Olesia Shmarakova[*]

DATA STRATEGIES AND DEVELOPMENT OF TRADE IN DATA: THREE POLICY APPROACHES

Abstract

The importance of data in the economy is no longer a debatable issue; it is taken for granted. Upon the recognition of this fact, many countries have been solving the problem of improving the quality and availability of data through the development of various models of data sharing for several years. Active academic and business discussions on data policy and governance have finally borne fruit: several jurisdictions have adopted national data strategies (or similar documents).

However, does the existence of a data strategy at the national level indicate that the best conditions for the development of data trade and data markets have been created? How is the strategic approach conducted at the state level related to the actual availability of data to private businesses?

Different jurisdictions define their data governance priorities differently, and the approaches outlined in the strategies are (or are not) reflected in subsequent "direct application" legislation.

This article is devoted to a comparative analysis of strategic documents in the field of data governance of the European Union, United Kingdom, and Russia in the context of their interrelation with the laws that directly regulate the legal regime of various categories of data for commercial turnover.

The first part of the paper will provide a brief overview of the data governance documents of the jurisdictions in question: the European Strategy for Data, the UK National Data Strategy, and the Russian national projects "Digital Economy" and "Data Economy," with a focus on the differences in goal-setting and their potential impact on the further development of both data legislation and digital markets in general.

In the second part of the paper, the EU, the UK, and Russia, respectively, will be analysed in relation to "tactical" legislation that has been adopted or is planned to be adopted in the wake of the said strategic documents. The comparative analysis will focus on those acts that address the regulation of data in commercial circulation, its accessibility for private business, and private business obligations related to data.

In particular, the impact on the data market of the EU Digital Package will be discussed and the recently adopted Data Act will be contraposed with the provisions of a similar initiative of the UK Data Protection and Digital Information Bill 2. Also, this section will touch upon the issue of recognizing data as a legal object under the laws of the relevant jurisdiction and the existence of a general regulation applying as *lex generalis* to any data category.

Finally, the last part of the article will be devoted to comparing the provisions defined at the strategic level with the changes made to regulating data in commerce. Considering this analysis, a policy model for data governance based on the balance of interests of three actors: state, businesses, and individuals, will be described. Based on this approach, an attempt will be made to determine the actual priorities of the

[*] PhD candidate, University of Turin.

DOI 10.13135/2785-7867/11804

legislator for each of the jurisdictions under consideration and their potential impact on the further development of the data markets in these areas.
The article demonstrates that compared jurisdictions differ substantially in terms of the consequences of the chosen regulation path. While Russia may improve state services based on enhancing data availability, it does not aim to create a commercial market for data. Despite increasing data availability, the EU imposes restrictions on data holders. Extensive European regulation may impede data-driven businesses due to high compliance requirements. Conversely, both in the strategic documents and legislative proposal, the UK aims to create a business-friendly environment via precise and unburdensome regulation. Thus, the UK approach is the most effective for enhancing data trade.

JEL CLASSIFICATION: F68; H73; K11; K15; O38.

KEY WORDS: data strategy, data access, data sharing, data policy, trade in data

SUMMARY

1 Introduction

With the further development of the digital economy and the rise of Artificial intelligence technologies in particular, data are gaining more and more importance. Data is fuel for AI; data can be used to understand, predict, and even nudge the behaviour of the market incumbents. Thus, the legislation on data, initially developed in most countries from privacy laws, is becoming more complicated and starts to cover issues well outside of the traditional privacy domain.

The recent adoption of the first strategic documents relating specifically to data governance confirms that governments from different jurisdictions acknowledge the importance of data. The EU has adopted the European Data Strategy for data, the UK – the National Data Strategy, and Russia – the federal "Data Economy" project. These documents lay down the basic principles for the further development of state policy and legislation concerning data.

At first sight, the three compared jurisdictions seem to base their data strategies on the same principles, as they declare that economic development requires more data, i.e., data of better quality and more accessible. The other basis is enhancing the functioning of the economy via more extensive use of available data, application of new data analysis technologies, and creation of data-extensive projects in both public and private spheres.

Per the data strategies, the compared jurisdictions plan or adopt particular pieces of legislation dealing with specific data types or particular rights and obligations related to data. These regulations and strategic documents shape the reality of the data market in the relevant jurisdictions and set goals and limits for its further development.

This paper will analyse data's strategic and "tactical" regulation in three jurisdictions: the EU, the UK, and Russia, primarily concentrating on the new legislation adopted or proposed after the relevant strategies. Given the recent adoption of a significant package of substantial new legislation in the European Union, analysing its origins as a policy document on data is interesting. While many states worldwide have adopted or are developing data policies, this paper has chosen to focus on European space and explore how approaches vary within the same European continent. EU policies in this regard are interesting to compare with the UK's approach, as on the one hand, they share common origins, but on the other hand, post-Brexit, the UK has shown a conscious divergence in certain areas. To contrast these two jurisdictions, Russia also borrows a lot from European legislation and approaches but differs significantly in terms of goal-setting and the balance of interests of market participants. A comparative analysis of these three jurisdictions will give an idea of the existing approaches to data governance and trade in data, which are crucial for the market of the European continent.

The paper aims to describe a policy model for data governance in each jurisdiction based on the balance of interests of three actors: state, businesses, and individuals. The literature on the European data strategy and related legal acts is extensive due to the long preceding discussion; Kerber, van Erp, Gallese, and numerous Commission Communications' contributions should be named here. The UK part of the literature is more limited and relates primarily to commenting on particular pieces of legislation without a general analysis of the legal situation (Kemp). The same is true for Russia, as apart from a couple of comprehensive studies (collective monography by the Higher School of Economics and a dissertation of Mefodieva), scholarship is yet scarce on the matter. Moreover, no works performing comparative analysis in the field of data governance were identified concerning these jurisdictions. This contribution opens the topic for further study.

The paper will proceed as follows: the second chapter will be devoted to the analysis of strategic documents on data in each of the three jurisdictions; the third chapter will analyse for the same jurisdictions the particular legislative acts adopted in the wake and on the basis of the strategic documents; finally, the fourth part will define the policy approaches based on the documents above and compare them between the jurisdictions.

This paper's main object of interest is the data in commercial use and how the adoption of strategic documents or further legislation could have changed the situation in the "data market."

2 Data Strategies and their Goals

In recent years, many states, including those belonging to different legal systems and economic formations, have started adopting data governance and access development documents. It is important to emphasize that this is the first time that such documents

have been created at the level of state-wide (and in the case of the EU, even region-wide) strategies, and the relevant documents are, in each jurisdiction where they have emerged, the first of their kind. Although the challenges posed to states by the global world powered by data are the same, states approach them differently. The goals stated in data strategies correlate to a large extent with the state-wide policies and values pursued in the respective jurisdictions.

2.1 European Strategy for Data

Over the last twenty years, the European Union has adopted many acts regulating various aspects of data and information, both of a legislative and political-strategic nature. Of course, many Commission Communications are generally devoted to data, and the most essential document is the European Strategy for Data.[1] Several Commission Communications preceded the adoption of this document on data regulation (2014 - "Towards a data-driven economy"[2]; 2015 - "A Digital Single Market Strategy for Europe"[3]; 2017 - "Building a European data economy"[4]; 2018 - "Towards a common EU data space"[5]), which indicates a long and thorough elaboration of the issue. Further analyses will show that the initial position on specific aspects of data regulation has changed dramatically.

The Strategy sets four pillars as the basis for all future legislation in this field[6]:

(1) Cross-sectoral governance framework for data access and use to avoid internal market sectoral fragmentation.
(2) Enablers: Investments in data and strengthening Europe's capabilities and infrastructures for hosting, processing, and using data interoperability.
(3) Competences: Empowering individuals and investing in skills in SMEs.
(4) Common European data spaces in strategic sectors and domains of public interest.

The European Strategy for Data has identified the problems and devised an action plan to deal with them, including legislative and non-legislative actions.

Among problems, the fragmentation issue between the EU Member States was first on the list due to the EU's unique regulatory situation. Overcoming barriers between Member

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, 'A European strategy for data' [2020] COM(2020) 66 (European Strategy for data).
[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, 'Towards a thriving data-driven economy' [2014] COM(2014) 442 (Communication Towards a thriving data-driven economy).
[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, 'A Digital Single Market Strategy for Europe' [2015] COM(2015) 192 (Communication A Digital Single Market Strategy for Europe).
[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, 'Building a European data economy' [2017] COM(2017) 9 (Communication Building a European data economy).
[5] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions 'Towards a common European data space' [2018] COM/2018/232 final (Communication Towards a common European data space).
[6] Art. 5C of the European strategy for data.

States involves not only the harmonization of legislation but also the removal of existing restrictions in national legislation on cross-border data transfers if they occur in another EU country.

However, the second problem, namely the availability of data for innovative reuse, including the development of AI, is common through the compared jurisdictions. The issue of data interoperability and quality is another side of the coin of data availability in general.

Another essential aspect that is specifically noted in the EU Data Strategy is the imbalances in market power. The Commission notes that small numbers of large online platforms "accumulate large amounts of data, gathering important insights and competitive advantages from the richness and variety of the data they hold"[7], and their market power result in “data advantage”. As with any competitive advantage, leveraging data can affect the market's contestability, particularly in a situation where other market incumbents have no legal ways to obtain necessary data from "data monopolies".

The Strategy is a determinant not of the current, but of the future data governance framework in the EU. Based on the Strategy, we expect, on the one hand, a reduction in sectoral data regulation (first pillar) and, on the other hand, the creation of cross-border data pools in specific sectors (fourth pillar).

The focus on specific groups of data users and specific economic sectors makes the European approach the most concrete, even without high-level data regulation at the most general level.

It should be noted that in addition to a wide range of organizational issues, a significant emphasis is placed on the rights of individuals, and the foundations are laid for detailed regulation in the field of private law. One of the planned actions under the strategy is to empower individuals concerning their data and invest in skills and SMEs.

In particular, the Strategy has set up several particular details on how the future regulation in this regard is to be (and was) developed:

1) Providing individuals with more power to enforce their data rights, among other things, via technical tools and standards.
2) Empowering individuals to be in control of their data.
3) Creating means allowing individuals to decide what is done to their data at a granular level.
4) Enhancing data portability rights for individuals.

A special emphasis on the data rights of individuals and particular detail and specificity in this matter, including the granting of new rights, not just better protection of existing ones, distinguishes the European Data Strategy from similar documents in other jurisdictions.

[7] Art. 4 of the European strategy for data.

By now, a significant part of the initiatives provided in the European Strategy for data, at least in the legal domain, has already been realized, the last one is the recently adopted Data Act (DA)[8] along with the Digital Package (to be discussed in detail later).

Therefore, in the coming years, it is likely expected at the European level to take stock of the application of new legislation rather than adopt new strategic documents in this area (with the possible exception of the development of artificial intelligence regulation).

2.2 UK National Data Strategy

Speaking about UK law, it should be noted that the peculiarities of the legal regime of any legal object in comparison with the EU or Russian regulation are related not only to the specific choice of policy concerning this object but also, in general, to the differences between civil and common law. It is commonplace that common law is "less regulative," meaning that common law countries tend to legislate less and give more freedom to the judiciary to decide on what the law should be. However, any general analysis of differences between civil and common law is outside the scope of this paper. Thus, such differences will be presumed without any further comment.

Moreover, the analysis of UK law is further complicated by the fact that EU law was fully applicable when the UK was part of the EU and was phased out after Brexit under the Withdrawal Agreement[9], except 'assimilated law', which is the part of the EU law that was retained upon expiration of the transition period and has now become a new form of domestic UK law. [10] Therefore, for the sake of clarity of comparison, the UK part of this paper will be based on current law. In contrast, the historical analysis of EU law is also applicable to the UK during the period when the UK was part of the EU, and it is not possible to make a valid distinction in this case. This approach limits the scope of the UK part of the analysis to some extent and avoids unnecessary repetition. In addition, it should be noted that the laws of England and Wales will be used for the analysis.

The data governance issue came under the scrutiny of the UK government in the previous decade when the House of Commons discussed a report, "The Big Data Dilemma" (2015).[11] The report addressed different concerns relating to the data economy, emphasizing personal data protection. It is worth noting that even back in 2015, the UK claimed the world-leading data capabilities.

[8] Regulation (EU) 2022/868 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 [2018] OJ N Series L.

[9] Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community [2019] /C 384 I/01 OJ CI 384/1 (Withdrawal Agreement).

[10] Section 5 of the Retained EU Law (Revocation and Reform) Act 2023.

[11] The House of Commons, Science and Technology Committee, 'The big data dilemma' [2015].

The most important document relating to data of recent years is the National Data Strategy[12], adopted in 2020, which provides a framework for government actions on data. Similarly to the EU approach, the UK Strategy indicates four pillars (Part 2):

1) Data foundations relating to quality and format of data for further use.
2) Data skills relating to ability to exploit data.
3) Data availability relating to access and reuse of data.
4) Responsible data relating to limitations on data use imposed by law, ethics, fairness, sustainability, and accountability.

Missions indicated in the Strategy seem even more critical, as they show particular policy approaches to be taken by the UK government concerning data (Part 3 of the Strategy). It is indicated that the government aims to maintain "a data regime in the UK that is not too burdensome for the average company". Along with a more general goal to enhance the availability of data in general and to share governmental data more efficiently (which are also present in the EU strategic documents), the UK directly underlines that it aims at championing the international flow of data. A more detailed policy framework for the first mission indicated in the Strategy (usability and data availability) is already out.[13] Research carried out supporting this mission states that government intervention may be needed to reduce the present legal barriers to data sharing, particularly in intellectual property, use of data and digital technology, and industry-specific regulation).[14] The other document based on the UK National Data Strategy is the data-sharing governance framework,[15] that along with the Data sharing code of practice prepared by the Information Commission Officer[16] and Freedom of Information Act[17] constitutes the main pillars of the UK framework for public data sharing.

2.3 Russian strategic documents on Data

The development of data regulation in Russia is part of digital transformation, which is declared one of the national goals until 2030.[18]

[12] Department for Digital, Culture, Media & Sport, 'UK National Data Strategy' [2019] <www.gov.uk/government/publications/uk-national-data-strategy> accessed 22 June 2024.
[13] National Data Strategy Mission 1 Policy Framework: 'Unlocking the data value across the economy' [2021] <www.gov.uk/government/publications/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy> accessed 22 June 2024.
[14] Art. 2.1 of the UK Department for Digital, Culture, Media and Sport, 'Increasing access to data across the economy' [2021] <www.gov.uk/government/publications/increasing-access-to-data-held-across-the-economy> accessed 22 June 2024.
[15] UK Central Digital and Data Office, 'Data sharing governance framework' [2022] <www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework> accessed 22 June 2024.
[16] UK Information Commissioner's Office, 'Data sharing code of practice' (May 2021)</ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/> accessed 31 August 2024.
[17] UK Freedom of Information Act 2000.
[18] Decree of the President of Russian Federation 'On national development goals of the Russian Federation for the period until 2030' No. 474 of 21.07.2020.

Working on data regulation framework started even earlier, a strategic document in this area is the Presidential Decree on the Information Society Development,[19] which regulates big data processing, analysis, and data protection.

However, the prominent practical step in digital transformation and data regulation development was made by the federal project "Digital Public Administration," adopted as part of the national "Digital Economy of the Russian Federation" program in 2019. The national data management system was created to increase the efficiency of management decision-making based on the use of State information resources.[20] These regulations deal exclusively with public data and address public management goals.

This project was carried out from 2019 to 2024. It included a wide range of sub-projects and initiatives united by the concept of digitalization of the economy, from IT education for children and the provision of grants for talented students to the creation of numerous new digital public services.

Significant efforts during this period were aimed at digitalizing all spheres related to public administration, developing state information systems, and the online transfer of most interaction mechanisms between the state and citizens and businesses.

The digital sphere, including digital data issues, has received tremendous attention from the government. Among other things, changes concerning IT and the digital sphere have been introduced in the Russian Constitution: in the article concerning the subjects of federal jurisdiction in the system of division of powers between the federal authorities and the regions of the Russian Federation, "information technologies" was added, as well as "ensuring the security of the individual, society and the state in the application of information technologies, circulation of digital data".[21]

Previously, the Constitution did not regulate such issues; moreover, there is no definition of "digital data" in Russian law. However, these amendments and the broader trend towards digitalization, including the development of relevant legislation, have sparked a broad academic debate, from questions of constitutional human rights in the digital age to the digital sovereignty of the state.[22]

However, does a discussion of data turnover mean that there is a specific legal regime for digital data[23] and they become a tradable commodity? Despite the provisions of the Russian Constitution, the "digital data" regime has not yet been further developed in legislation.

[19] Decree of the President of Russian Federation 'On strategy for the information society development in Russian Federation for 2017-2030' No. 203 of 09.05.2017.

[20] Order of the Government of the Russian Federation 'On approval of the Concept of creation and functioning of the national data management system and the action plan ('roadmap') for creating the national data management system for 2019 – 2021' of 03.06.2019 No. 1189-r.

[21] Art.71 of the Constitution of the Russian Federation.

[22] Elena Alferova, 'Digital novels of the Constitution of the Russian Federation: a view of the legal scholars' (2023) 4 Social and humanitarian sciences 106.

[23] MV Yakushev and AA Efremov (ed), *Data Regulation in the Russian Federation: Current status, Problems, Prospects* (Higher School of Economics Publishing House, 2021).

In 2023, work started on a new national project, "Data Economy," until 2030, which will continue the Digital Economy project being finalized. The project will cover all stages of data handling, from data collection (which involves the creation of new sensors) to data transmission and developing communication systems, data storage and security, technical standardization, and data processing and analysis issues. The legislative plan will be created for 2024-2026 in the relevant spheres.

The aim is to create a management system based on big data in the economy and social sphere, whereas the digital infrastructure should be unified for the key industries and spheres.[24] At the same time, according to the president's statement, the Data Economy is necessary due to the threat to national security. Previously, many critical technologies were developed on foreign platforms.[25]

It is noted, though, that this project is, first of all, the state's initiative and not of the market players, and it aims to optimize state governance using big data.[26] For example, one of the project's goals is to build digital platforms in all sectors of the economy.

However, the government should not manage such platforms where there is no need. The project has been criticized for denationalizing the data market and design to create state or near-state monopolies instead of market mechanisms.[27]

Generally, the project includes initiatives aiming to digitalize the work of the government, provision of state services, develop domestic IT equipment, and further strengthen digital sovereignty[28].

Thus, Russia is currently working actively at the strategic state level to create a system of data regulation, including the introduction of new legislation. However, the initiatives are entirely in the area of public law and do not address the issues of private rights concerning data. The discussion of recent years in this area, unlike the European discussion, has never dealt with the development or change of regulation in the area of property or quasi-property rights to data. Since the projects under discussion are primarily concerned with state data or how the state manages data and have not addressed private rights issues, the claim of "state monopolization" of this area seems justified.

From the above comparisons of strategic data management policies and the reflection of the general concept of data or information in the law, all countries under consideration have paid much attention to the issue in recent years and are actively developing policies.

[24] Official communication of the Ministry of Digital Development, Communications, and Mass Media of the Russian Federation of 13 July 2023 [2023].
[25] Julia Tishina and Anna Oris, 'Data go on a national level' (*Kommersant*, 6 December 2023) <www.kommersant.ru/doc/6380045?ysclid=lxanueiplb230066310> accessed 11 June 2024.
[26] Tishina and Oris ibid.
[27] Karen Kazaryan and Irina Levova, 'Numbers for "digital": what is wrong with national project "Data economics"' (*Forbes.ru*, 5 March 2024) <www.forbes.ru/mneniya/507425-cifry-dla-cifry-cto-ne-tak-s-nacproektom-ekonomika-dannyh?ysclid=lxanuj7tjy327964660> accessed 11 June 2024.
[28] 'Data economics and digital transformation of the state' (*TAdviser.ru*, 18 May 2024) <https://www.tadviser.ru/a/745913> accessed 11 June 2024.

At the same time, significant differences are noticeable in target setting and the approach to regulation.

A comparison of strategic approaches to data management shows that all countries under consideration recognize the importance of data in the economy and note the need to develop data availability and reuse. However, significant differences may also be noted. As one of the strategic goals, the EU indicates the creation of common EU data spaces and fighting "internal borders" for data transfer, which is logically taking the possible different approaches and regulations in the Member States. The other policy goal of the EU is empowering individuals. Though the UK and Russia also address the issue of personal data protection in their strategic documents, unlike the EU, they plan to keep the legislation the same to provide any new rights concerning data. In this regard, an essential difference in EU policy is that it is aimed, among other things, to benefit the individuals. The Russian emphasis in data policy is on using data and enhancing government practices via digitalization. At the same time, businesses could reuse the data previously collected by the government. Thus, the state is the primary beneficiary of projects related to big data and the evolution of data governance. As for the UK, a market-oriented approach draws special attention, as the UK government emphasizes that UK companies should benefit from the practical and not too burdensome data regulatory framework. The UK also aims to support its championship in the global arena in this area. Thus, the UK approach is more utilitarian and favoring entrepreneurs.

3 Legislation in the Wake of Data Strategies

3.1 European strategy-based Acts

It should be noted that there is no legislation regulating data/information at the EU level, rather than a specific type. Though the European Strategy for Data operates with the concept of data as such, it does not directly establish a specific legal regime for data that would apply in all Member States. The EU has never discussed or planned to develop such a regulation. Since other regulations dealing with various types of data (such as GDPR[29], Database Directive[30]) are already in place, it would be difficult, if not impossible, to harmonize them for commercial purposes.

Member States, therefore, still have the option to regulate "data or information in general" at the level of national law, for example, in civil codes (provided that such a regime does not conflict with pan-European legislation on a particular type of data).

[29] Regulation of the European Parliament and of the Council No 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1 (GDPR).
[30] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases OJ L 77 (EU Database Directive).

Still, in the wake of the European Strategy for Data, several very important legal acts were adopted, dealing with various goals named in the Strategy: Data Governance Act (DGA)[31], Digital Markets Act (DMA)[32], Digital Services Act (DSA)[33], and, finally, the most recent Data Act (DA).

These acts fully or almost completely cover the directions of development of data regulation outlined in the Strategy, including those aimed at increasing data accessibility for private business and commercial turnover.

The DGA is a 'paired' document to the Open Data Directive[34] and regulates, first of all, the conditions for reuse within the EU of specific categories of data held by public sector bodies that the Open Data Directive does not cover. Adopting the DGA will allow the public sector to provide access to protected data (e.g., commercially confidential data) under certain conditions.

In addition, the DGA regulates a significant concept such as data altruism, that is defined as 'data altruism' means the voluntary sharing of data based on the consent of data subjects to process personal data on them or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest".[35]

These are the two most important innovations within the DGA aimed at enhancing data availability for further reuse and deleting the barriers relating to obtaining the data (for example, the need to receive consent to reuse personal data beyond the initial purpose of collection and processing.

Undoubtedly, the adoption of the DGA increases the opportunities for both public bodies and private businesses to access the necessary data. At the same time, the provisions of the DGA are inherently permissive: they impose certain obligations on public bodies, providing counter-opportunities for business.

The other two acts adopted in 2022 in fulfillment of the Strategy are rather opposite in balancing public and private interests concerning data. DSA and DMA primarily regulate obligations and set limits for digital businesses concerning different aspects of their activities, including operating with data. The regulation of data, including the issue of its availability for commercial circulation, is not central to these acts. However, applying their provisions inevitably affects, among other things, the regime of data generated in the provision of digital services.

[31] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 [2018] OJ L 152/1.
[32] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 OJ L 265/1.
[33] 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 [2022] OJ L 277/1.
[34] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information (recast) [2019] OJ L 172/56.
[35] Art. 2 (16) DGA.

DMA essentially aims to redistribute the benefits linked to the factual possibility of accessing and using the data between the "gatekeepers" (specifically designated undertakings providing core platform services) and the users of their services, both private and public. Thus, DMA changed the de facto situation by prohibiting the gatekeepers from using certain users' data for certain purposes and granting the users the right to access the data held by the gatekeepers. For example, gatekeepers shall not process personal data of end users using services of third parties that make use of the cope platform services of the gatekeeper in order to provide online advertising services (Art. 5(2)(a) DMA). Though the gatekeeper may continue accessing such personal data, their legal use is banned. Alternatively, the gatekeepers are obliged to provide business users access to data provided for or generated in the context of using relevant core platform services (Art. 6(10) DMA). Thus, on the one hand, DMA expands the possibilities of accessing and reusing data for some persons, and on the other hand, restricts them to the primary addressees of the act - gatekeepers.

Similarly, the DSA sets limitations and obligations concerning data for providers of online platforms, though significantly milder compared to the DMA. Thus, providers of online platforms cannot use users' data for advertisement (even though they have legal access to them) if they are aware and have reasonable certainty that the recipient is a minor (Art. 28(2) DSA). Providers of very large online platforms or very large online search engines are obliged to grant access to necessary data to public bodies (namely Digital Services Coordinator) and vetted researchers (Art. 40 DSA).

The most European relevant act in terms of making data more accessible to market participants is the recently adopted DA. Given the existence of a substantively similar bill in the UK, both of these instruments will be reviewed below in the form of a comparative analysis to highlight better the commonalities and differences in the data policies of these two jurisdictions.

3.2 UK Legislative Proposals on Data

As regards the legal regime of data as such in the UK (in particular in trade and within the horizontal relationships of market participants), the law of England and Wales does not acknowledge any legal (not to say property) rights in data. This approach is further confirmed by the Law Commission, noting that "digital things such as normal digital files that are not (as currently designed) capable of attracting personal property rights as a matter of law."[36]

The laws of England and Wales regulate rights related to data, both in intellectual property and contract law. While intellectual property issues will be discussed separately

[36] Art. 3.19 of the Law Commission's report, 'Digital assets as personal property. Short consultation on draft clauses' [2024] <lawcom.gov.uk/document/digital-assets-as-personal-property-draft-clauses/> accessed 31 August 2024 (UK Digital Assets Draft).

later, it should be noted that data-related contacts are mainly developed under English law, as legal consultants make particular advice for contract drafting.[37] Thus, a precisely defined status of the legal object is necessary for data tradability under contract law, provided the subject matter is defined enough.

It may be added that the laws of England and Wales do not contain any general legal definition of "data" or "information". Concerning data law, the proposal for the Property (Digital Assets) Act 2024 is an important initiative.[38] This proposal covers regulating digital assets such as crypto-assets, NFTs, etc. In its initial stage (2022) is utilized the terminology "data objects", was somehow confusing and was described as *"composed of data represented in an electronic medium, including in the form of computer code, electronic, digital or analog signals", however, further detalization showed that pure information was excluded* from becoming a data object.[39] Later, though the idea evolved to its current status, "data objects" were (more appropriately) renamed into "digital objects", and even the requirement for them to be "composed of data" was deleted as excessive.[40] The actual version of the proposal explicitly excludes information and data (in the form of digital files) as such[41] and implicitly, as the qualifying requirement for the digital asset is vivaciousness. Data, in general, though, is characterized by non-rivalry. Still, the Property (Digital Assets) Act proposal (part of the UK Digital Assets Draft) and previous Law Commission documents are of huge importance for data regulation in the UK, as they introduce completely new doctrinal concepts that can be applied to data, at least to some extent. Digital assets are summed up into the new "third category" of private property apart from things in possession and things in action.[42] Another important concept for data is "control", which is understood by the Law Commission in both factual dimensions ("ability to (1) exclude or to permit access to a third category thing; and (2) put the third category thing to the uses of which it is capable"[43]) and legal. The same concept lies in the basis of any data regulation, for example, personal data (figure of "controller) or trade secret (legal control), and is, to a large extent, applicable to data without any changes.

Thus, although the legislation of England and Wales does not regulate data as such and does not protect under the property rights regime, the regulation of the data-based asset is evolving, which shows the legislator's attention to this area. The approach to the

[37] Richard Kemp, Paul Hinton and Paul Garland, 'Legal rights in data' (Thomson Reuters Practical Law, 25 January 2011) <uk.practicallaw.thomsonreuters.com/5-504-1074?transitionType=Default&contextData=(sc.Default)&firstPage=true> accessed 21 June 2024.
[38] UK Digital Assets Draft.
[39] Harriet Jones-Fenleigh, Aditya Badami and Jonathan Hawkins, 'The Law Commission's 'data objects': Digital assets as a new property class' (Norton Rose Fulbright, 1 August 2022) <www.nortonrosefulbright.com/en/inside-disputes/blog/202208-the-law-commissions-data-objects-digital-assets-as-a-new-property-class> accessed 22 June 2024.
[40] Law Commission, 'Digital Assets. Summary of final report' [2023] 9 (UK Digital Assets Summary).
[41] Art. 3.31 UK Digital Assets Draft.
[42] Art. 2.2 UK Digital Assets Draft.
[43] UK Digital Assets Summary.

Property (Digital Assets) Act wording reflects the overall common law approach, as the regulation is kept to a minimum despite pervasive preparatory work, and all possible open questions are left to the discretion of the jurisprudence.

The Property (Digital Assets) Act proposal idea is somewhat novel. The legal scholarship also proposes a compromise model of the data law regime, the quasi-property rights, as the traditional concept of possession cannot be applied to data. However, the concept of control used in practice may be introduced instead.[44] Sjef van Erp argues that data already falls within the *numerus clausus* of legal objects. However, some fitting is required in terms of terminology, as about data "ownership and revindication must be replaced by control and access; perhaps – so it might be added – the concept of "transfer" should be replaced by "distribution".[45]

DA specifically regulates the product data and related service data, and, as per the Brussels effect, the regulation in other jurisdictions may also be assessed concerning this specific category of data, as it will have a worldwide effect, similar to the act from the Digital Markets package. Though it is not indicated directly in the DA, the scholars generally agree that the DA primarily covers data from IoT devices[46], i.e., machine-generated, that is also evident from the DA Recitals.

In the UK, there has yet to be any legislation enacted covering a similar scope. However, a legislative proposal has almost made it to the legislation – the Data Protection and Digital Information Bill (DPDI)[47]. DPDI is mainly devoted to data protection regulation, and the differences it plans to introduce in the personal data regime in the UK compared to the EU attract most of the attention of a few commentators. However, the DPDI also contains provisions for sharing customer and business data, which are mainly similar to the DA scope. The DPDI is also essential as a marker of the direction in which the legislation and policies of the UK evolve after Brexit.

[44] Sief van Erp, 'Ownership of Digital Assets and the Numerus Clausus of Legal Objects' (2017) European Private Law Institute Working Paper No. 2017/6, 21.
[45] Ibid. 22.
[46] Martina Eckardt and Wolfgang Kerber, 'Property Rights Theory, Bundles of Rights on IoT Data, and the EU Data Act' (2024) 57 European Journal of Law and Economics 113-143. See Recital 112: "In order to eliminate the risk that holders of data in databases obtained or generated by means of physical components, such as sensors, of a connected product and a related service or other machine-generated data, claim the *sui generis* right under Article 7 of Directive 96/9/EC, and in so doing hinder, in particular, the effective exercise of the right of users to access and use data and the right to share data with third parties under this Regulation, it should be clarified that the *sui generis* right does not apply to such databases" (emphasis added).
[47] UK DPDI has not yet become legislation: it passed the House of Commons at the end of 2023 and was introduced to the House of Lords; there, it stopped at the report stage when the Parliament was prorogued for dissolution in the run-up to the general elections in the UK. The commentators have noted that if the Labour Party wins (which has eventually happened), it will likely introduce the new version of the Bill (see: David Naylor and Hannah-Mei Grisley, 'What Happened to the UK's Data Protection and Digital Information Bill?' (*Privacyworld Blog*, 2024) <www.privacyworld.blog/2024/06/what-happened-to-the-uks-data-protection-and-digital-information-bil> accessed 06 September 2024). Shortly after this article was finished, the winning Labor Party introduced this new version under the new title Data Use and Access Bill to the Parliament. Thus, this paper still needs to accommodate possible changes in provisions but should be considered in further research. For this reason this paper operates with the name and text of the initial DPDI version.

The scope of the DA covers product data and related service of the connected product or related service, including personal and non-personal data. DPDI, in its turn, deals with the two types of data – "customer data" and "business data", defining them both more widely than DA. Customer data definition, as in the DA, relates to one single customer, while the business data covers the trader's activity concerning all the customers. DA limits the scope of data derived from the connected product or related services. Meanwhile, DPDI covers any product data (connected or not) and data relating to the transaction, such as price and place of conclusion.

DA sets up three main parties of the relations: data holder, user, and third parties authorized by a user. DPDI provides for a wider variety of stakeholders about data: the three similar to DA plus third parties authorized by the data holder, plus "another person of special description" (namely a third party authorized by law), plus the interface bodies. It can be said that the DA reflects the classical contractual structure. At the same time, the DPDI is more oriented towards the market structure as a whole and considers both the direct parties to the interaction and their counterparties and the 'market facility'. Such a comprehensive regulation that considers the multi-stakeholder problem is more optimal if the development of the data market is prioritized. Gallese correctly points out that "Gaining access to the data is a good starting point for Users, but it does not significantly affect the EU market".[48] Given the lack of a clearly defined mechanism for the subsequent use of the data, there is a risk that even if users realize their rights in full, the data will settle with them, and the resulting redistribution of access will not lead to significant changes in the market.

The analysis in this section allows us to conclude that there are many similarities and differences between the legal frameworks of DA and DPDI. Both acts are aimed at solving a radically new task for the state - to create a legal basis for data sharing, first of all, between private parties, and thus overcoming the existing 'technical' monopoly on data that ended up in the hands of manufacturers of goods or providers of services. Currently, the EU legislation is the world's leading legislation in this area, and, of course, the authors of the DPDI cannot fail to take into account the provisions of the DA. The act's adoption was preceded by a very long scientific discussion and several communications of the European Commission, which significantly changed from the initial approach.

Thus, the significant divergences in the DPDI regulatory model were not accidental or deliberate, and DPDI shows the intention of the British legislator to depart from the uniform EU norms. In both the regulation of personal data and approaches to data sharing, the UK legislator demonstrates a more liberal approach to the obligations of businesses. In general, this reflects the overall goal, outlined at the strategic level, of the UK,

[48] Chiara Gallese, 'A first commentary to the proposal for a new Regulation on fair access and use of data (Data Act)' (2022) 3 Media Laws 237-270.

achieving (or maintaining) its championship as a jurisdiction that ensures the international flow of data.

Both acts impose an obligation on the de facto data holder to share the data with the user/customer or third parties authorized by the user. Both provide the possibility of charging a fee for the provision of data, at least to cover the costs of the data holder. In other aspects, however, the acts differ to a large extent.

A feature of the DA model is not simply that the user activates sharing - instead, all or most rights to operate with the data are locked on the user. Without the user's consent, data cannot be used by third parties or the data holder. Thus, the EU is changing the *de-facto* model of relations that existed before the act's adoption, in which the data holder operates the data (particularly non-personal data) freely without any specific regulations just because it has a complete technical control over the data. Under the DA model, data are not just shared with the user - most of the legal powers relating to data are officially transferred to the user. The user becomes a central figure whose actions depend on data availability in economics in general.

DPDI does not go that far: it does not touch the de facto situation of data holders having control over the data and operating with them. UK legislative proposal adds an obligation to share these data with the user or other authorized parties – without depriving the data holder of any of its previous powers regarding the data. Unlike the DA, the DPDI does not redistribute data rights by taking actual rights away from one person (data holder) and giving them to another (user); instead, it expands the range of people who can use the data.

In many regards, the model set in the DA is similar to those of the GDPR, as the use of data in both cases is linked to the consent of the "data producer" – user, even though DA covers both data of individual and business users. In a way, DA is also similar to consumer law, as it explicitly empowers the users of connected devices or data-generating services and creates obligations and limitations for manufacturers and service providers. It is customer-centric in most aspects, and the interests and will of the customers prevail over all other market participants.

Moreover, the peculiarity of DA is the contract-based approach to data sharing. Scholars have already called it the "contractualization" of sharing, as in most cases, the provision of data is supposed to be made under the contract. DPDI does not provide for concluding contracts between parties and follows a more public obligation model than a contract.

Overall, following the approval of the data strategies, the EU and the UK have started to actively work on creating new regulations for certain types of data. Moreover, one of the key objectives of the regulation is to define and increase the availability of data specifically for commercialization in the private sector.

3.3 Data Governance in Russia

Scholars note that legal regulation of the tradability of Big Data, including relevant contract rules, is of particular economic importance in Russia.[49] Still, neither the Russian Civil Code nor the sector-specific "digital" legislation provides any particular rules relating to data as such.

A closed list of "tradable" objects is provided in art. 128 of the Russian Civil Code (RU Civil Code I)[50]; before 2007, the list contained the notion of "information", however, it was deleted thereof simultaneously with the adoption of the Fourth Part of the Civil Code (RU Civil Code IV) [51] devoted to intellectual property rights. Amendments of 2019 have introduced to the Russian Civil Code (RU Civil Code III)[52] a particular type of contract for providing information services (art.783.1), but legal norms contain only the general provision that such a contract may require to keep the information secret.

A special law on information[53] covers a large set of issues relating to the information society. Over the last years, it has turned from a highly abstract piece of legislation into a law regulating the Internet and particular types of Internet activities (such as search engines, hosters, marketplaces, etc.) as well as the functioning of the state information systems. This regulation is primarily public, as it defines, to a large extent, the obligations of Internet actors towards the state (such as reporting) or general requirements and prohibitions. This law is similar to the DSA.

The law on information defines information as "messages, data irrespective of the form of its presentation" (art.2) and explicitly states that information may be the object of public, civil, and other legal relations (art.5), though provides a complicated mechanism which is not quite in line with the RU Civil Code I approach. The law states that "the holder of information unless otherwise provided for by federal laws, shall have the right to authorize or restrict access to information, determine the procedure and conditions of such access" (art.6). This norm creates significant difficulties in practice, as it is not clear whether such granting of access is a transaction and how it should be qualified from the point of view of civil law (i.e. special provisions on what types of transactions should be applied to it), as well as what norms of tax legislation are applicable.

Since then, the Russian legal and scientific community has been engaged in a sluggish debate on whether or not information can be considered a tradable object under civil law and whether it should be so.[54] Most scholars agree that information is de facto tradable

[49] Higher School of Economics (n 23).
[50] The Russian Civil Code. Part One. Federal Law of 30.11.1994 N 51-FZ (RU Civil Code I).
[51] The Russian Civil Code. Part Four. Federal Law "of 18.12.2006 N 230-FZ (RU Civil Code IV).
[52] The Russian Civil Code. Part Three. Federal Law of 26.11.2001 N 146-FZ (RU Civil Code III).
[53] Russian Federal law 'On information, information technologies and information security' No. 149-FZ of 27.07.2006 (RU Law on information).
[54] Christina Mefodieva, 'Digital data as an object of civil law regulation in Germany, the USA, and Russia' (Institute of Legislation and Comparative Law under the Government of the Russian Federation Government of the Russian Federation. Dissertation Paper 113 2019).

as any other object under civil law[55], though its tradability is limited by legislative deficiencies, and its exclusion from the Civil Code was a mistake[56]; some insist that information is a sui generis object, "capable of taking the form of other objects of civil rights".[57] The trend of the Russian legal science of recent years is the idea to recognize not information but digital data as a separate object of civil rights, i.e., property in the form of a sui generis right,[58] that shall ensure its tradability on equal footing with other intangible objects.

It is worth noting that despite the general provisions on freedom of contract and the consensus of scientists, transactions related to data turnover in Russia are complicated by the lack of regulation, so in practice, the subject of the transaction is usually clothed in one of the more "understandable" forms - a database or know-how. Thus, legal regulation of data in Russia in recent years has been very active but one-sided, as it mainly affects digitalization and the use of data to improve the efficiency of public administration and vertical relationships but practically does not affect the horizontal relationships of the market participants. The abundant but fragmented regulation without an articulated legal doctrine must be clarified. Given the attention given to the issue of data regime in the economy and public administration, symmetrical work in the field of law is needed to support all initiatives qualitatively.

Thus, the maturity of legal regulation in Russia regarding the product and service-generated data regime lags far behind Europe and the UK, given the need for approved legislation and elaborated legislative initiatives. Attention should also be paid to Russian scientific literature discussing the issue of singling out such data as an object of rights. However, the issue of rights distribution between different persons or access to such data needs to be analyzed. Despite scientific discussions, there are no significant legislative initiatives to regulate this data category in Russia, and there have been none in the past.

Thus, the Russian Federal projects "Digital Public Administration" and "Data Economy", though being by their nature the closes analogy to the Data Strategy, have not resulted in any particular legislation aimed at enhancing the data availability for businesses or developing the regulation (including commercial turnover) of the new types of data. In recent years, there have been different calls from academia to amend the law to accommodate the new digital reality, but they still need to be addressed by the legislature.

[55] D Lebedeva and A Yatsenko, 'Information as an object of civil rights' (2017) 4 Scientific Notes of the V. I. Vernadsky Crimean Federal University 166.
[56] EA Abramova, NN Averchenko and YV Baigusheva et al., *Civil law: textbook* (Prospect, 2013) 387.
[57] AG Tukhvatulina, 'Information as an object of civil rights' (2017) 2 Bulletin of Young Scientists and Specialists of Samara University 249.
[58] Mefodieva (n 54).

4 Three Policy Models for Data Governance

As the above review shows, the data policy documents in all the jurisdictions compared above, to a certain extent, take into account the interests of three groups: the state, business, and individuals. This reflected in the acts that are based on these strategic documents and directly regulate the legal regime of certain categories of data. However, it is important to note that the compared jurisdictions pay attention to the interests of different parties to different degrees and cater to them differently.

In the EU, the further development of data regulation has focused on users' rights, primarily individuals' rights. Back in 2020, the European Strategy for Data proposed to extend the rights of individuals within the framework of Art. 20 GDPR (portability right) by "giving them more control over who can access and use machine-generated data (possibly as part of the Data Act in 2021)".[59]

As the business consultations on the Data Act project demonstrated, the data stemming from professional use of the devices equipped with IoT is interesting for the majority of respondents, who express concerns about these data being exclusively held by the manufacturers.[60]

Thus, the field of attention of the European legislator was not limited only to the interests of individuals but also covered corporate users who could get some value from data. From an economic point of view, if we set aside the value issues of personal data protection, granting business users certain rights to the data they generate is of great value. Because it is business users who are likely to be able to find practical applications for that data and use it to create new value (e.g., by improving their own product) or at least to reduce their costs (e.g., by fixing broken equipment themselves instead of having to go to the manufacturer and pay for their services as necessary). Such data may also be of further economic interest to third parties to whom the user may wish to sell or transfer it (e.g., data on the performance of agricultural machinery for seed producers). As for individuals' data, it will undoubtedly be of personal interest to them. However, it is still difficult to imagine how individuals might subsequently use this data to maximize personal or public welfare.

Besides the explicitly declared goal of user empowerment not declared but self-evident goal of the DA is imposing further limitations on the Big Data monopolies (mostly non-European companies). The omnipresent marker power of a particular set of platforms and data ecosystem and their impact on the data markets has been noted by legal scholars (as well as economists, sociologists, etc.) for a long time now.[61] The current set of particularly

[59] Art. 5C European Strategy for data (n 7).
[60] European Commission, 'Public consultations on the Data Act: Summary report' [2021] <digital-strategy.ec.europa.eu/en/library/public-consultation-data-act-summary-report> accessed 15 April 2024.
[61] See, for example, a 2016 article by Lundqvist: Bjorn Lundqvist, 'Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet of Things World' (2016) Faculty of Law, University of Stockholm Research Paper No. 1.

"dangerous" companies exists in the form of the designated gatekeepers[62] under DMA or very large online platforms under DSA. Thus, one can allege that EU DA is the next station in the EU crusade against GAFAM and other Big Tech.

The DGA is generally focused on the interests of businesses and individuals, as it is about greater openness of public data. However, DMA and DSA aim to protect individual users (both business and private persons) and grant them additional data rights at the expense of other businesses. The same is true for the DA, as it gives new rights to data to individuals while limiting the rights of businesses holding the data. The interests of the public sector in acquiring necessary data are also addressed in these acts, though one can hardly allege that they are the cornerstone of the regulation.

Thus, it cannot be said that DSA and DMA aim solely to enhance access to data but rather to redistribute opportunities (including commercial opportunities) for data use between different market participants. Depending on the parties' activity in data use, these acts may either increase or decrease the actual commercial over-use of data. Regarding commercial use of data by private businesses, DMA and DSA regulation is based on the logic of antitrust regulation aimed at balancing the market and ensuring access to a resource (in this case, data) for some persons by restricting this access to others.

Thus, the EU primarily solves the task of rebalancing the data market. The European Strategy for Data raises concerns regarding the vast amounts of data accumulated by Big Tech companies and their high degree of market power.[63] As Bradford notes, the EU, despite the general market orientation, embraces the more state-driven economic policy to assert digital sovereignty[64] (as most of the Big Tech, or gatekeepers, or very large online platforms are not of European origin).

Thus, in choosing between the interests of the three parties mentioned above, in data regulation, the EU puts a stake in protecting the interests of individuals and limiting the interests of businesses (primarily multinationals). This is a striking feature of European regulation that is absent in the other two jurisdictions. Another characteristic feature of the EU model is the detail of regulation and the abundance of extensive legislation. However, this is more a style of European regulation in general than a feature of data regulation specifically.

In its National Data Strategy, the UK has expressed primarily the issues of developing a flourishing data market. Unsurprisingly, further legislative proposals relating to particular data issues are based on enhancing the trade in data and creating more opportunities for data-related businesses within the country. The UK aims to champion itself as a market attracting national and foreign businesses and providing them with opportunities for easier and safer operations. Notably, the UK National Data Strategy, unlike the EU one, does not

[62] European Commission, 'Gatekeepers' <digital-markets-act.ec.europa.eu/gatekeepers_en> accessed 06 September 2024.
[63] Part IV of the European Strategy for Data.
[64] Anu Bradford, *Digital Empires. The Global Battle to Regulate Technology* (Oxford University Press, 2023) 132-133.

emphasize promoting the interests of the individuals or the need to curb the powers of Bit-Tech.

The two most significant legislative proposals concerning data regulation are the Property (Digital Assets) Act 2024 and DPDI, and they are both aimed at simplifying data access and trade rather than limiting it. Property (Digital Assets) Act is made to give more clarity concerning the legal regime of digital assets as tradable commodities and, therefore, enhance their trade. DPDI, in turn, does not define any new type of property but regulates access to existing data for a broader category of users.

The new UK bill - DPDI - develops and extends the Smart Data concept already implemented in all areas of legislation, which is based on slightly different assumptions and values than what has been discussed at EU level.

The DPDI does not use the term Smart Data, instead using the terms 'customer data' and 'business data', however, Smart Data has been used in UK government policy documents, official and unofficial communications, and general business practice and is thus an informal term not so much for the categories of data regulated by Part 3 of the DPDI as for the data exchange model it envisages. Smart Data is officially defined as "secure sharing of customer data, upon the customer's request, with Authorised Third-party Providers (ATPs)" (UK Smart Data Roadmap).

The concept was called Smart Data, and it incorporates both ideas of secure and consented sharing of customer data with third parties. Implementing the project, the UK aims to drive innovation in the financial sector, where it already has an established position as one of the major international financial centers. It also fosters competition, allowing third parties access the needed customer's data. The UK Smart Data Roadmap states that based on the Open Banking success, the government wants to commit to "a Smart Data Big Bang" in the following sectors, including energy, banking, finance, retail, transport, homebuying, and telecommunications (nevertheless, the DPDI is not sector specific).

Thus, even with the imminent adoption of the DPDI, the UK leaves itself room for manoeuvre by being able to introduce the new data-sharing mechanism envisaged by it gradually and piecemeal, assessing the situation in each sector of the economy separately. In this regard, we can agree with the position that "in comparison with the EU developments, the Smart Data proposals appear modest":[65] on the one hand, the project creates positive expectations among its possible beneficiaries (which are rather small and medium-sized businesses than consumers); on the other hand, due to the graded approach, it causes less anxiety among those businesses that will have to incur compliance costs sooner or later.

Though the European and British projects of product and service data regulation are similar in many respects, the UK has considered the experience of discussions. At the same

[65] Kemp, Hinton and Garland (n 37).

time, the UK was part of the European Union, so the background and objectives of the current legislation are different. It is noteworthy that in the EU legislation, it can be called a cornerstone and one of the key goals and values of the project, while in the UK, at all levels of communication it is more about creating business value and developing the data market and asserting the UK's leading role in the world in the field of data trade. The UK project has a decidedly more practical and market-oriented orientation, as seen from the official communications rhetoric. The EU project, in turn, addresses not only the development of the data market and data sharing, but also issues of fair distribution, user's control and protection of user's rights. Undoubtedly, the rights of users who create data have a significant economic component. However, the rhetoric of the DA itself, as well as the previous communications of the European Commission and scientific papers, certainly shows that enhancing transparency, fairness, and protection of the weaker party are no less important in this legislation.

A comparative analysis of the two acts (DA and DPDI) reveals that although both are based on a desire to create a legal framework for data sharing, they come from different value orientations. The DA puts the user and their interests at the center, allowing the user to block further data reuse (at least theoretically). The DPDI creates a framework where data holders would be obliged to share the data under the law without entering into any contracts with the user or third parties. Preliminarily (given that the DPDI is still a bill and does not provide direct application but for the adoption of a delegated law), the model envisaged by the DPDI would be more conducive to data sharing.

This allows to conclude that UK version of strategic development with regard to data is business-oriented, particularly compared to the European one. New legislation proposed does not limit the de facto rights of the businesses they have acquired; however, it gives more opportunity for the other businesses to access this data and, hence, to compete.

Additionally, the UK legislative model is generally characterized by a limited volume of regulation, while many issues are left for the case law. In particular, the Law Commission, while preparing the report, which lies on the basis of the Property (Digital Assets) Act, noted that modern case law also mainly acknowledges digital assets as particular type of property. Thus, the Law Commission has yet to invent the proposed law, but rather, it has systematized the already existing approach. Compared to the European, the UK legislative proposals are generally shorted and less detailed, thus leaving more discretion to the courts.

Unlike other compared jurisdictions, Russia has not yet adopted any legal acts regulating rights to data or access to data concerning the private parties and markets for data in the wake of strategic documents. Neither are there any legislative proposals at a meaningful stage of development that would address these issues. The detailed contents of the new Russian federal project “Data Economy” is yet to be defined, however, judging by its structure, it addressed primarily two types of issues: development of particular

data-related technologies and enhancement of use of data in public administration and provision of state services.

There have been several proposals relating to developing a legal regime of data in the academic literature. However, no unified position was formalized by the scholars, and none of the proposals matured into draft legislation. Despite the high development of various digital services in Russia, the issue of user access to data and its further reuse in the economy must be carefully considered by the legislator or in the scientific literature. From this point of view, the Russian legislation lags behind the EU and UK in terms of maturity, even though at the level of strategic documents on data, the need to improve data accessibility is also indicated.

It should be noted that the lack of development of legislation in commercial data circulation (in particular, regulation of granting access to data to private individuals and private businesses) does not prevent development towards the use of data by public authorities. The rhetoric of several federal projects related to data and the digital economy is primarily aimed at technological development and achieving public goals through data. The new federal project dedicated to data also names 'Digital platforms in public administration' as one of the key directions. Thus, the implementation of Russian strategic documents is primarily aimed at achieving state interests, which differs significantly from the approaches of the EU or the UK.

There is no objective to increase data availability for businesses. However, this could be a side-effect if the state initially accumulates this data and then, if necessary, can provide it to businesses on request. It is not only about the data generated during public activities but also about the data provided by the business. Thus, the state plans to act as an intermediary and, possibly, as a 'trading platform' of business data.

Also, Russia is very technically orientated. The project is primarily aimed at technology development and import substitution. The new project specializes in developing technological solutions in specific areas, for example, artificial intelligence, cloud services, cybersecurity, etc.[66] As the Russian Ministry of Digitisation explains, the new national project “Data economy” “will provide for data collection, including using highly sensitive sensors based on quantum sensors, data transmission, creation of computing and data storage infrastructure using domestic equipment, ensuring data security, including using quantum encryption technology, and obtaining information in real time”.[67]

In general, the policy of the Russian Federation is characterized by a strong focus on public rather than private interests in the field of data use and technologisation, with emphasis on the development of data technologies rather than on the development of the

[66] R Spectr, ‘Structure of the National project “Data Economy” <rspectr.com/novosti/predstavlena-struktura-naczproekta-ekonomika-dannyh?ysclid=m321xb23nz399565880> accessed 09 November 2024.
[67] ‘On the new project “Data Economy”’ (*Portal26km.ru*) <portal26km.ru/articles/obzor/o-novom-natsproekte-ekonomika-dannykh/?ysclid=m321o7m4wj455328312> accessed 09 November 2024.

data market. On the other hand, it is evident that the development of the market in this area requires the development of technologies and can even be mediated by it.

It can be concluded that the EU, having proclaimed empowering individuals as one of its key objectives, continues its trend in the new regulation of machine-generated data to fight international data-driven corporations primarily through breaking their data monopolies and limiting their powers to use the data from EU users. On the other hand, the UK pursues a different policy, focusing on moderate regulation of the data market and creating a regulatory model to ensure the most active circulation of data in the economy without being too burdensome for business. Russia, in turn, focuses on data availability to meet the needs of state bodies and administration. In contrast, legislation concerning the market circulation of data between private individuals has mostly stayed the same since it was initially adopted.

As a matter of policy, though compared jurisdictions have strategic documents on data based more or less on the same level of understanding of the importance of data governance for the economy, further analysis shows significant differences in priorities, which would likely have different impacts on data markets.

5 Conclusion

The existence of strategic documents in the data field in three jurisdictions, the EU, the UK, and Russia, demonstrates that the governments have started acknowledging the critical importance of data governance for future development, irrespective of the political or economic models. This hints that shortly, we may see the adoption of strategic documents on data by many other countries, including developing ones, as they will follow the example.

The high-level goal that can be read out of all the compared strategic documents is to enhance economy and governance by applying the new data-extensive technologies. In turn, it requires an increase in the amount and quality of accessible data and the development of the relevant technologies. This understanding is unified across the compared jurisdictions.

Still, compared jurisdictions differently formulate particular policy goals and emphasize the interests of different interested groups at the strategic level. The EU tends to protect the interests of individuals, in some cases – even at the expense of businesses. The UK is intensely focused on the interests of businesses, including the convenience of operating in the country and the clarity of legal provisions. Conversely, Russia concentrates mainly on the interests of public authorities and better public services.

As for the legislation adopted in the wake of the data strategies, the EU is most active in this area, as it has adopted at least four vast and important acts dealing with various goals set in the strategy: DGA, DMA, DSA, and DA. Though they address various aspects of data governance, their essential feature is rebalancing the "data market". These acts aim

to change the de facto situation on data access and use by authorizing new actors (individuals, users, and partially the governments) to access the data while prohibiting or limiting the use by other actors. The UK, alternatively, opts to legally provide access to data to a broader range of interested parties without limiting the de facto data holders. Though the UK acts on data governance are yet to become legislation, judging by the existing legislative proposals, no new limitations on businesses relating to the data they hold are to be implemented. As for Russia, it has yet to adopt any new laws to amend the existing legal regime for data based on the available strategic documents. However, existing regulations regarding data in the commercial sphere will likely remain the same, as the strategic document is mainly oriented to the public use of data and the development of particular technologies. So far, Russia has not created any new regulations for the relationship between private parties concerning data.

Thus, for Russia, the interests of the state in accessing and using the data prevail in the current policy. As a result of data collection, the state may improve its services and serve as a mediator, or data marketplace, for the businesses. The UK prioritizes business development interests, including attracting data-extensive business to the country by creating unburdensome and effective regulation. The EU in trying to balance the interest of all the three groups of actors, on the one hand, gives more protection to the individuals, but on the other, may hinder data-extensive businesses by too strict requirements and complicated regulatory model.

The EU and the UK approach is based on a similar premise: to increase access to data and grant additional data rights to users. They follow the general trend of protecting the rights of individuals, which continues to evolve across Europe with the development of new technologies and the legislation governing them. However, the UK's approach aims to develop the data market and create optimal conditions for data trading, including for foreign partners. In the European Union, a company operating with data will have to face many requirements and restrictions resulting from the extensive legislation on different data types in recent years. Therefore, in forum shopping, foreign businesses, mutatis mutandis, are likely to prefer the UK due to its more beneficial approach. It will give the UK a competitive advantage by reducing legislative barriers to its business and attracting foreign companies for which European requirements would be too onerous to fulfill. Russia does not impose such onerous restrictions on the use and circulation of data. Still, the lack of regulation and its apparent focus primarily on the interests of the state administration, all other things being equal, make the jurisdiction less attractive as a data market. The significant role of the state in data regulation processes also does not exclude the emergence of burdensome business requirements in data handling and reporting.

The UK has chosen the most favorable and balanced model from the point of view of data market development and trade in data. This model will promote domestic business development and increase the country's attractiveness as a trading partner. The approaches in other comparable jurisdictions are less likely to achieve this goal.