical boundaries of the nation state – the modern, Westphalian concept of 'national sovereignty'.[28]

The notion of 'digital sovereignty' stems from the traditional need of the nation state to exercise power on a newly emerged set of assets: it is 'control of the digital', as Floridi puts it to denote the state's struggle to govern data, software, standards, protocols, processes, hardware, services and infrastructures that underpin the digital society.[29] However, this contemporary form of sovereignty at the same time shares some of the elements that characterised this notion centuries ago. Indeed, the digital can hardly be caged within national boundaries – data circulate across nations; hardware is made of components built in different jurisdictions; virtual infrastructures serve the needs of customers and public institutions located in various states; private multinational companies ideate, manage, sell digital products and services on a global basis without tailoring their standards to the rule of all the countries where they are commercially active. For this reason, nation states attempt to protect their sovereignty in the digital field not only by regulating what occurs in their physical territories – as they should do according to the traditional notion of Westphalian sovereignty – but also put in place two strategies: either they apply their rules extraterritorially or they try to attract digital assets within their territories. We can therefore identify two simultaneous policy trends that characterise digital sovereignty claims: one which is centrifugal, i.e. consists in extending a state's regulatory reach beyond its boundaries, and another one which is centripetal, i.e.

[25] Luciano Floridi, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU' (2020) 33 Philosophy & Technology 369.
[26] See Fabbrini, Celeste and Quinn (n 23); Federico Fabbrini and Edoardo Celeste, 'The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders' (2020) 21 German Law Journal 55; Dan Jerker B Svantesson, 'Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation' (2015) 5 International Data Privacy Law 226; Christopher Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5 International Data Privacy Law 235.
[27] 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).
[28] See George W White, *Nation, State, and Territory: Origins, Evolutions, and Relationships* (Rowman & Littlefield 2004); Celeste, 'Digital Sovereignty in the EU: Challenges and Future Perspectives' (n 27).
[29] Floridi (n 25) 371; see also Patrik Hummel and others, 'Data Sovereignty: A Review' (2021) 8 Big Data & Society <http://journals.sagepub.com/doi/10.1177/2053951720982012> accessed 18 May 2022.

attempts to attract important digital assets within the physical boundaries of the state so that the latter can better regulate and control them.[30]

An example of the first tendency is the above-mentioned extraterritorial scope of application of EU data protection law. In this way, the EU ensures that personal data related to EU residents, even when they quit the EU soil – and are technically subject to the law of another jurisdiction – are processed according to EU law and standards.[31] While, an example of a policy aiming to preserve digital sovereignty in a centripetal way is the adoption of data localisation laws, which are pieces of legislation requiring personal data related to a country's data subjects to be processed and stored within that jurisdiction.[32] In this case, nation states remain anchored to the traditional Westphalian notion of sovereignty and instead of attempting to regulate a digital assets located in another jurisdiction, they impose the repatriation of those assets within national boundaries.

The UK's willingness to exercise and protect its digital sovereignty is not per se surprising. France and Germany were among the first states in Europe to have championed the idea that more protection of their national digital assets was needed in order not to succumb to regulatory and economic diktats from powerful countries at the forefront of digital innovation, such as the US and China, and their multinational companies.[33] However, these states soon understood that little could do a solitary fight to preserve or reconstitute their digital assets vis-à-vis the advanced state of development of foreign digital superpowers. Hence the idea of developing a common policy to achieve digital sovereignty at European level, transitioning from a national to a supranational perspective.[34] It is therefore also in this context that the UK data reform does not seem in phase with the recent policy trends. Not only is the UK the first country to depart from the EU data protection model but is also going against the tide by cultivating the ambition to be able to succeed, alone, in proposing an alternative regime that will be ultimately successful on a global basis.

However, the announced UK data reform does not simply denote an unconventional and maverick attitude, but its concrete likelihood of success may be questioned due to disparity of economic forces between the UK and the EU. EU digital sovereignty claims have emerged to contrast the American and Chinese economic imperialism in the digital field and preserve EU fundamental rights.[35] As said, the trend has been to escalate policy objectives from a national to an EU, supranational level in order to maximise the forces and be able to compete on a global level. The project of creating a cloud made in the EU, the so-called Gaia X, which is an example

[30] I have first illustrated this distinction in Celeste, 'Digital Sovereignty in the EU: Challenges and Future Perspectives' (n 27).
[31] See Orla Lynskey, 'The Extraterritorial Impact of Data Protection Law through an EU Law Lens' in Federico Fabbrini, Edoardo Celeste and John Quinn (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart 2021); Svantesson (n 26).
[32] See Edoardo Celeste and Federico Fabbrini, 'Competing Jurisdictions: Data Privacy Across the Borders' in Grace Fox, Theo Lynn and Lisa van der Werff (eds), *Data Privacy and Trust in Cloud Computing* (Palgrave 2020).
[33] See Georg Glasze and others, 'Contested Spatialities of Digital Sovereignty' [2022] Geopolitics 1; Julia Pohle and Thorsten Thiel, 'Digital Sovereignty' (2020) 9 Internet Policy Review.
[34] See Floridi (n 25).
[35] See Carla Hobbs (ed.) and others, 'Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry'.

of centripetal trend, as well as the imminent adoption of a solemn Declaration of European digital rights and principles, which, in a centrifugal way, would work as a global manifesto of European digital values, are two examples of this tendency. At the same time, what we are currently observing in the UK a form of national sovereignty-propelled – normative, rather than economic – spin-off from its much bigger neighbour, the EU, in order to be able to develop a new regulatory model in the digital field that would eventually lead to a prominent role in the digital economy. We therefore witness an unpair clash between national (UK) and supranational (EU) digital sovereignty policies, which, simply from an economic point of view, does not seem to leave much hope in the UK's ability to resist the Brussels effect, not to say to play a 'London effect' that would affirm the UK as a global leader and standard setter in the digital economy.

An example that is already possible to provide relates to the UK's intention to conclude an agreement regulating data transfers from the UK to the US.[36] An opportunity that the UK was seeking in order to find an economic advantage to compete with the EU, where the CJEU has invalidated for the second time the legal mechanism allowing personal data to be transferred to the US. However, the economic weight of the EU has led the US to agree a new data pact with the group of 27 member states rather than with the UK, which might have seen as a rebel, but still dependent satellite of the EU data protection galaxy.[37] Yet, notwithstanding the different economic weight of these two competing players, the UK might gain a short-term economic advantage. Indeed, the current links with the UK, the still de facto embeddedness of Britain in the EU data protection galaxy, may prompt American and Chinese companies to relocate in the UK to obtain and easy access to EU data.[38] However, this condition might only be temporary due to the possibility, as observed below, of suspending or invalidating the UK adequacy decision.

UK digital sovereignty policies, if re-contextualised from a global perspective, might be frustrated by the relatively small economic and regulatory relevance of the UK on the international plane. Digital sovereignty strategies risk to be reduced to short-sighted sovereignist claims.

IV. The risks of digital sovereignism

The notion of digital sovereignism denotes the advocacy or adoption of sovereignist policies in the digital field. The scholarship also used the terms 'digital statism', 'data' or 'tech nationalism'.[39] Basile et al. identify three components of sovereignism in general, which can

[36] Anabelle Dickson, Vincent Manancourt and Samuel Stolton, 'Distractions Plague UK's Post-Brexit Tech Plan' *POLITICO* (18 April 2022) <https://www.politico.eu/article/distractions-plague-post-brexit-tech-plan/> accessed 5 May 2022.

[37] See European Commission, 'Joint Statement on Trans-Atlantic Data Privacy Framework' <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087> accessed 2 September 2022.

[38] See Charles Grant, 'Ten Reflections On A Sovereignty-First Brexit' (*Centre for European Reform*, 28 September 2020) <https://www.cer.eu/insights/ten-reflections-sovereignty-first-brexit>.

[39] Respectively, Floridi (n 25) 374; Anupam Chander and Uyên P Lê, 'Data Nationalism' (2015) 64 Emory Law Journal 677; Carla Hobbs (ed.) and others (n 35) 24.

help us schematise and better define how this concept can be applied in the digital field: a political, cultural and economic dimension.[40] Digital sovereignism would denote policies that:

- from a political point of view, claim to regain control of national digital assets against the influence of foreign actors;
- from a cultural point of view, rely on the assumption that national identity, including its normative values and economic approach, are under threat; and,
- from an economic point of view, are associated with protectionist or isolationist strategies.

Populism would be the gluing element of these three components as digital sovereignism is usually characterised by claims purporting that local regulators and industry have lost the power to determine the destiny of national digital assets and that regaining that control would be the panacea to all economic and social problems.[41]

The UK's recent policy moves seem to go in a similar direction and can be qualified as an expression of digital sovereignism. They are politically pushed by the will of emancipating the UK from the EU regulatory influence. It is perceived that the UK digital economy and its assets are subject to bureaucratic sets of legislation that frustrate the UK's traditional pro-business approach to innovation. If protectionist trends are not detectable, an isolationist strategy is well apparent, being the UK the first country to depart from the well-established and much imitated model of EU data protection. The whole accompanied by a populist rhetoric that the depicts EU data protection law as a set of outdated and burdensome norms imposed by Brussel's bureaucrats – as if the UK did not participate in its drafting – and thus posits the need to 'take control back' and adopt new rules that would be more innovation and business friendly and that would allow the UK to become a leader in the digital economy.

The UK sovereignist policy moves in the digital field, if justified from a political perspective as an attempt to give follow to the Brexit claims, may have significant consequences, both from a legal and from an economic point of view. Despite its regained legislative sovereignty, the UK is dependent on the EU Commission's adequacy decision in order to be able to receive EU data. Paradoxically, now that the UK is no longer part of the EU, it is even more subject to the Commission's scrutiny, as it is no longer implied, being a third state, that its legislation is in line with EU data protection standards.[42] Therefore, the UK adequacy decision theoretically works as a bridle on UK law. If the UK wants to maintain its adequacy status, it should abstain itself from radically departing from EU law and keep following EU standards, in a sort of forced Brussels effect. Indeed, the CJEU has clarified that for the purposes of international data transfers, 'adequate' does not mean 'identical', but a 'substantial equivalence' is required.[43] Now, if the DPDI bill will be passed into law, the UK will introduce significant reforms that in the eyes of the Commission will be very probably regarded as not providing an adequate level of protection to EU fundamental rights. In particular, the reform of the ICO and the dismantling

[40] Linda Basile, Rossella Borri and Luca Verzichelli, '"For Whom the Sovereignist Bell Tolls?" Individual Determinants of Support for Sovereignism in Ten European Countries' (2020) 21 European Politics and Society 235.
[41] See Basile, Borri and Verzichelli (n 40).
[42] See Celeste, 'Data Protection' (n 5).
[43] *Schrems* (n 9); see Ojanen (n 9).

of data controllers' accountability framework seem to be significantly contrasting the EU approach and necessarily leading to a withdrawal of the adequacy status from the EU Commission or its invalidation by the CJEU following an ad hoc litigation. Taking a political perspective, this outcome might also make the EU-UK relationship even more tense and might reduce the likelihood of success of future negotiations about a data transfer agreement.[44]

If the legal prize to pay to adopt the UK data reform would be the loss of the adequacy decision, from an economic point of view this might have a significant impact, especially in the short term. Indeed, the UK economy is deeply integrated in the EU economy. The UK's DCMS, in its impact assessment of the proposed data reform calculated a potential loss of £1.4 billion, of which £1 billion in reduced trading revenue and £420 million in compliance costs, due to need to identify and implement alternative data transfer mechanisms such as standard contractual clauses and binding corporate rules.[45] Moreover, the data reform, by enhancing the risk of loss of adequacy status, increases legal uncertainty among economic partners, and generates preventive legal compliance costs among those firms that desire to adopt alternative data transfers mechanisms in the fear of a sudden invalidation or suspension of the adequacy decision. From a consumer perspective, instead, as many parties have observed in their answers to the DMCS' public consultation, the proposed reform might lead to an increased distrust in UK data controllers.[46] Indeed, by introducing a more business and innovation friendly regime, the UK government has unavoidably reduced the bureaucratic aspects of the GDRP that however precisely aim to protect data subjects' fundamental rights.[47]

UK digital policies are certainly not the only ones that risk incurring in forms of digital sovereignism. Looking at the plank in our own eye, it is also true that EU digital sovereignty claims have potential sovereignist deviations. In particular, in so far as they adopt protectionist attitudes by subsidizing EU tech industry, for example for the creation of a cloud made in the EU, or imposing norms that necessarily lead to a de facto obligation to process data within the EU, as required by the case law of the CJEU in the case of data retained by telecommunication operators for the purposes of public and national security.[48] These policies too, if merely supported by the need to promote digital autarchy, boost the EU economy and become leaders in the digital sector, appear as 'economically anachronistic'.[49]

---

[44] See Kathryn Wynn, '"Data: A New Direction" - but Is It the Right One?' (2022) 22 Privacy & Data Protection 13.

[45] Department for Digital, Culture, Media & Sport, *Data: A New Direction - Analysis of Expected Impact* (2021) 22.

[46] The Law Society of England and Wales, Law Society response: Department for Digital, Culture, Media & Sport consultation, 'Data: a new direction' (2021), para 4.

[47] See Orla Lynskey, 'EU-UK Data Flows: Does the "New Direction" Lead to "Essentially Equivalent" Protection?' (*DCU Brexit Institute News*, 22 September 2021) <https://dcubrexitinstitute.eu/2021/09/eu-uk-data-new-direction/>; cf. Edina Harbinja and others, 'Written Evidence Submitted by: British and Irish Law, Education and Technology Association (BILETA) Data: A New Direction Inquiry (DCMS)' (British and Irish Law, Education and Technology Association (BILETA) 2021) who observe that the proposed data reform leads to an erosion of rights without necessarily fostering innovation.

[48] See Chander and Lê (n 39).

[49] Floridi (n 25) 374.

V. Legitimising digital sovereignty policies in a plural environment

Digital sovereignism is not an effective and successful policy in the long term. From an economic point view, short term gains generated by protectionist attitudes are overcome by lack of longer-term sustainability and increase of costs related to legal compliance. From a political point view, digital sovereignist policies exacerbate tensions, hinder cross-border collaboration practices, which are essential in a closely connected digital environment. At the same time, digital sovereignty claims may well be legitimate and justified. Therefore, the conundrum, both in the UK and in the EU, currently lies in the definition of the boundaries between legitimate digital sovereignty claims and digital sovereignism.

Of utmost importance is to reflect on what would be the legitimate objectives to pursue through digital sovereignty policies. In the case of EU, the US and Chinese digital superpower are seen as a threat to the EU's possibility of protecting its fundamental rights. Following this argument, the EU desires to emancipate itself from this foreign predominance in the digital field by regaining an ability to produce, shape and control its digital assets.[50] The EU's willingness to protect its fundamental rights is certainly legitimate but it degenerates in a form of sovereignism when it becomes a justification to subsidise the EU tech industry or when it does not take into account the effect that an extraterritorial application of EU law has on the diversity and plurality of values and principles on a global level. Protecting EU digital rights should be therefore seen as the first lighthouse guiding the navigation of EU digital sovereignty policies in order to prevent their degeneration in forms of sovereignism. Digital constitutionalism, intended as the ideology that is pushing towards a re-articulation of fundamental rights in the mutated context of the digital society, can thus be used as a conceptual barrier to digital sovereignism in the EU.[51] This approach would also be in line with the human-centric attitude that the EU has promoted over the past decades, and is in particular stressing at the moment in the context of development of a normative framework for artificial intelligence.[52]

But also, an increased awareness of diversity and plurality should be sought. Otherwise, a stubborn and blind protection of EU fundamental rights risks to lead to contestable results akin to imperialist or colonialist phenomena, when EU law is required to apply or de facto applied extraterritorially by virtue of the principle of the law of the strongest. An apparent example of this threat was represented by the implementation of the right to be forgotten, as articulated by the CJEU in the seminal case *Google Spain*.[53] In the aftermath of the case, Google wondered

[50] See, e.g., European Council, Remarks by President Charles Michel after the Special European Council meeting on 2 October 2020 <https://www.consilium.europa.eu/en/press/pressreleases/2020/10/03/remarks-by-president-charles-michel-after-the-special-europeancouncil-meeting-on-2-october-2020/> accessed 30 August 2022.

[51] For a more detailed illustration of the scholarship on digital constitutionalism see Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33 International Review of Law, Computers & Technology 76; see also Edoardo Celeste, *Digital Constitutionalism: The Role of Internet Bills of Rights* (Routledge 2022).

[52] See Edoardo Celeste and Giovanni De Gregorio, 'Digital Humanism: The Constitutional Message of the GDPR' (2022) 3 Global Privacy Law Review 4.

[53] *Google Spain v APED* [2014] ECJ C-131/12, ECLI:EU:C:2014:317; on the aspect of extraterritorial application of the right to be forgotten see Dan Jerker B Svantesson, 'The Google Spain Case: Part of a Harmful Trend of Jurisdictional Overreach' (2015) EUI Working Papers <http://cadmus.eui.eu//handle/1814/36317> accessed 15 January 2020; Paul De Hert and Vagelis Papkonstantinou, 'Google Spain: Addressing Critiques and Misunderstandings One Year Later Comment' (2015) 22 Maastricht Journal of European and Comparative Law

whether the effect of delisting obtained on foot of the exercise of the right to be forgotten by an EU resident should have the effect of compelling the search engine to eliminate the results in question from all the versions of its website worldwide. In the subsequent *Google vs CNIL* case, the CJEU clarified that the delisting was not required on a global level but only on the versions of the search engine accessible from Europe, thus showing an increased attention and respect towards the existence of other legal systems that do not share the same European values.[54]

UK digital sovereignty claims conversely aim to pursue different policy objectives. The protection of fundamental rights is not one of the priorities of the proposed data reform.[55] The UK conversely seeks to boost innovation, reduce bureaucratic tick-boxing practices imposed by the inherited EU data protection law and affirm itself as a leader in the digital sector. In light of this, one can observe that there is no common solution applicable to all potential digital sovereignist deviations. Indeed, arguing that digital constitutionalism and the promotion of diversity and pluralism should be the guiding principles to pursue to avoid digital sovereignism in the UK would risk sounding as an attempt to impose an EU approach on a state that has voluntarily decided to leave the union. The solution is not merely asking the UK to reform its data protection law within the perimeter of EU standards in order to maintain at all costs the adequacy status. However, at the same time, the UK should carefully assess whether the results of the Brexit referendum should be interpreted as a sign that the 'new direction' that the UK should pursue is one increasingly diverging from the until so far shared European values. The UK should also evaluate the pros, cons, and the timing of its proposed reform, basing any amendments to the current normative framework on economic and legal justifications relying on empirical evidence. Populist rhetoric and international arm-wrestling in the name of the Brexit promise of regaining a lost parliamentary sovereignty might not lead to an optimal solution for the UK economy and society, especially when the economic gains of the proposed reform are not clear and there is the risk of loss of public trust.

In parallel, the UK might reconsider its role as a contributor to the EU, if not global, discussion on digital law. So far, the UK has played a crucial role in developing and enforcing EU data protection law. Even if no longer a member state, the UK might still help share EU digital policies, by participating for example in a new vest in the works of the European Data Protection Board or in another institutional setting created ad hoc to foster collaboration between the EU and the UK. This solution would indeed represent a gain both for the EU that would be more open to recognise foreign values and priorities avoiding imperialist or colonialist trends, and for the UK that would not have to resort to a frustrating and draining arm-wrestling with its bigger neighbour.

Figure 1. Comparison of EU and UK digital sovereignty policies

624; Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the "Right to Be Delisted"' (2015) 5 International Data Privacy Law 105.

[54] *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* [2019] ECJ C-507/17, ECLI:EU:C:2019:772; see also John Quinn, 'Google vs CNIL: Circumscribing the Extraterritorial Effect of EU Data Protection Law' in Federico Fabbrini, Edoardo Celeste and John Quinn (eds), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart Publishing 2021).

[55] See Lynskey (n 47).

Actor	Foreign powers to circumscribe	Stated objectives	Sovereignist attitudes	Negative effects	Potential solutions
EU	China; US	Protection of fundamental rights	Pursuit of digital autarchy; Protectionism; (Unjustified) Data localisation Extraterritorial effect of EU law	Increased economic costs due to made in EU; Slow innovation; Regulatory imperialism / colonialism / Brussels effect	Recognition of diversity; International collaboration; Collaborative standard setting
UK	EU	Support to innovation; Simplification / Debureaucratisation; Economic leadership	Populist arguments about EU law Reform proposed with evidence of net economic gains Isolationism	Relinquishment of EU fundamental rights Loss of public trust Creation of tensions with EU (adequacy)	Collaborative standard setting; International collaboration

VI. Conclusion

Despite its promises, Brexit did not lead to a 'separate but equal' relationship between the UK and the EU.[56] Regaining national sovereignty in the digital field cannot rely on the assumption that a surgical exercise between legal, political and socio-economic frameworks that were not so far ago strictly linked is possible. It is not only a question of 'filiation' or previous relationship. The digital society is largely interconnected. Data and digital goods and services circulate, are traded and shared across the world. The UK is an integral part of this complex mosaic and, even if no longer sharing the EU piece of the puzzle, it should take into account the effects of its policies on a transnational and cross-border level. The Brexit rhetoric of regaining legislative sovereignty and the idea of introducing a brand-new data protection legislation significantly diverging from the current one inherited by the EU seem to be based on a Westphalian notion of sovereignty that no longer holds in the digital society. The adoption and implementation of new digital law and policies have transnational effects as it is not veracious to think that by leaving the EU the UK can get rid of the GDPR, as in any case the extraterritorial features of the latter will continue to exercise effects in the UK, be it willing or

[56] See Karlin Lillington, 'Britain Looks to Weaken Rules on Data Privacy' *The Irish Times* (16 September 2021) <https://www.irishtimes.com/business/technology/britain-looks-to-weaken-rules-on-data-privacy-1.4675042> accessed 31 August 2022.

not. The UK has to consider its size and economic relevance on the global plane as the battle for digital sovereignty is dominated by big players, namely the US and China, with the EU currently struggling to emerge as a single entity.

Introducing a data protection reform without fully assessing its potential economic impact and longer-term consequences at a societal level for the sake of demonstrating that the UK has finally emancipated itself from EU law risks to represent a short-sighted form of digital sovereignism. Populist arguments about the need to reacquire a long stolen parliamentary sovereignty and to reintroduce the traditional British pro-business regulatory approach here replace economic evidence and an analysis of the legal and political impact of the recently proposed data protection reform. A potential solution to this sovereignist deviation is certainly not imposing to remain legislatively inert and subject to the inherited EU law. Room for change is available but the UK should carefully assess the consequences of losing the EU adequacy status. Indeed, adequate does not mean identical, and eventually the UK could play a role in fostering a conversation about a reform at EU level too. However, it is also important for the UK to interrogate itself on the democratic mandate of this reform. UK people voted to leave the EU but this does not necessarily imply a consent about a sudden departure from EU data protection values as well, which would rather mark a constitutional value U-turn, not to say a crisis.

Enlarging the perspective, the question of the worldwide emergence, development and complementarity of different data protection systems in order to preserve national or regional digital sovereignty is announced to be the legal conundrum of the next decade. The EU digital law model, which poses the human being and their fundamental rights at the centre, is having a great success, being imitated by many states across the globe in what has been called the 'Brussels effect'. However, the EU strategy is not exempt from potential sovereignist deviations, especially when it comes to subsidise the emergence of a tech industry and services made in the EU. As occurred after the horrors of WWII, the exercise of sovereignty needs to be guided and circumscribed by the objective of preserving fundamental rights, and not by economic considerations. Digital constitutionalism thus emerges as a potential lighthouse to guide the navigation of EU digital strategies in this complex sea. Promoting a rearticulation and a recognition of fundamental rights in the digital field might serve the twofold objectives of ensuring that digital sovereignty policies do not degenerate in forms of sovereignism and of promoting a constitutional recognition of digital rights.

At the same time, the EU needs to interrogate itself on the potential imperialist or colonialist consequences of its data protection framework. Alternative models based on different values and principles exist or are gradually emerging. This may well occur in jurisdictions which will become able to economically compete with the EU in the tech sector. Hence, to avoid that an economic war will eventually decide which data protection model will prevail following the law of the strongest, 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 plurality of values and technical innovation. To avoid a digital sovereignty arm-wrestling, this form of cross-border cooperation is necessary. Starting, of course, from our neighbours across the Channel.