**8**

**Regulatory divergence: The effects of UK technology law reforms on data protection and international data transfers**

Edina Harbinja

**I. Introduction**

The post-Brexit UK is characterised by a turbulent and chaotic political, economic and social environment and a lively and often disintegrated policy and law reform landscape. To deliver on Brexit promises of ‘independence from Brussels’,[[1]](#footnote-1) the government has introduced law reform in various areas, with digital regulation and law being particularly significant and controversial. Shortly after Brexit, the government announced reforms in data protection, online safety, human rights and AI regulation*, inter alia*. After a period of intense political turmoil and prime minister resignations, we seem to be left with fewer reform proposals. At the moment, it seems that the human rights reform has been scrapped,[[2]](#footnote-2) and the data protection and online safety reform have been delayed, contrary to the government’s initial promises.[[3]](#footnote-3) The AI regulation reform is ongoing, but comprehensive primary legislation in this area will not be expected soon.[[4]](#footnote-4)

Notwithstanding the uncertainty of the regulatory environment, it is apparent that current reforms have not been considered holistically. Their effects have been assessed rather in isolation and the piecemeal approach results in regulatory discrepancy, inconsistency, and divergence. Consequently, regulatory and law reform goals may be undermined, particularly regarding their impact on fundamental rights and freedoms.

This chapter examines aspects of this ‘digital law reform package’, and analyses the effects of a specific technology law reform on another area of law reform in the digital sphere. In particular, and in line with the overall subject matter of this book, I question the effects of online safety law reform (the Online Safety Bill) and AI regulation on data protection in the UK and commercial data transfers between the UK and the EU. The focus will be on the most significant proposal in these reforms that may compromise or otherwise impact the UK data protection regime, its adequacy and its relationship with the EU data protection regime. I challenge these proposals on the basis of their divergence and inconsistency and conclude that the technology (and other) law reform needs are approached holistically, or we risk 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.

As a framework, the chapter endorses the regulatory alignment/divergence model developed by Armstrong. He submits that regulatory alignment/divergence in any given policy area will be a ‘function of the operation and interaction of different modes of governance: hierarchy, competition, co-ordination, networks and community.’[[5]](#footnote-5) Briefly, hierarchy is a coercive form of governance based on rules and discipline. In the context of Brexit, UK regulatory alignment/divergence is ‘a function of the external discipline’ of agreements between the UK and the EU, other instruments they are parties of, and ‘the institutional apparatus through which such instruments would be implemented and enforced.’[[6]](#footnote-6) In the context of data protection, the UK adequacy decision represents a hierarchical mode of governance. Second, competition as a form of governance means the market forces the extension of EU governance outside its territory. An example of this may be companies applying GDPR standards of data protection outside the EU to simplify compliance and governance.[[7]](#footnote-7) Third, co-ordination entails voluntary mutual agreements and negotiations. An example could be the UK Withdrawal Agreement. Finally, governance by ‘network’ or ‘community’ includes public or private actors and the mechanisms of transfer and diffusion, which result in ‘common socialisation activities and joint knowledge production.’[[8]](#footnote-8) Examples could include regulatory or academic knowledge production that may result in a greater regulatory alignment between the EU and the UK in different areas of technology regulation in the future.

The chapter approaches these questions of relevant law reforms comparatively, looking at the proposals in context and action, assessing their consequences and effects on individuals and society. It cross-references many relevant chapters in this book, where aspects of these reforms have been considered, mostly independently, focusing on one or two reforms.[[9]](#footnote-9)

In section I, I briefly consider UK data protection adequacy to set out the scene for the assessment of the effect other law reforms may have on UK data protection adequacy. In section II, I consider the online safety reforms and their potential effect on regulatory divergence and data protection adequacy. Section III looks at the government’s approach to the regulation of AI in the context of data protection and adequacy before offering conclusions and ways forward. The chapter will not focus on the proposed human rights reform, as it has been withdrawn for now. I will, however, mention it briefly to provide another example of the regulatory divergence and the resulting discrepancy that I assess in this chapter.

**II. UK adequacy challenged**

The UK data protection adequacy decision and the events that preceded it have been introduced in detail in Chapter 2, as well as McCullagh’s earlier excellent work.[[10]](#footnote-10) In Chapter 3, Pearce also ably explores aspects of adequacy, questioning the unambitious proposal for law reform in the UK and arguing that the UK government could have proposed an even more radical data protection model.[[11]](#footnote-11) Additionally, Erdos offers one of the most detailed analysis of the law reform proposal in his two recent pieces.[[12]](#footnote-12) To avoid the repetition of these analyses, I will only briefly explore the most significant aspects of the data protection reform relevant for this chapter.

After the UK left the EU on the 31st of January 2020, the early data protection and technology law scholarship mostly focused on challenges associated with the UK being granted an adequacy decision by the European Commission.[[13]](#footnote-13) Following a period of uncertainty that saw the publication of European Commission’s draft decisions,[[14]](#footnote-14) the two final UK adequacy decisions were adopted on the 28th of June 2021, allowing transborder personal data flows to continue between the EU and the UK.[[15]](#footnote-15)

When assessing the data protection adequacy, the Commission had to determine whether the UK provides an ‘essentially equivalent’ level of protection to that in the EU. UK law did not need to mirror the GDPR entirely,[[16]](#footnote-16) as long as it contained the core requirements set out in Article 45 GDPR and further elaborated on in CJEU case law, the EPDB’s Recommendations on Essential Guarantees for surveillance measures[[17]](#footnote-17) and in the EDPB’s ‘adequacy referential.’[[18]](#footnote-18) Importantly for the purpose of this discussion, the de jure substantive protection of personal data in UK law was assessed by reference to the criteria set out in Art 45(2) of the GDPR. The article required the European Commission to take into consideration not just the domestic data protection law *stricto sensu*, but also the rule of law, respect for human rights and fundamental freedoms, relevant legislation, and the international commitments the UK has entered into. This provision thus compels the Commission to consider other legislation, case law and the rule of law more broadly, all of which may impact data protection and privacy in the UK, including the legislative proposals (once adopted) that we analyse in this chapter. This is a clear example of Armstrong’s hierarchy as a coercive form of governance, where regulatory alignment is achieved through a set of rules and adequacy decision.

In terms of the data protection law specifically, the UK government's intention has been for UK data protection law to continue to adhere to the EU GDPR post-Brexit.[[19]](#footnote-19) Nevertheless, the potential for divergence has never been ruled out. The first sign of the divergence arose in September 2021, when the Department for Digital, Culture, Media and Sport (DCMS) launched a public consultation and the law reform paper ‘Data: A new direction’.[[20]](#footnote-20) The paper outlined various proposed changes to the UK’s data protection regimes, with legislative aims to reduce barriers to innovation, reduce compliance burdens on businesses, boost trade, and improve public services.[[21]](#footnote-21) Responses to the consultation were mixed, with vocal academic and social society critics suggesting that the proposal would weaken many established data protection rules and jeopardise the UK adequacy decision.[[22]](#footnote-22) On 18th of July 2022, the Data Protection and Digital Information Bill (the DPDIB) was introduced in the House of Commons to amend a number of provisions of the UK GDPR and DPA 2018.[[23]](#footnote-23)

Despite the proposed reforms set out in the consultation paper ‘Data: A new direction’ aiming to be substantive and innovative, they are, in reality, quite unambitious and do not seem to diverge radically from the EU data protection regime, *prima facie*. Only a few significant proposals may diverge from GDPR to an extent.[[24]](#footnote-24) Their impact is yet to be evaluated after the final text has been passed and we could assess the law in action. Indeed, as anticipated, the programme parliamentary discussion of the bill originally planned for September 2022 has been postponed.

In her analysis of the DPDIB in chapter 2, McCullagh argues that the proposed changes ‘if implemented in their current form, are unlikely to jeopardise the UK adequacy decision.’[[25]](#footnote-25) Erdos shares this view, finding the reform proposal ‘wide-ranging but not radical’.[[26]](#footnote-26) McCullagh analyses the plan to retain the UK GDPR's definition of personal data with only minor amendments. The ‘Data: a New Direction’ Consultation proposed revising the definition, but the DPDIB proposes that data will be identifiable if another person is ‘likely’ to ‘obtain the information as a result of the processing’ and the data subject ‘will be, or is likely to be identifiable’ by that person ‘by reasonable means.’[[27]](#footnote-27). This limits the assessment of identifiability to the controller or processor and persons who are likely to receive the information rather than anyone in the world.[[28]](#footnote-28) The proposed change of definition would thus narrow the scope of what is considered personal data under the UK GDPR[[29]](#footnote-29) and, arguably, it will provide controllers more certainty that they have anonymised data effectively so that they can ‘use it more innovatively within their organisations, or when shared with organisations that adhere to similar standards on anonymisation and re-identification.’[[30]](#footnote-30) Erdos offers a similar analysis arguing that this would represent ‘a plausible gloss on the definition found in the EU GDPR’.[[31]](#footnote-31) The proposal mirrors the principle adopted in *Breyer,* andin McCullagh’s view,that I share, it is unlikely to prove problematic when the UK adequacy decision is reviewed.

The second significant change relates to one of the lawful bases for the processing of personal data, i.e. the processing that is necessary for the legitimate interest of a data controller (Article 6(1)(f) UK GDPR). Currently, this ground can be used by a data controller to the extent that the controller conducts the so-called ‘balancing test’ and establishes that their interests are not outweighed by the interests of the individual.[[32]](#footnote-32) In the ‘Data: a New Direction’ consultation, the UK government stated that applying the balancing test is too complex and forces organisations to inappropriately rely on consent as a lawful basis for processing. The government then proposed to remove the balancing test for a limited list of legitimate interests specified in the DPDIB.[[33]](#footnote-33) The list includes matters of ‘public interest’, such as national security, public security, defence, emergencies, preventing crime, democratic engagement, and safeguarding children/vulnerable adults. McCullagh submits that the list of categories is unlikely to prove problematic when the UK adequacy decision is reviewed. However, she also notes that the DPDIB further stipulates that the Secretary of State may, in the future, amend this list so that more processing may be conducted on a legitimate interest basis without necessitating a balancing test.[[34]](#footnote-34) The amendments would need to undergo an affirmative resolution procedure, and the Secretary of State would explicitly have to regard data subjects' rights and fundamental freedoms, inter alia.[[35]](#footnote-35)

Thirdly, and more concerningly, there are proposals in the DPDIB that would reduce the independence of the ICO, the UK national data protection authority, which may attract scrutiny by the European Commission when the UK’s adequacy decision is reviewed. Under the proposal, the ICO would be reorganised into a corporate board with the primary objectives of securing an appropriate level of data protection and promoting trust and confidence in the data processing. However, the ICO would also be formally required to take into account other objectives, such as tackling crime and ‘promoting innovation and competition’.[[36]](#footnote-36) The ICO will need to have regard to the government’s strategic priorities (which will be set out by the Secretary of State in an official ‘statement of priorities’ laid before Parliament) when exercising its regulatory functions.[[37]](#footnote-37) There is also a provision for the Secretary of State to approve statutory ICO Codes of Practice. Erdos adds another concern to this list, noting that ‘the proposed changes do not effectively address the extremely limited reality of ICO enforcement action and, relatedly, the lack of an accessible mechanism to ensure that data subject complaints are properly handled’.[[38]](#footnote-38) In his detailed analysis, he points to various deficiencies in the ICO’s action, complaint handling, ineffective accountability and the lack of holistic scrutiny. To address this, Erdos advances a couple of solutions, including the proposition the Equality and Human Rights Commission (EHRC) should be required to review the ICO’s regulation biennially from a human rights perspective and lay the review before Parliament for democratic scrutiny.[[39]](#footnote-39)

Therefore, the question of the ICO’s independence remains particularly concerning in the context of adequacy. McCullagh rightly posits that if the UK government uses these proposals to limit the independence and regulatory freedom of the ICO, they are likely to affect the adequacy when the UK adequacy decision is reviewed. These issues might also warrant close scrutiny by the Commission as the European Data Protection Supervisor has observed: ‘that any changes that make it less independent or require it to push through a political agenda will naturally force the Commission to raise concerns, ask questions, and seek assurances.’[[40]](#footnote-40) Additionally, the UK adequacy decision contains a sunset clause and it is valid for four years expiring on 27th of June 2025 if the Commission has not renewed it by then.[[41]](#footnote-41) In McCullagh’s opinion, this combination of continuous review and a sunset clause ‘will exert pressure on the UK to identify deficiencies and ensure that it does not diverge to a significant extent from the EU GDPR standard if the UK is to secure a renewed adequacy decision in the coming years.’[[42]](#footnote-42) McCullagh also believes that, once Brexit was perceived to be ‘done’ and no longer the focus of intense political scrutiny in the UK, the UK government might be more accepting of the need to address deficiencies in the UK legal framework to retain it because of the economic consequences that would flow from disruption of EU-UK personal data transfers. Erdos, however, is not so optimistic and points at the dangers of granting the Government powers to amend data protection and e-privacy laws under statutory instruments outside the full and open democratic discourse through primary legislation, which ‘may indicate that the direct changes set out in this Bill may simply be the first stage in UK data protection reform’.[[43]](#footnote-43) His pessimism perhaps stems from the finding that ‘almost all of the changes proposed are weighted in favour of those who control rather than who are the subject of personal data.’[[44]](#footnote-44)

There are other changes proposed in the DPDIB, notably those related to the purpose limitation principle and research, archiving and statistical purposes, the solely automated decision-making right, and some of the compliance and accountability mechanisms (the data protection office obligation, data breaches, data protection impact assessments). These proposals have been analysed in detail by Erdos, and I invite you to consult his research for more detail. Importantly for this analysis, their introduction would not create a radical shift from the current regime either.[[45]](#footnote-45)

In conclusion, the analysis above suggests that the proposed changes to the UK data protection law are indeed mainly evolutionary and are therefore likely to be favourably received during any review of the adequacy decision by the Commission.[[46]](#footnote-46) I do however, submit that the proposals affecting the ICO independence and the Secretary of State having the power to add to the list of legitimate interest categories and amend the law through secondary legislation will increase divergence from the GDPR and, in tandem with other technology law reforms, could compromise the UK adequacy decision in the foreseeable future.[[47]](#footnote-47) Looking at this relationship from the perspective of Armstrong’s regulatory model set out above, the EU may need to resort to hierarchy as a regulatory model to maintain regulatory alignment. However, due to the importance of trade between the UK and the EU, co-operation and market as regulatory models may interact with hierarchy and allow for a level of divergence in the area of data protection and e-privacy that may not be entirely compatible with the requirement of ‘essentially equivalent’ data protection regimes.

**III. The Online Safety Bill**

The Online Safety Bill seems to be a never-ending bundle of uncertainty.[[48]](#footnote-48) Following the initial Online Harms White Paper,[[49]](#footnote-49) the Bill was introduced in the Parliament in May 2021, and the current version includes amendments by the Public Bill Committee and the new Government.[[50]](#footnote-50) Leiser and I have criticised the reform since its inception, and it is not my intention to rehearse these points again here.[[51]](#footnote-51) *Inter alia*, we focused on the premise of the risk-based regulation, duty of care and the human rights implications of the Bill, emphasising the inadequate provision aimed at protecting privacy and the freedom of expression.[[52]](#footnote-52)

The Online Safety Bill is a gigantic document of 230 pages. In the whole Bill, however, data protection as a term has been mentioned only five times in the context of the disclosure of information to Ofcom, the UK’s communications regulator.[[53]](#footnote-53) The term personal data has been mentioned eleven times.[[54]](#footnote-54) This may seem superficial, but I deem this an indication of the importance the Bill places on data protection and the right to privacy.

In the latest iteration of the Online Safety Bill, there has been some improvement compared to the initially very vaguely defined service providers' duty to have regard to the importance of the protection of privacy and the freedom of expression.[[55]](#footnote-55) The revised clause 20 expands on the duty about privacy and free speech, requiring service providers to ‘have regard to the importance of protecting users from a breach of any statutory provision or the rule of law concerning privacy that is relevant to the use or operation of a user-to-user service (including but not limited to, any such provision or rule concerning the processing of personal data)’[[56]](#footnote-56) when designing their processes and policies. This is quite an imprecise provision where the Bill seems to conflate privacy and data protection as mechanisms and concepts.[[57]](#footnote-57) Leaving that conceptual distinction aside, the clause still broadly refers to the data protection regime and relates safety measures to comply with the data protection law and privacy. The provision emphasises the importance of having a robust data protection law that service providers need to comply with in the context of online safety. That also may sound quite superfluous since data protection compliance has been established much more strongly in data protection law, requiring not only ‘having regard to its importance’, but requiring strict compliance with data protection principles and other provisions under a threat of hefty fines. Therefore, compliance with the data protection law in clause 20 of the Bill appears quite vague and almost optional. On the other hand, this provision potentially invites scrutiny of the online safety law (if passed in this form) in the UK data protection adequacy assessment context. The link between online safety and data protection established here, albeit vague and insufficient, invites the European Commission to consider the law, if adopted, in the context of the adequacy assessment. As noted in the previous section, the Commission is required to assess not only data protection law *stricto sensu*, but also the rule of law, respect for human rights and fundamental freedoms, relevant legislation etc. The online safety legislation most certainly falls within such ‘relevant legislation’ remit.

While clause 20 refers to data protection very explicitly, other proposals in the Bill may also impact data protection safeguards more impliedly. One of the biggest concerns related to Bill’s impact on privacy and data protection is the likely requirement that service providers proactively monitor personal data to comply with the duty of care.[[58]](#footnote-58) This requirement is set out in clause 120, entitled ‘Confirmation decisions: proactive technology’, which empowers Ofcom to require proactive monitoring by use of technology (e.g. algorithms, keyword matching, image matching, image classification or behaviour pattern detection). Ofcom can impose the use of such technology when ordering a service provider to comply with a duty pertaining to illegal content, children’s online safety and fraudulent advertising. The clause also prohibits the use of this except to analyse ‘user-generated content communicated publicly’ and ‘metadata relating to user-generated content communicated publicly’. However, the fact that the data is shared publicly does not mean that it is not personal and that the monitoring obligation does not extend to compromise user privacy and data protection rights. Under EU law, and in particular with regard to the e-Commerce Directive, a general monitoring obligation of a sort is prohibited and will remain so with the introduction of the Digital Services Act.[[59]](#footnote-59) The UK has always had an unsettling stance towards this obligation since Article 15 of the e-Commerce Directive appears nowhere in UK domestic legislation.[[60]](#footnote-60) The Online Safety Bill confirms this.[[61]](#footnote-61)

Another concern relates to end-to-end encryption (E2EE). Clause 106 of the Bill grants the Ofcom a new power to issue notices to service providers requiring them to identify and take down terrorism content that is communicated ‘publicly’ by means of their services or Child Sex Exploitation and Abuse (CSEA) content being communicated ‘publicly or privately’. The inclusion of ‘private’ communications raises concerns related to E2EE. In the recently published report, Ryder and Wills take the view that the Bill, rather than forcing messaging platforms to abandon E2EE, will push them towards deploying a controversial technology called client-side scanning (CSS) to comply with notices issued by Ofcom. CSS refers to systems that scan message contents for matches or similarities to a database of problematic content before the message is sent to the intended recipient.[[62]](#footnote-62) According to Ryder and Wills, CSS is ‘likely to be the primary technology whose use is mandated’.[[63]](#footnote-63) They thus conclude: ‘The Bill notes that the accredited technology referred to c.104 is a form of “content moderation technology”’, meaning ‘technology, such as algorithms, keyword matching, image matching or image classification, which […] analyses relevant content (c.187(2)(11). This description corresponds with CSS.’[[64]](#footnote-64)

Furthermore, a recent government’s amendment to the Bill provides that a provider given a technology notice has to make such changes to the design or operation of the service as are necessary for the technology to be used effectively. This is another argument in favour of concerns around requiring E2EE to be modified, ‘which might, for instance, involve client-side scanning.’[[65]](#footnote-65) The integrity of E2EE is crucial not only for the confidentiality and privacy of communications but also for moral and essential cybersecurity reasons. Researchers have provided very solid evidence that compromising E2EE compromises the network security and safety of the same users we wish to protect. [[66]](#footnote-66)

Provided that the Bill is passed, its actual impact is yet to be seen since a lot of its implications will depend on Ofcom’s codes of practice and the relevant secretary of state’s regulations. It will also depend on the relationship between data protection and online safety regimes, their overlaps and tensions. Ofcom and the ICO have issued a joint statement outlining their common objectives, shared competences and cooperation in implementing the online safety law.[[67]](#footnote-67) Ofcom promises to engage with the ICO from an early stage in developing its proposals for the codes and guidance required by the Bill and, where appropriate, publish the ICO’s formal responses to their consultations. The ICO commits to publishing its expectations on how safety technologies that use personal data should be developed in line with data protection law. They commit to collaborating within the Digital Regulation Cooperation Forum (DCRF).[[68]](#footnote-68) Some of their planned actions include: building and maintaining a common understanding of the areas of overlap and tension between the data protection and online safety regimes; engaging with industry to understand the practical challenges of complying with both regimes; collaboration in developing policy and guidance; and ‘establishing effective processes to maintain mutual awareness of our supervisory and enforcement actions’.[[69]](#footnote-69) What is missing there is a much greater emphasis on the tensions within the general monitoring obligation and E2EE, as discussed above. These areas are mentioned in the statement as 'examples' rather than major concerns that they are. Second, the regulators promise to 'engage with industry to understand the practical challenges of complying with both regimes', seemingly and unfairly excluding civil society, academia, and users. Finally, there does not seem to be a recognition of the regulatory capacities in this statement. Notwithstanding Erdos’ findings about the ICO enforcement deficiencies, a question of these commitments' practical and effective viability arises.

In summary, what can be drawn from the face of the Bill and analysis of the likely consequences is that the Bill threatens to undermine privacy and data protection rights. The essence of this Bill, if adopted in this or similar form by the Parliament, may affect the UK's data protection and privacy rights. The Bill is, therefore, likely to increase the level of regulatory divergence between the UK and the EU in the area of privacy and data protection, but also technology law and regulation more broadly. I submit that the European Commission should review the Bill in the context of the adequacy decision periodic review. In this exercise, the Commission would, again, exert hierarchy as a regulatory model to ensure that regulatory alignment is broadly maintained in the context of privacy and data protection rights.

The example of the proposed Human Rights Act reform would add to the divergence even further had the government decided to proceed with the reform. Fortunately, as it stands, the reform has been scrapped, but given the political turmoil noted above, it is not difficult to imagine that a similar proposal could be tabled by a new government in the future.[[70]](#footnote-70) To exemplify, the previous proposal barely mentioned data protection (only in Appendix 1 Examples of relevant domestic legislation and common law provisions which cover Articles within the HRA and in the context of Article 8 ECHR, where the DPA and UK GDPR were mentioned). Privacy was mentioned a few times, but even that was insufficient as it only appeared in the context of human rights balancing acts, i.e. the freedom of expression vs the rights to privacy balancing exercise by the courts.[[71]](#footnote-71) The proposal placed a much greater emphasis on the freedom of expression, and the balance between this right and the right to privacy could have been arguably disrupted if the proposal had gone through.

**IV. The emerging UK AI regulation**

It is hard to offer solid answers as to what the UK AI regulation may look like. There are ongoing government consultations, so we can only draw some conclusions from various consultation documents and strategies the government has introduced so far. Consequently, the impact of this reform on the data protection regime and adequacy is difficult to predict at the moment. However, we can derive some more general conclusions as to the nature and contours of this impact.

The National AI Strategy published in 2021 supported the proposals of the consultation ‘Data: A new direction’ analysed above*.* Theshort-term goal is to ‘determine the role of data protection in wider AI governance following the Data: A new direction consultation’.[[72]](#footnote-72) This has changed due to the revisions introduced in the DPDIB, noted above. Amendments have been proposed to the GDPR Article 22 right related to automated decision-making and processing, but this is not a radical shift either.[[73]](#footnote-73) In clause 11, the Bill provides additional statutory clarification of the thresholds, i.e. that automated decisions can include ‘profiling and carrying out profiling’, and that solely automated means that ‘there is no meaningful human involvement in the taking of the decision’. The Bill also narrows rights not to be subject to such decisions which are based entirely or partly on special categories of data. The Bill confirms and specifies that the safeguards which must apply when solely automated decision-making produce legal or similarly significant include the provision of information about and the enabling of them to make representations, to obtain human intervention and contest a decision. Moreover, subject to parliamentary approval under the affirmative resolution procedure, the Secretary of State would be granted power under statutory instrument to determine what is a ‘similarly significant effect’ and to amend the safeguards required of controllers in this area. Considering the substantive changes to this right, Erdos argues that these ‘seriously narrow the circumstances when a data subject will be able to resist automated decision-making entirely’. Consequently, he argues, an emphasis is placed on the general safeguards which are subject to slightly expanded specification, which target the key risks that have been located in this area (transparency, fairness etc.).[[74]](#footnote-74)

As analysed above, overall, the Bill includes fewer provisions that diverge from GDPR. However, the AI Strategy and the subsequent government consultation document both refer to innovation, trade, and data flows as policy goals, noting that these would be championed ‘while maintaining the UK’s high standards for personal data protection.’[[75]](#footnote-75) This is an extremely difficult balance to strike, and following the above analysis, it could be argued that the former goal may be championed to the detriment of the latter.

Turning to the proposed AI regulatory framework, notably, it rejects primary legislation in most cases and relies on self-regulation, industry standards and regulation by the existing regulators and their forum – DCRF.[[76]](#footnote-76) Many commentators have expressed concerns around the proposal, ranging from concerns about the algorithmic governance and scrutiny to the actual power, capacity and legitimacy of the regulators and the DCRF. In chapter 7, Mitrou compares the current attempts to regulate artificial intelligence in the UK and the EU. She notes that the EU AI Act proposal is ‘the most important and influential regulatory step taken on the international level and, if not the first, the most comprehensive one.’ Similar to the GDPR, the AI Act could become a global model, mostly due to its extraterritorial scope.[[77]](#footnote-77) The UK, however, claims that ‘having exited the EU, we have the opportunity to build on our world leading regulatory regime’[[78]](#footnote-78) and become a ‘global AI superpower’ with ‘the most trusted and pro-innovation system of governance in the world.’[[79]](#footnote-79) Scholars find that the UK could achieve desirable leadership or competitive position in AI regulation concerning some aspects of the regulatory approach.[[80]](#footnote-80) However, they also view regulation as the ‘missing link on the UK’s overall AI strategy’[[81]](#footnote-81), a gap that the UK needs to address to become an AI superpower. Researchers note that the reality sets constraints to the UK’s ability ‘to establish a unique post-Brexit governance regime for AI’, as ‘the EU’s shadow continues to loom large over UK policymaking’.[[82]](#footnote-82) At the same time, they criticise the UK’s data protection reform as ‘misguided for ensuring ethical outcomes and innovation’.[[83]](#footnote-83)

Irrespective of the actual form and detail the UK AI regulation will adopt following the consultation, these concerns relate to the heart of the reform and its policy goals that are unlikely to change. It is thus safe to assume that the reform may compromise data protection in favour of innovation and growth. This is, therefore, another area of divergence for the European Commission to consider when reviewing the UK’s adequacy decision. This relationship, once more, cannot be viewed through the lens of regulatory co-operation that would result in regulatory alignment. Instead, the effects of the UK AI regulation are currently predominantly viewed through the lens of hierarchy and the EU’s threat of revoking data protection adequacy if the regulation impacts data protection adversely.

**V. Conclusion**

This chapter examined the potential effects of the UK’s ongoing ‘digital law reform package’, including the new data protection, online safety and AI regulation bills, on data protection and international data transfers. I considered these effects through the lens of Armstrong’s regulatory alignment/divergence model. I challenged the reform proposals on the basis of their divergence and inconsistency with EU law. I submitted that the technology (and other) law reform needs to be approached holistically, or we risk unintended and adverse consequences, not only on the implementation and 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. A piecemeal reform could lower data protection standards in practice and thus risk adequacy in international data transfers.

To address this, the UK government should consider the effects of hierarchy, co-operation,[[84]](#footnote-84) market and network modes of regulation and analyse their interaction in the area of technology law and policy. A comprehensive regulatory approach should be guided by the need to enable commercial data transfers with the EU and protect the digital rights of UK citizens. Currently, both policy goals seem to be undermined.

1. British government, Briefing notes, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/524040/Queen_s_Speech_2016_background_notes_.pdf>; Philip Johnston, ‘Do you want your sovereignty back? Then vote Leave the EU’ (8 February 2016, The Telegraph) <http://www.telegraph.co.uk/news/news/newstopics/eureferendum/12146990/Do-you-want-sovereignty-back-Then-vote-to-leave-the-EU.html>; See more in Chapter 11 of this book. [↑](#footnote-ref-1)
2. Sebastian Payne and Jane Croft, ‘ Liz Truss scraps proposed British bill of rights’, (Financial Times, 7 September 2022), <https://www.ft.com/content/9b0a32fc-980b-4f00-9cf5-6c3f29756800>. [↑](#footnote-ref-2)
3. Rowland Manthorpe, ‘Online Safety Bill: Culture Secretary Nadine Dorries vows to get tough on tech firms - as executives could face jail for breaches’, (Sky News, 4 November 2021), <https://news.sky.com/story/online-safety-bill-culture-secretary-nadine-dorries-vows-to-get-tough-on-tech-firms-as-executives-could-face-jail-for-breaches-12459767>; John Woodhouse et. al., ‘The Data Protection and Digital Information Bill 2022-23’, (UK Parliament Research briefing, 06 September 2022), <https://commonslibrary.parliament.uk/research-briefings/cbp-9606/>. [↑](#footnote-ref-3)
4. UK Government, Establishing a pro-innovation approach to regulating AI, CP 728, 20 July 2022, <https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai/establishing-a-pro-innovation-approach-to-regulating-ai-policy-statement> [↑](#footnote-ref-4)
5. Kenneth A. Armstrong, ‘Regulatory alignment and divergence after Brexit’, (2018) *Journal of European Public Policy*, 25:8, 1099-1117, DOI: [10.1080/13501763.2018.1467956](https://doi.org/10.1080/13501763.2018.1467956), 1115. [↑](#footnote-ref-5)
6. Ibid, 1104 – 1105. [↑](#footnote-ref-6)
7. On the point, see Ch 10 by Costello in this volume. [↑](#footnote-ref-7)
8. Ibid, 1105. [↑](#footnote-ref-8)
9. See chapters 2, 3, 7 and 9.. [↑](#footnote-ref-9)
10. K McCullagh, ‘Brexit: potential trade and data implications for digital and ‘fintech’ industries’ [2017] 7(1) International Data Privacy Law 3-21; and Chapter 2. [↑](#footnote-ref-10)
11. See Chapter 3. [↑](#footnote-ref-11)
12. David Erdos, ‘A Bill for a Change? Analysing the UK Government’s Statutory Proposals on the Content of Data Protection and Electronic Privacy’ (September 7, 2022). University of Cambridge Faculty of Law Research Paper No. 13/2022, Available at SSRN: https://ssrn.com/abstract=4212420 or <http://dx.doi.org/10.2139/ssrn.4212420>; ‘Towards Effective Supervisory Oversight? Analysing UK Regulatory Enforcement of Data Protection and Electronic Privacy Rights and the Government’s Statutory Reform Plans’ (November 28, 2022). University of Cambridge Faculty of Law Research Paper No. 16/2022, Available at SSRN: https://ssrn.com/abstract=. [↑](#footnote-ref-12)
13. See, for example: C Kuner et al, ‘The global data protection implications of ‘Brexit’’ [2016] 6(3) International Data Privacy Law 167-169; A Murray, ‘Data transfers between the EU and UK post Brexit?’ [2017] 7(3) International Data Privacy Law 149-164; L Moerel and R Tigner, ‘Data Protection Implications of Brexit’ [2016] European Data Protection Law Review 381-383; O Butler, ‘The implications of a ‘no-deal’ Brexit for data protection in the United Kingdom’ [2019] 3(1) Journal of Data Protection & Privacy 8-20; P de Hert and V Papakonstantinou, ‘The rich UK contribution to the field of EU data protection: Let’s not go for “third country” status after Brexit’ [2017] 33(3) Computer Law & Security Review 254-260; A Vanberg and M Maunick, ‘Data Protection in the UK post-Brexit: the only certainty is uncertainty’ [2018] International Review of Law, Computers & Technology 190-206; K McCullagh, ‘Brexit: potential trade and data implications for digital and ‘fintech’ industries’ (n 8). [↑](#footnote-ref-13)
14. European Commission, 'Data protection: European Commission launches process on personal data flows to UK' 19 Feburary 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip\_21\_661 [↑](#footnote-ref-14)
15. European Commission 'Data protection: Commission adopts adequacy decisions for the UK' (European Commission, 28 June 2021), https://ec.europa.eu/commission/presscorner/detail/en/ip\_21\_3183 [↑](#footnote-ref-15)
16. Case C-362/14, *Maximillian Schrems v Data Protection Commissioner,* (“*Schrems I*”), ECLI:EU:C:2015:650, para 81. [↑](#footnote-ref-16)
17. EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, <https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en>. [↑](#footnote-ref-17)
18. Article 29 Working Party, ‘Adequacy Referential’ adopted on 28 November 2017, as last revised and adopted on 6 February 2018, WP254 rev.01 (endorsed by the EDPB, the Art 29WP successor body), <https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines>. For a more in-depth analysis, see Chapter 2. [↑](#footnote-ref-18)
19. Out-Law news, ‘GDPR will come into force in the UK in 2018, minister confirms’ (Pinsent Masons, 9 November 2016), https://www.pinsentmasons.com/out-law/news/gdpr-will-come-into-force-in-the-uk-in-2018-minister-confirms. See also Edoardo Celeste, ‘Data Protection’ in Federico Fabbrini, *The Law & Politics of Brexit: Volume III* (Oxford University Press 2021). [↑](#footnote-ref-19)
20. Department for Digital, Culture, Media & Sport, ‘Data: A new direction’, 10 September 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/1022315/Data\_Reform\_Consultation\_Document\_\_Accessible\_.pdf. [↑](#footnote-ref-20)
21. Ibid. [↑](#footnote-ref-21)
22. See, for example: W Damen et al, ‘Data protection in post-Brexit Britain: A response to the Government of the United Kingdom’s public consultation on reforms to the data protection regime (“Data: A new direction”)’ [2021] Leadership, Enterprise & Diversity Lab, University of Birmingham. [↑](#footnote-ref-22)
23. Data Protection and Digital Information Bill. https://publications.parliament.uk/pa/bills/cbill/58-03/0143/220143.pdf. [↑](#footnote-ref-23)
24. For more detail see Erdos, ‘A Bill for a Change? Analysing the UK Government’s Statutory Proposals on the Content of Data Protection and Electronic Privacy’, (n 10). [↑](#footnote-ref-24)
25. McCullagh, Chapter 2. [↑](#footnote-ref-25)
26. Erdos, ‘A Bill for a Change? Analysing the UK Government’s Statutory Proposals on the Content of Data Protection and Electronic Privacy’, (n 12), 2. [↑](#footnote-ref-26)
27. Data Protection and Digital Innovation Bill, (n 23) c. 1(2). [↑](#footnote-ref-27)
28. Consistent with the EU case law. [↑](#footnote-ref-28)
29. This reflects the position in *Breyer v Bundesrepublik Deutschland,* Case C-582/14 Patrick Breyer [2016] EU:C:2016:779, Opinion of AG Campos Sánchez-Bordona, para 65. [↑](#footnote-ref-29)
30. DCMS, ‘Data: A new direction,’ (n 20), 46. [↑](#footnote-ref-30)
31. Erdos ‘A Bill for a Change? Analysing the UK Government’s Statutory Proposals on the Content of Data Protection and Electronic Privacy’, (n 12), 5. [↑](#footnote-ref-31)
32. GDPR, art. 6 1. (f). [↑](#footnote-ref-32)
33. Erdos ‘A Bill for a Change? Analysing the UK Government’s Statutory Proposals on the Content of Data Protection and Electronic Privacy’, (n 12), 7-8. [↑](#footnote-ref-33)
34. Chapter 2. [↑](#footnote-ref-34)
35. Data Protection and Digital Innovation Bill, (n 20), Clause 5 [↑](#footnote-ref-35)
36. Ibid, Clause 27; Section 120B; Erdos, ‘Towards Effective Supervisory Oversight? Analysing UK Regulatory Enforcement of Data Protection and Electronic Privacy Rights and the Government’s Statutory Reform Plans’ (n 7), 3. [↑](#footnote-ref-36)
37. Data Protection and Digital Innovation Bill, (n 20), Clause 28. [↑](#footnote-ref-37)
38. Erdos, ‘Towards Effective Supervisory Oversight? Analysing UK Regulatory Enforcement of Data Protection and Electronic Privacy Rights and the Government’s Statutory Reform Plans’ (n 12) 3. [↑](#footnote-ref-38)
39. Ibid. [↑](#footnote-ref-39)
40. Neil Hodge, ‘EDPS: U.K. GDPR reforms could create friction with EU,’ (Compliance Week, 13 July 2022)

    <https://www.complianceweek.com/data-privacy/edps-uk-gdpr-reforms-could-create-friction-with-eu/31851.article>. [↑](#footnote-ref-40)
41. Art 45 (3) GDPR; European Commission, Commission Implementing 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, C(2021) 4800 final, <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> Article 4, recitals 289-290. [↑](#footnote-ref-41)
42. Chapter 2. [↑](#footnote-ref-42)
43. Erdos ‘A Bill for a Change? Analysing the UK Government’s Statutory Proposals on the Content of Data Protection and Electronic Privacy’, (n 12), 23. [↑](#footnote-ref-43)
44. Ibid. [↑](#footnote-ref-44)
45. Ibid, 5-11. [↑](#footnote-ref-45)
46. Chapter 2. [↑](#footnote-ref-46)
47. Ibid. [↑](#footnote-ref-47)
48. Mark Leiser, ‘The Online Safety Bill is a mystery wrapped in a riddle inside an enigma’, (The Drum, 17 November 2022), <https://www.thedrum.com/opinion/2022/11/17/the-online-safety-bill-mystery-wrapped-riddle-inside-enigma>. [↑](#footnote-ref-48)
49. UK Government, ‘Online Harms White Paper: Full Government Response to the Consultation’, <https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response>. [↑](#footnote-ref-49)
50. Online Safety Bill, as amended on report, 6 December 2022, <https://bills.parliament.uk/bills/3137/publications> [↑](#footnote-ref-50)
51. Mark Leiser and Edina Harbinja, ‘Content not available: Why the United Kingdom’s Proposal For A ‘Package Of Platform Safety Measures’ Will Harm Free Speech’ (2020) Technology and Regulation 78-90; Edina Harbinja and Mark R. Leiser, ‘[Redacted]: This Article Categorised [Harmful] by the Government’ (2022) 19:1 SCRIPTed 88 https://script-ed.org/?p=4050. [↑](#footnote-ref-51)
52. Ibid. [↑](#footnote-ref-52)
53. Online Safety Bill (n 50). [↑](#footnote-ref-53)
54. Counted by the author. [↑](#footnote-ref-54)
55. Harbinja and Leiser (n 51). [↑](#footnote-ref-55)
56. Online Safety Bill (n 50), c. 20. [↑](#footnote-ref-56)
57. Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP, 2015), Chapter 4. [↑](#footnote-ref-57)
58. Graham Smith, ‘Mapping the Online Safety Bill’, (CyberLeagle, 27 March 2022), <https://www.cyberleagle.com/2022/03/mapping-online-safety-bill.html>. [↑](#footnote-ref-58)
59. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance), OJ L 277, 27.10.2022, p. 1–102. [↑](#footnote-ref-59)
60. Graham Smith, ‘Time to speak up for Article 15’, (CyberLeagle, 27 March 2022), <https://www.cyberleagle.com/2017/05/time-to-speak-up-for-article-15.html> [↑](#footnote-ref-60)
61. Smith (n 58). [↑](#footnote-ref-61)
62. ISOC, ‘Fact Sheet: Client-Side Scanning’, 24 March 2020, <https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/> [↑](#footnote-ref-62)
63. Matthew Ryder KC and Aidan Wills, ‘Surveilled and exposed: How the Online Safety Bill creates insecurity’ (Index for Censorship, 31 October 2022) <https://www.indexoncensorship.org/2022/11/new-legal-opinion-on-the-online-safety-bill/>. [↑](#footnote-ref-63)
64. Ibid, 22. [↑](#footnote-ref-64)
65. Smith (n 58). [↑](#footnote-ref-65)
66. Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague, Carmela Troncoso, “Bugs in our Pockets: The Risks of Client-Side Scanning”, Oct 14, 2021; Chat Control or Child Protection? Ross Anderson, arXiv:2210.08958v1 [cs.CY] <https://doi.org/10.48550/arXiv.2210.08958> [↑](#footnote-ref-66)
67. Ofcom and ICO, ‘Online safety and data protection: a joint statement by Ofcom and the Information Commissioner’s Office;, 25 November 2022, <https://www.gov.uk/government/publications/online-safety-and-data-protection-a-joint-statement-by-ofcom-and-the-information-commissioners-office> [↑](#footnote-ref-67)
68. Ibid, 12. [↑](#footnote-ref-68)
69. Ibid. [↑](#footnote-ref-69)
70. See the Bill of Rights Bill (2022) and the report of the ‘Independent Human Rights Act Review’ available at <https://www.gov.uk/guidance/independent-human-rights-act-review#about-the-independent-human-rights-act-review> accessed 27 July 2022; Ministry of Justice ‘Human Rights Act Reform: A Modern Bill of Rights – consultation’ (2022), ch. 4. [↑](#footnote-ref-70)
71. Ministry of Justice ‘Human Rights Act Reform: A Modern Bill of Rights – consultation’ (2022), ch. 4. Para. 206, 214, 215; see also Chapter 10. [↑](#footnote-ref-71)
72. HM Government, ‘National AI Strategy’, September 2021, CommandPaper 525, <https://www.gov.uk/government/publications/national-ai-strategy>, 51. [↑](#footnote-ref-72)
73. David Erdos, ‘A Bill for a Change? Analysing the UK Government’s Statutory Proposals on the Content of Data Protection and Electronic Privacy’ (n 12) 16-18. [↑](#footnote-ref-73)
74. Ibid, pp. 16 - 18. [↑](#footnote-ref-74)
75. HM Government (n 72). [↑](#footnote-ref-75)
76. UK Government (n 4). [↑](#footnote-ref-76)
77. See Chapter 7. [↑](#footnote-ref-77)
78. UK Policy paper Digital Regulation: Driving growth and unlocking innovation, 6 July 2021, <https://www.gov.uk/government/publications/digital-regulation-driving-growth-and-unlocking-innovation> [↑](#footnote-ref-78)
79. National AI Strategy, GOV.UK. (2021). <https://www.gov.uk/government/publications/nationalai-strategy/national-ai-strategy-html-version> [↑](#footnote-ref-79)
80. Ada Lovelace Institute, Regulate to Innovate, 29 November 2021, <https://www.adalovelaceinstitute.org/report/regulate-innovate/#:~:text=A%20report%20which%20sets%20out,beneficial%20for%20people%20and%20society>. [↑](#footnote-ref-80)
81. Ibid, 9, 12. [↑](#footnote-ref-81)
82. H. Roberts, A. Babuta, J. Morley, C. Thomas, M. Taddeo and L. Floridi, ‘Artificial Intelligence Regulation in the United Kingdom: A Path to Global Leadership?’ (September 1, 2022). Available at SSRN: <https://ssrn.com/abstract=> [↑](#footnote-ref-82)
83. Ibid. [↑](#footnote-ref-83)
84. See some useful suggestions in Chapter 12. [↑](#footnote-ref-84)