https://doi.org/10.38044/2686-9136-2022-3-4-71-88

ARTICLES

DATA-SHARING AS A QUID PRO QUO OF CO-REGULATION IN THE EU

Mark L. Entin,[1]* Ekaterina G. Entina[2], Dmitriy V. Galushko[3]

[1]Moscow State Institute of International Relations (MGIMO-University)
76, ave. Vernadsky, Moscow, Russia, 119454

[2]Higher School of Economics (HSE University)
3, Bolshoy Trekhsvyatitelskiy Pereulok, Moscow, Russia, 109028

[3]Financial University
49, Leningradsky Prospect, Moscow, Russia, 125993

Abstract

The paper focuses on the defining of the co-regulation of national and supranational legal regimes' features of data-sharing in the digital platforms' functioning on the example of the EU's practice with a special attention to the disintegration process of Brexit. Data-sharing is one of the most appropriate spheres to demonstrate specific traits of digital platforms — the cross-border character of their operation. This demands quid pro quo interaction of the national and supranational regulatory regimes, filling the gap associated with the lack of international regulation and the inability to harmonize law. We begin with the theoretical characterization of information and personal data, the right to privacy, and classifications of interventions in private life. The EU has been chosen as an example, acting as a flagship of interaction of national and supranational legal orders in relation to the co-regulation of cross-border data-sharing in digital platforms. Interaction of the EU on the principle of quid pro quo, based on the practice of making decisions on adequacy, is considered in the context of Brexit and the relevant law-making practice of the UK. The discussion is complemented by examples of similar EU relations with South Korea and the United States. Based on the analysis, the authors conclude that the EU supranational legal order has a high degree of influence on the national legislation of third countries, which contributes to the constant development of regulation in the sphere and the strengthening of international integration.

Keywords

data-sharing, personal data, privacy, publicity, European Union, Great Britain, GDPR, Brexit

Conflict of interest	The authors declare no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Entin, M. L., Entina, E. G., & Galushko, D. V. (2022). Data-sharing as a quid pro quo of co-regulation in the EU. *Digital Law Journal, 3*(4), 71–88. https://doi.org/10.38044/2686-9136-2022-3-4-71-88

* Corresponding author

Submitted: 18 Sep. 2022, accepted: 10 Nov. 2022, published: 31 Dec. 2022

СТАТЬИ

ОБМЕН ДАННЫМИ КАК QUID PRO QUO СОВМЕСТНОГО РЕГУЛИРОВАНИЯ В ЕС

М.Л. Энтин[1,*], Е.Г. Энтина[2], Д.В. Галушко[3]

[1]Московский государственный институт международных отношений (МГИМО-Университет) МИД России
119454, Россия, Москва, просп. Вернадского, 76

[2]Национальный исследовательский университет «Высшая школа экономики»
109028, Россия, Москва, Большой Трехсвятительский пер., 3

[3]Финансовый университет при Правительстве Российской Федерации
125167, Россия, Москва, просп. Ленинградский, д. 49/2

Аннотация

Статья посвящена определению особенностей совместного регулирования национальными и наднациональными правовыми режимами обмена данными в функционировании цифровых платформ на примере практики ЕС с особым вниманием к дезинтеграционному процессу Брекзита. Обмен данными является одной из наиболее подходящих сфер для демонстрации специфических черт цифровых платформ — трансграничного характера их функционирования. Данный процесс требует взаимодействия национальных и наднациональных режимов регулирования по принципу quid pro quo, заполняя пробелы, связанные с отсутствием международного регулирования и неспособностью гармонизировать соответствующее право. Авторы начинают исследование с теоретической характеристики информации и персональных данных, права на неприкосновенность частной жизни и классификации вмешательств в нее. В качестве примера был выбран опыт ЕС, выступающего в качестве флагмана взаимодействия национального и наднационального правопорядков в отношении совместного регулирования трансграничного обмена данными в рамках цифровых платформ. Взаимодействие ЕС по принципу quid pro quo, основанное на практике принятия решений об адекватности, рассматривается в контексте Брекзита и соответствующей правотворческой практики Великобритании. Обсуждение дополняется примерами аналогичных отношений ЕС с Южной Кореей и Соединенными Штатами. На основе проведённого анализа авторы приходят к выводу о высокой степени влияния наднационального правопорядка ЕС на национальное законодательство третьих стран, что способствует постоянному развитию регулирования в рассматриваемой сфере и укреплению международной интеграции.

Ключевые слова

обмен данными, персональные данные, конфиденциальность, публичность, Европейский союз, Великобритания, Брекзит

Конфликт интересов	Авторы сообщают об отсутствии конфликта интересов.
Финансирование	Исследование не имеет спонсорской поддержки.

Для цитирования Энтин, М. Л., Энтина, Е. Г., Галушко, Д. В. (2022). Обмен данными как quid pro quo совместного регулирования в ЕС. *Цифровое право, 3*(4), 71–88. https://doi.org/10.38044/2686-9136-2022-3-4-71-88

* Автор, ответственный за переписку

Поступила: 18.09.2022, принята в печать: 10.11.2022, опубликована: 31.12.2022

Introduction

The phrase *'quid pro quo'* can be described as an exchange of something for something. In the context of the functioning of digital platforms, it usually refers to an exchange of goods and services for personal data or other information products in place of compensation (Walker, 2015). Significant progress in the development of digital platforms — namely the introduction of information and telecommunication technologies and the associated increase in the volume and directions of using the information in various spheres of public life, as well as its transmission by the latest communication means — have significantly expanded the possibilities for collecting, storing, and processing information in relation to individual citizens. A traditional firm can only collect data on its own customers, but a digital platform can access a vast amount of data related to all sellers and buyers on multiple sides of its platform (Eisenmann et al., 2011).

Activity in the formation of automated databases, processing, and dissemination of information about persons without their knowledge has led to the emergence of a global problem, in particular, the scale (in both time and space) of the problem of information security of people, society, and the state for the protection of personal data. The data that fuels digital platforms heightens these dynamics in a way that is qualitatively and quantitatively different from the way it effects conventional markets (Kira et al., 2021); that is, the problem of protecting the interests of the individual in the information sphere is also the problem of protecting personal data, which concerns all spheres of human activity, society, and the state. The well-being of both the individual and the state depends on understanding the importance and necessity of creating a mechanism to protect personal data.

Globalized trade and increased cross-border transactions present interesting legal implications for the ability of public and private subjects to control and protect data. Digital platforms have made it possible for transactions to be concluded beyond national borders.[1] Consequently, the development of digital platforms has led to a huge growth in the volume of cross-border transmitted personal data, which acts as a new currency in the *quid pro quo* interaction of national and supranational regulatory regimes, particularly their co-regulation at the normative and institutional levels.

The globalization of trade in digital data and services has not been accompanied by a general harmonization of Internet law (Voss, 2019), nor a true convergence of data protection and data privacy laws (Voss, 2020). Consequently, now it is possible to envisage an avalanche of new laws and regulations attempting to govern and impose order on a dizzying array of tech developments.[2] It is expected that international authorities will make full use of their new powers in order to apply

[1] Serzo, A. L. O. (2020). *Cross-border data regulation for digital platforms: Data privacy and security.* [Discussion Papers DP 2020-47]. Philippine Institute for Development Studies.

[2] Tene, O. (2022, January 3). The year ahead: Privacy developments in 2022. *Goodwin*. https://www.goodwinprivacyblog.com/2022/01/03/the-year-ahead-privacy-developments-in-2022/

and enforce their respective data protection legislation in the near future.[3] The headliner legislator is the European Union, which is recognized as the creator of the global standard for 'best practice' in data governance and co-regulation between national and supranational legislators.[4] Examining the relationship between national legal regimes and supranational data protection regulation is of special interest in the context of the unique process of Great Britain's withdrawal from the European Union — Brexit.

Methodology

The methodological basis of this article is a complex of general scientific and special methods, the expediency of which is determined by the specifics of the object of research. A systematic approach and structural and functional analysis were used in the course of this study to reveal the essence and genesis of data-sharing, its structure and functions in modern society, and the role of digital platforms. When studying the mechanisms for legal support of data sharing at national and supranational levels, a system-structural and dialectical method of scientific knowledge of legal processes and phenomena was used, which manifested itself, in particular, in the widespread use of certain categories of dialectics. The application of the formal-logical method made it possible to carry out a logical, grammatical, and morphological analysis of the existing legal norms. The use of the comparative method made it possible to study the compliance of national legislation with European standards in this area, as well as to analyze the process of transfer and protection of personal data between the European Union and the United Kingdom after Brexit.

Results

From the outset, it should be mentioned that the term 'information' entered scientific circulation long before the rapid development of communication tools, digital platforms, and data conversion, as well as transmission technologies based on it. The emergence of branches of science and technology directly related to them have turned it into an iconic symbol of the modern era. There are many definitions of information as a result of scientific discussion and various approaches to the interpretation of this concept. The original concept of 'information' was associated exclusively with communicative activities in society (Nitecki, 1985). It was found that information is the highest, most complex result of an orderly reflection in the form of messages, knowledge, and information about nature, society, and objective reality in general, covering all spheres of human activity used in the process of communication, management, production, cognition, creativity, upbringing, education, etc. This makes it possible to pay attention to the managerial nature of the information. Information is seen as the unity of updating diversity and as its limitation. The main function of information is to convey an idea (to inform) about an object, while reflecting its properties.

One kind of information is personal information that reflects both the individuality of a person and their universal biological and social properties. Personal information reflects human diversity: the individuality of each person as a carrier of unique elements of physical, physiological, mental, economic, cultural, and social identity. The defining feature of personal information is its

[3] Gibson Dunn. (2022, January 31). *International cybersecurity and data privacy outlook and review — 2022*. https://www.gibsondunn.com/international-cybersecurity-and-data-privacy-outlook-and-review-2022/

[4] Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business*. https://www.privacylaws.com/reports-gateway/articles/int169/s_int169dplaws2021/

individualized nature and the ability to identify a specific person using certain criteria. During such identification, the process of personifying certain information takes place: that is, linking them to a specific person. Identifying information makes it possible to identify a person, either directly or with the help of other factors. Information (both documented and oral) is a form of reflection of the biological and social identity, as well as the individuality of each person (Mingers & Standing, 2018).

To refer to information about an individual that has already undergone certain processing, has been recorded and ordered in a certain medium, and is suitable for automated processing, the term 'personal data' is used (Lat. *personalitas* — personality).

The unlawful collection, use, and dissemination of personal information damages the image of the individual. This does not only apply to biographical data, such as a person's surname, name, patronymic, date of birth, place of birth, nationality, religious, political, or philosophical beliefs, education, place of study and work, information about marital status, presence of children, or attitude to military service. Personal information includes information about a person's material and financial condition (bank accounts, payments in them, real estate and movable property, property rights), health status, personal relationships of a private nature, and a lot of other information in material form in various areas of public life that are created, collected, stored, distributed, and used in other ways, both with the consent of the data subject, and without their knowledge. This information allows society to evaluate a person as an individual, to form their reputation (Lat. "reputatio" — evaluation).[5]

Protecting the confidentiality of personal information has become relevant during the emergence and widespread risks to life, health, reputation, and human well-being due to the illegal collection and use of personal information — that is, from unwanted intrusion into the internal sphere of human life, which is protected by the right to respect for private life (Beck et al., 2016).

If half a century ago it was necessary to expend considerable effort to obtain information about a person, the current level of information technology development — in particular, the functioning of digital platforms — makes it possible to process data on thousands of people in a matter of seconds without incurring excessive costs. The combination of inaccurate or outdated personal data will create a misleading impression of an individual.

The capabilities of digital platforms that allow the collection and processing of personal information are constantly and rapidly expanding. Technologies are improving, and their cost is decreasing. Even with conventional information collection technologies, a significant amount of personal information is constantly collected. For example, any payment transaction on a digital platform, whether it is a purchase, sale, or investment, creates a collection of personal data. Subsequently, digital platforms can use such information both for commercial purposes and for reporting to the fiscal authorities of the state.[6]

It should be noted that, from the point of view of a person's security, that different kinds of personal information have different degrees of importance per individual, which is determined by the level of risk of harm. Given the threat of poor perception by others, discrimination on a certain basis, or other illegal use of personal information, its potential to create 'vulnerability' for a person must be foreseen. To take into account the interests of the individual and their subjective attitude to information, which cannot be fully covered in generalized regulatory prescriptions, a voluminous

[5] Sierra, C. & Debenham, J. (2009). *Information-based reputation*. Proceedings of the first international conference on reputation: Theory and technology — ICORE 09, 5 – 19. https://opus.lib.uts.edu.au/handle/10453/10892

[6] OECD. (2019). *The role of digital platforms in the collection of VAT/GST on online sales.* www.oecd.org/tax/consumption/the-role-of-digital-platforms-in-the-collection-of-vat-gst-on-online-sales.pdf

list of data must be legally classified as 'sensitive data' (including that concerning racial or ethnic origin or nationality, political views, religious or philosophical beliefs, membership in trade unions or public organizations, information related to health or the provision of health care, family and personal relationships of a private or sexual nature, criminal acts or illegal behavior), and people must be granted the right to independently determine the boundaries of the circulation of their personal information in society. This creates a territorial space in which a person can control the boundaries of their individuality. To effectively protect this space, a person must have the right to define these boundaries — that is, to determine what personal information can be transferred, for what purposes, to what extent, and to what recipients.

This approach is due to the fact that only the person to whom the personal information relates can assess the likely risk of misuse of such information. This is the basis of the nature of the right to privacy of personal information and the awareness of such as belonging to the 'private sphere' of human life. Legal doctrine uses the term 'privacy' to refer to this legal institution. It characterizes the qualitative state of the object, which follows from its belonging to the 'private sphere' of human life. In addition, this term is immediately associated with what belongs directly to a private person and is inaccessible to the public as a 'private matter', as opposed to a 'public' one.

The first concept of the right to privacy passed judicial testing in the United States. In the practice of American courts, cases of commercial use of the personal characteristics of individuals, such as appearance, name, and voice, have often been considered. Such cases concerning human rights violations have often been accompanied by violations of property rights. American courts have recognized these individual personality traits, which were encroached upon by other persons, as an object of protection of property interest. The traditional Western idea of the right to privacy originates from the right to the inviolability of homeownership, and the Western doctrine of privacy is territorial in nature, since it protects the personal living space of a person.[7]

After studying the precedents created by US courts when considering cases regarding interference with a person's private life, an American lawyer, William L. Prosser (1964), proposed the following classification: disclosure of facts relating to private life, reporting false information about a person, misuse of images of a person's appearance, voice, and, finally, physical harassment (Prosser, 1964).

The Swedish researcher Stromholm proposed his own classification of interventions in private life. Having singled out 14 types of unlawful attacks on privacy, he grouped them into three groups, taking into account the direction of the offenders' actions:

1) actions aimed at invading the private sphere of a person's life — an illegal search, sending letters with insults, harassment by phone calls

2) illegal actions, thanks to which violators obtain information about the private life of a person: wiretapping, interception of correspondence, etc.

3) dissemination or other use of information about a person's private life: publication of information about a person's private life in the press, the use of a person's name and appearance (Resta, 2011).

Since it is the right of a person to the privacy of personal information that becomes the object of legal protection, this type of privacy is called 'informational privacy'. This kind of privacy also has a territorial dimension, since information flows circulate in a certain space. A person is the main source of information generated within their own living space and is a consumer of information that comes to them from the outside, particularly within digital platforms.

[7] Solove, D. J. (2006). A brief history of information privacy law. In *Proskauer on privacy. PLI.* https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications

It is also necessary to distinguish between the spheres in which the social activity of a person is realized. This makes it possible to break down the general problem of protecting human privacy into sectors that require separate legislative regulation. According to this criteria, four types of privacy can be distinguished:

1) informational privacy, which covers the rules for the collection and processing of personal data

2) bodily (physical) privacy, relating to the protection of the physical integrity of a person from coercive procedures, such as drug testing, etc.

3) communication privacy, covering the security and confidentiality of postal items, telephone conversations, electronic correspondence, and other forms of communication

4) territorial inviolability, with regard to the establishment of a legal framework for protection against interference in the family sphere, other environments, the workplace, or a vehicle (Resta, 2011).

This classification makes it possible to understand the complexity and interconnectedness of the legal regulation of data-sharing, being a key to protecting the privacy of personal information. At the same time, digital platforms act as carriers of such data. The rapid development of digital platforms, in which messages are transmitted in digital form, does not set up the possibility, technically or normatively, to distinguish between where communication privacy ends and personal data confidentiality begins. This makes the legal developments in the sphere quite complicated. Nevertheless, legislative measures continue to develop at speed all over the world.[8]

In addition, the problem of ensuring the right to privacy of users of digital platforms is complicated by the extraterritorial nature of information exchange. Digital platforms make it possible to establish direct contact between a human data subject under the jurisdiction of one state and other subjects of information exchange that may be located on the territory of other states. In the era of digital platforms and Big Data, legal relations arise at the intersection of jurisdictions, since the personal data of any person (a citizen of any state) can be processed by business entities in foreign jurisdictions. Ensuring the operation of national provisions — and therefore guaranteeing an adequate level of privacy protection for its citizens in this environment — becomes problematic for the state. At the same time, the creation by national governments of artificial obstacles to the free cross-border circulation of personal information will negatively affect international cooperation in many areas. Understanding this problem prompted the international community to develop cooperation in order to ensure the continuity of information exchange, which led to the creation of a set of international norms and principles that are covered by the international legal institution for the protection of the confidentiality of personal information.

Thus, in protecting the right to privacy of personal information, there is a focus on ensuring the freedom of the individual to determine the spatial and temporal framework of information contact with other subjects, as well as the controllability of the circulation of personal information in society, which is important for maintaining the autonomy of the individual, as well as protecting the private sphere of their life. That is the case for the European Union, where the issue of personal data protection is often considered in the context of the protection of fundamental human rights guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union. This protection afforded to the data of European citizens extends beyond the borders of the Union, especially when data is transferred outside European territory. More specifically, the transfer of personal data outside the

[8] DataGuidance. (2022, June 2022). *Keeping up to date with global privacy updates.* https://www.dataguidance.com/resource/keeping-date-global-privacy-updates

European Union is only permitted if the protection of data offered by the country receiving the data is considered 'adequate' by the EU. Therefore, such a state must provide guarantees equivalent to those provided by the Union's law.

EU data protection law provides for the unimpeded flow of personal data in the European Economic Area (hereinafter referred to as the EEA), which includes the EU member states, Norway, Iceland, and Liechtenstein. The transfer of personal data to non-member countries is only permitted in limited cases due to the fact that this issue acts as an element of the digital sovereignty of the EU.

As the European Union is lagging behind the United States and China in certain areas of information and communication technology development, concern over the dominance of digital platforms and security issues has naturally led to increased attention being paid to the problem of the EU establishing its own 'digital' sovereignty.[9] Ursula von der Leyen, President of the European Commission, has specifically pointed out this need.[10] The need to "establish digital sovereignty as the leitmotif of European digital policy" was also expressed by the German side in its EU Council Presidency program of July 2020.[11] In general, calls are increasingly being made in the EU to build a European cloud and information infrastructure for strengthening European digital sovereignty and addressing the fact that, today, the cloud and IT market is almost exclusively dominated by non-European digital platforms — with potentially detrimental consequences for the security and rights of EU citizens (Martirosjan, 2021). Later on the French Presidency[12] of the Council of the European Union has picked up the baton in this regard, paying the most serious attention to the protection of personal data.[13]

The principles of the EU Charter on personal data are also embodied in the Lisbon Treaty of 2009. On November 4, 2010, the European Commission published a strategy for strengthening data protection at the European level.[14] In January of 2012, the European Commission approved a comprehensive reform plan, including the need to replace the Directive with an EU Regulation that would establish uniform requirements across the EU.[15] In 2016, the same year the Brexit referendum was held, the EU data protection law saw the most significant change since the introduction of the Data Protection Directive in 1995 through the adoption of the General Regulation on Data Protection Regulation

[9] Gueham, F. (2017). Digital sovereignty — Steps towards a new system of internet governance. *Fondapol.org.* https://www.fondapol.org/en/study/digital-sovereignty-steps-towards-a-new-system-of-internet-governance/

[10] European Commission. (2019). *Political guidelines for the next European Commission 2019–2024.* https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf

[11] Hasanova, A. (2021). Evropejskij podhod k «tehnologicheskomu suverenitetu» [European approach to "technological sovereignty"]. *RIAC*. https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/evropeyskiy-podkhod-k-tekhnologicheskomu-suverenitetu/

[12] French Presidency of the council of the European Union. (n.d.). *Personal data*. Retrieved August 4, 2022, from https://presidence-francaise.consilium.europa.eu/en/personal-data/

[13] Council of the European Union. (2021). *Council Decision on the conclusion, on behalf of the Union, of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, and of the Agreement between the European Union and the United Kingdom of Great Britain and Northern Ireland concerning security procedures for exchanging and protecting classified information.* https://data.consilium.europa.eu/doc/document/ST-5022-2021-REV-3/en/pdf

[14] European Commission. (2010). *European Commission sets out strategy to strengthen EU data protection rules.* https://ec.europa.eu/commission/presscorner/detail/en/IP_10_1462

[15] European Commission. (2012). *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses.* https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46

(GDPR),[16] the first EU legal instrument regulating the protection and free flow of personal data that is directly applicable in all EU member states.

The GDPR aims to protect the regulation on personal data, which is set out in the EU Charter and the Treaty on the Functioning of the European Union. The GDPR's substantive scope concerns automatic and non-automatic data processing, with the exception of the processing of data by EU institutions, which is regulated by another regulation. The application of the GDPR has several justified exceptions: criminal prosecution procedures, security provisions under the Treaty on the Functioning of the European Union, scope of data processing that goes beyond EU law, and the processing of personal data of natural persons for exclusively private purposes ("private processing") (Voigt & Von dem Bussche, 2017).

The GDPR's principles provide that personal data:

- is processed lawfully, fairly, and transparently ("legal, fair, and transparent")
- is collected for specific, explicit, and legitimate purposes ("limitation for purposes")
- must be adequate, appropriate (for the purposes of processing), and limited solely to the purposes for which they are processed ("data minimization")
- processed accurately ("accuracy")
- stored in a form that allows the identification of the data subject no longer than is necessary for the purposes of the processing ("storage limit")
- processed in such a way as to ensure adequate security of personal data ("integrity and confidentiality")

It should be noted that some of the GDPR's principles have been elaborated and improved on the basis of the jurisprudence of the EU Court of Justice.

According to Chapter V of the GDPR, there are several legal bases that allow the transfer of data from the EU to non-EU countries. One of the most convenient ways to seamlessly transfer data from the EU to a state that is not a member of the Union is to obtain a decision from the European Commission on adequacy. The transfer of data to a state that is not a member of the EU, but which has an adequacy decision, does not require additional legal grounds for cross-border transfer (Article 45(1) of the GDPR). The procedure and requirements for the adequacy decision are qualified and specified in the EU decision on adequacy.[17] An adequacy decision is considered a proper basis for cross-border transfer for four years after it has been made and/or successfully reviewed, or unless it is challenged before the Court of Justice (for example, the *Privacy Shield case*).

In practice, the European Commission issues an adequacy decision based on an opinion issued by the European Data Protection Board (EDPB) in accordance with Article 70(1)(s) of the GDPR and Articles 2 and 12 of the EDPB Rules of Procedure.[18] This function was previously performed by the Working Party on Article 29 (hereinafter — 29WP). The 29WP produced 12 adequacy decisions. Prior to the adoption of the first adequacy decision in 1998, the 29WP published a special Working Paper that covered all the

---

[16] European Union. (2016b). *Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation) (Text with EEA relevance).* https://eur-lex.europa.eu/eli/reg/2016/679/oj

[17] European Commission. (2018). *Working document on Adequacy Referential (wp254rev.01).* https://ec.europa.eu/newsroom/article29/items/614108

[18] EDPB. (2018, May 25). *European Data Protection Board Rules of Procedure*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_rop_version_6_adopted_20200129_en.pdf

important issues related to adequacy decisions.[19] Although 29WP has been superseded by the EDPB (Article 94(2) of the GDPR), this Working Paper remains a solid step-by-step plan for assessing the adequacy of protection afforded by a non-member country containing practical steps to be taken by the applicant country concerned in order to obtain an adequacy decision from the EU side.

When deciding on adequacy, the EDPB and the European Commission take into account, inter alia, the following circumstances:

- due diligence on data protection and the rule of law in a broad sense (including other international obligations, such as those within the EEA)
- access of the data subject to effective law enforcement and judicial protection
- the existence of an independent and effective supervisory body
- the jurisprudence of the EU Court of Justice and the European Court of Human Rights on matters related to privacy
- compliance with 29WP and EDPB guidelines
- recent and future changes to the General Regulations (for example, the decision on the Privacy Shield was made subject to the GDPR's entry into force)

In general, the participation of the European Union in dialogue and, if necessary, negotiations with non-member countries (including EU strategic partners and the countries of the European Neighborhood Policy) and international organizations (such as the Council of Europe, the Organization for Economic Cooperation and Development, United Nations) tends to promote highly compatible data protection standards worldwide.[20] The EU acts as a supranational entity that sets global rules in a number of areas of regulation: antitrust, privacy, health (through chemicals regulation), environmental protection and food safety. The area of privacy protection, where Europe sets the tone, is central, because EU legislation in this area affects the laws of territories outside its borders (Bradford, 2012). Thus, unsurprisingly, the issue of data-sharing has acquired particular relevance in connection with disintegration reflections — the UK's withdrawal from the European Union.

Cross-border data-sharing after Brexit is no longer free but must be supported by a specific legal instrument or mechanism since the United Kingdom is no longer subject to EU law. However, it seems that the importance of such a decision cannot be truly appreciated without highlighting the crucial role that data-sharing plays in terms of trade and economic relations, as well as other forms of non-commercial cooperation between the UK and the EU. That is why some researchers note that "data protection could potentially be among the problems that could 'make' or 'hinder' a possibly successful Brexit" (De Hert & Papakonstantinou, 2017).

The months leading up to the 2016 Brexit referendum and the first few months afterwards were characterized by lively discussions about the advantages and disadvantages of the UK leaving the EU (Nicolaïdis, 2017). A plethora of figures and data describing current trade relations with EU and non-EU countries, as well as speculation about potential future UK relations, have been used to substantiate sometimes quite opposing opinions and points of view. However, data regarding data-sharing between the EU and the United Kingdom clearly points to a deeply intertwined architecture of trade and economic relations between the parties, as well as other forms of cooperation in many areas

[19] European Commission. (1998). *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* [Working Document]. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf

[20] Shadrin, S. A. (2019). *Pravovoe regulirovanie zashhity personal'nyh dannyh v Evropejskom Sojuze: Genezis i perspektivy razvitija* [Legal regulation of personal data protection in the European Union: genesis and development prospects: Ph.D. dissertation] [Unpublished doctoral dissertation]. Kazan.

that are heavily dependent on the exchange of personal data, which will be damaged in the event of a sudden impediment to such cross-border exchange.[21]

In 2018, the UK, then an EU member state, updated its legislation to GDPR standards. The EU's GDPR came into force on May 23, 2018, and the UK Data Protection Act of 2018 was passed on the same day. Still, on January 31, 2020, Great Britain left the EU and entered an 11-month transition period, during which EU legislation continued to fully apply to the territory of the country.

The 2018 Act firstly supplemented the GDPR in areas where EU regulation allowed member states to adopt additional regulations, such as on conditions for processing special categories of data (Article 9 of the GDPR) or on derogations from the rights of data subjects (Article 23 of the GDPR). Secondly, it applied a limited set of GDPR rules to rare cases of data processing that went beyond its scope — for example, to government bodies that process personal data in unregistered documents, as well as bodies other than law enforcement or intelligence services that process data for national security or defense purposes. Thirdly, the 2018 Act implemented EU Directive 2016/680 in UK legislation, which regulates the processing of personal data by law enforcement agencies. Fourthly, it created a legal framework for the protection of personal data processed by intelligence agencies.

This legal regime was in effect until Exit Day. The European Union (Withdrawal) Act of 2018 provides that, at the end of the transitional period, EU law in force on December 31, 2020 — including regulations such as the GDPR and European Commission adequacy decisions — will be incorporated into UK law as "EU retained law".[22] Thus, the GDPR and its principles have been and remain part of UK law. The British Parliament has published explanatory notes confirming that the 2018 Act and the GDPR apply substantially the same standards for most data processing in the UK and are sufficient to create a clear and consistent data protection regime.[23]

Based on this, UK businesses were required to comply with both the GDPR and the 2018 Act during the transition period, and to comply with the requirements of UK law upon its completion.

In October of 2018, the UK regulator published its first enforcement notice under Section 149 of the 2018 Act against AggregateIQ Services Ltd. In 2020, a notice of intent to fine the Marriott International hotel network was published (with a fine of £18.4m) due to a data breach.[24] The first fine was imposed on December 20, 2019, on the Doorstep Dispensaree pharmaceutical company. The fine was £275,000.[25] It should be noted that the GDPR and the 2018 Act affect digital platforms in the UK in a similar way as in the European Union. At the same time, companies in the UK are having difficulty meeting the requirements of the GDPR. Since the implementation of GDPR, the UK has reported 40,026 personal data breach notifications, with 8,355 reported in 2020, and 9,490 in 2021 — a 13.6% increase in one year.[26]

21 UK Government. (2020). *Explanatory framework for adequacy discussions — Section A: Covering note*. https://www.gov.uk/government/publications/explanatory-framework-for-adequacy-discussions

22 UK Legislation. (2018). *European Union (Withdrawal) Act 2018*. https://www.legislation.gov.uk/ukpga/2018/16/contents/enacted

23 UK Parliament. (2018). *Data Protection Bill Explanatory Notes*. https://publications.parliament.uk/pa/bills/lbill/2017-2019/0104/18104en01.htm

24 Information Commissioner's Office. (2020). *ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure*. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/

25 Information Commissioner's Office. (2020). *Doorstop Dispensaree Ltd monetary penalty notice*. https://ico.org.uk/action-weve-taken/enforcement/doorstep-dispensaree-ltd-mpn/

26 Weston, S. (2022, January 18). European data regulators issued €1.1 billion in GDPR fines in 2021. *ITPro*. https://www.itpro.co.uk/policy-legislation/general-data-protection-regulation-gdpr/362000/european-data-regulators-issued

In general, British legislative changes have been aimed at the sovereignization of the legal regulation of the sphere in question. The Data Protection Act of 2018 temporarily allowed the transfer of data to countries that received adequacy decisions from the European Commission before the EU exit day, along with EU and EEA member states, until the rule was repealed by the appropriate competent national minister. At the same time, on the one hand, the 2018 Act made the British domestic data protection system more consistent. On the other, British and European business entities have had to comply with the requirements of two different legal systems since the end of the transition period. Thus, the extraterritorial scope of EU and UK legislation forces digital platforms applying to data subjects residing in different jurisdiction to apply to both regimes, which may no longer be in harmony with one another.[27]

Discussions

The Trade and Cooperation Agreement between the European Union and Great Britain signed on Christmas Eve of 2020 largely established the legal framework for the future architecture of relations between the parties in trade, the economy, and other areas (Babynina, 2021). The UK ratified this Agreement almost immediately by passing the European Union (Future Relations) Act of 2020. Within the EU, ratification stretched until April 29, 2021, when, after receiving the consent of the European Parliament on 27 April,[28] the Council of the EU decided on ratification. Until then, the previous EU legal regulation applied to the United Kingdom in its entirety, as if the UK was still a member state, during an additional transition period, the maximum duration of which could be six months (Article 782 of the Agreement). The purpose of this transition period appears to have been twofold: on the one hand, it prevented a sudden halt in data flows between the EU and the UK. On the other, it gave the European Commission sufficient time to decide on adequacy. Indeed, the Agreement explicitly provides that this transition period would end as soon as a decision on adequacy was made, or, failing that, after six months, whichever came first.

Title III of Part II of the Agreement governs digital trade, i.e., commerce carried out by "electronic means." This section focuses on cross-border data-sharing and its protection. Both parties made a formal commitment to ensure sufficient data-sharing, while avoiding the imposition of requirements regarding its location, as well as equipment and networks. Both parties committed to recognizing and protecting the right to data protection and privacy in order to increase the level of trust between market participants. The EU and UK are free to develop their own legal frameworks for data protection and sharing, while being obligated to ensure that general purpose data transfers in the digital marketplace are appropriate. Part III of the Agreement is devoted to cooperation between law enforcement and judicial authorities. Both parties are committed to protecting personal data, along with other fundamental rights. The provisions of the Agreement confirmed the need to ensure

[27] Manancourt, V. (2020, December 28). What the interim Brexit data flows deal means for Britain. *Politico*. https://www.politico.eu/article/what-the-interim-brexit-data-flows-deal-means-for-britain/

[28] European Parliament. (2021). *European Parliament legislative resolution on the draft Council decision on the conclusion, on behalf of the Union, of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, and of the Agreement between the European Union and the United Kingdom of Great Britain and Northern Ireland concerning security procedures for exchanging and protecting classified information (05022/2021 — C9-0086/2021 – 2020/0382(NLE))*. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0140_EN.html

compliance with data protection principles, such as the principle of security and storage restrictions, in relation to this data.

Thus, by establishing the possibility of making an adequacy decision in relation to the UK as a non-member country, the European Commission also indicated the nature of the future relationship between the parties from the position of the sphere of personal data protection. Great Britain, as a former member state of the Union, will not be granted any special status, particularly with respect to automatic mandatory bilateral recognition of the adequacy of the level of protection, as originally proposed by the UK during the negotiations. From the point of view of the legal regulation of the protection of personal data, this rule lays the foundation for a potential divergence between the legal systems of the EU and UK, which, in the context of the adopted bilateral documents, can develop independently, without being tied to a specific architecture for the chosen model of future relations (Entin & Galushko, 2021).

The European Commission issues decisions on adequacy unilaterally, at its discretion, subject to an assessment of the adequacy of the legal system of the non-member country, and is obliged to update the decision regularly thereafter. Thus, the decision on adequacy is not final or irrevocable and can be withdrawn at any time. This is confirmed by the practice of the Court of Justice of the European Union, which, in its decision in the Schrems I case, pointed out that adequacy decisions are evolving documents reflecting the current state of the foreign legal system in question. Through these mechanisms, the European Commission certifies that the non-member country provides adequate guarantees to justify the authorization for the transfer of personal data out of the EU. Thus, a positive assessment of the adequacy of a non-member country can suddenly change in the event of reforms or the emergence of new legal regulatory mechanisms that affect the system of protection of cross-border personal data. This possibility clearly shows to what extent the British legal system (although formally already independent) will still be, de facto, subject to a number of restrictions implicitly derived from EU law.

Moreover, adequacy decisions can be challenged in the Court of Justice, as Mr. Schrems successfully did in relation to an adequacy decision related, firstly, to the privacy regime of the US (Safe Harbor principles) and then to a decision related to the approval of another mechanism introduced between the EU and the USA (the EU-US Privacy Shield). In addition, adequacy decisions can be suspended, since, if competent national authorities of EU member states have doubts about the adequacy of the data protection regime of a non-member country, they can suspend cross-border data-sharing with it (Fabbrini et al., 2021).

On May 21, 2021, the European Parliament adopted a resolution on the adequate protection of personal data by the UK[29] calling on the European Commission to make an appropriate decision on adequacy in relation to the United Kingdom. At the same time, as mentioned earlier, the EU Parliament once again expressed concern about the actions of the UK in this area. Firstly, inappropriate law enforcement practices of the British authorities in relation to compliance with EU law was noted, particularly with respect to the EU's GDPR. In addition, there were problems in the immigration sphere, plus concerns about mass surveillance by British intelligence services and the subsequent transfer of personal data, primarily to American authorities and services. At the same time, the resolution welcomes the fact that the decision of the European Commission will only apply for four years, while calling on it to constantly monitor the relevant practices applied by the British authorities.

[29] European Parliament. (2021). *European Parliament resolution on the adequate protection of personal data by the United Kingdom (2021/2594(RSP))*. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0262_EN.htm

Finally, on June 28, 2021, the European Commission adopted an adequacy decision for the United Kingdom under the GDPR. Since that time, it has been possible to freely conduct data-sharing between the European Union and the United Kingdom, where it benefits from an essentially equivalent level of protection to that guaranteed under EU law. The adequacy decision also facilitated the correct implementation of the EU-UK Trade and Cooperation Agreement, as it includes strong safeguards in case of future divergence, such as a 'sunset clause' that limits the duration of adequacy to four years.[30]

Moreover, to build upon this, the UK Government has established a new post-Brexit council to ensure that personal data transfers around the world match the protection they have in Britain.[31] On January 25, 2022, a group of experts consisting of the world's leading academics and digital industry figures (including representatives of Google, Mastercard, and Microsoft) met for the first time to help Britain seize the opportunities of better global data sharing. The International Data Transfer Expert Council was launched to provide independent advice to the government so that it could achieve its mission to unlock the benefits of free and secure cross-border data flows now that the country has left the EU.[32] This is one of the measures enshrined in the UK government's recent consultative document, 'Data: A New Direction', which explores various ways in which the UK might reform its data protection regime, but does not actually state a change in policy.[33]

On July 18, 2022, the Data Protection and Digital Information Bill[34] was introduced in the British House of Commons, containing a package of amendments to the UK's data protection regime. The Bill is currently making its way through Parliament, but very slowly. This is due to the change to the UK's governmental leadership. The Bill's impact assessment states that «the government's view is that reform of UK legislation on personal data is compatible with the EU maintaining free flow of personal data from Europe».[35] However, whereas the proposed multiple amendments the Bill looks quite different to the EU' regulatory approach in the field. The more the UK diverges from GDPR, the more likely its adequacy agreement with the EU could be undermined.[36] Those seeking a substantial streamlining of requirements and the removal of obstacles to innovation and business may feel the Bill does not go far enough; on the other hand, the proposals could be viewed as diverging sufficiently from the EU GDPR to threaten the UK's adequacy status, which to be reviewed in 2024. Much depends on the balance struck in the final text of the Bill. In any case, the EU's rules compliance is a huge influencing factor in the UK's legal drafting even after Brexit.

Another recent example may be added here to support our thesis on the EU's influence on co-regulation. The European Commission has decided to allow personal data to be transferred from the

30 European Commission. (2021). *Data protection: Commission adopts adequacy decisions for the UK.* https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_3183

31 Phillips, A. (2022, January 25). Brexit truimph: UK forges ahead with tech giants to use new powers to boost data flow. *Express.* https://www.express.co.uk/news/uk/1555689/Brexit-news-Britain-tech-giants-data-flow-protection-privacy-google-microsoft

32 UK Government. (2022). *Global data experts fire up government's plans to promote free flow of data: Press release.* https://www.gov.uk/government/news/global-data-experts-fire-up-governments-plans-to-promote-free-flow-of-data

33 Dove, E. (2021, November 10). Data: A new direction — But which direction? A commentary on the UK Government's public consultation on reforms to the data protection regime. *The Mason Institute Blog.* https://blogs.ed.ac.uk/mason-institute/2021/11/10/data-a-new-direction-but-which-direction-a-commentary-on-the-uk-governments-public-consultation-on-reforms-to-the-data-protection-regime-by-edward-dove/

34 UK Parliament (2022). *Data Protection and Digital Information Bill.* https://bills.parliament.uk/bills/3322

35 UK Government. (2022). *Data Protection and Digital Information Bill: Impact assessments.* https://www.gov.uk/government/publications/data-protection-and-digital-information-bill-impact-assessments

36 *UK to reform data protection, throwing EU adequacy ruling into doubt.* https://www.euractiv.com/section/digital/news/uk-to-reform-data-protection-throwing-eu-adequacy-ruling-into-doubt/

European Union to South Korea under the GDPR.[37] The adequacy decision was issued only after amendments were added to South Korea's Personal Information Protection Act (PIPA), which strengthened the investigatory and enforcement powers of PIPC, South Korea's independent data protection authority. Furthermore, during the adequacy talks, the European Commission and the PIPC agreed on several additional safeguards to increase the protection of personal data processed in South Korea, including with respect to transparency (by requiring South Korean digital platforms to inform Europeans about the processing of their data) and onward data transfers (by ensuring that data continues to benefit from the same level of protection when further transferred to third-party countries).[38]

After the recognition by the European Court of Justice in 2020 of the EU-US Privacy Shield as a document that no longer ensures the proper and legal transfer of personal data from the territory of the European Union to the United States of America,[39] there were many misunderstandings when US companies operate in the EU territory.[40] And the United States and the European Commission have agreed in principle on a new Transatlantic Data Privacy Framework that will make it easier for companies to transfer personal data, including employee data, from the EU member-states to the United States.[41] The new framework cooperation, announced in March 2022, aims to address the privacy concerns referred to by the EU Court of justice in 2020 when it invalidated the previous EU-US Privacy Shield document.

The Transatlantic Data Privacy Framework aims to introduce better privacy protections to limit US intelligence activities related to the personal data of EU residents and allow EU residents to claim compensation through an independent Data Protection Court.

The European Commission cited several key principles of the new structure, noting that:

- based on the new framework, data will be able to flow freely and safely between the EU and participating U.S. companies;
- a new set of rules and binding safeguards to limit access to data by U.S. intelligence authorities to what is necessary and proportionate to protect national security;
- U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards;
- a new two-tier redress system to investigate and resolve complaints of Europeans on access of data by U.S. Intelligence authorities, which includes a Data Protection Review Court;
- strong obligations for companies processing data transferred from the EU, which will continue to include the requirement to self-certify their adherence to the Principles through the U.S. Department of Commerce;

---

37 European Commission. (2021). *Commission implementing Decision of 17.12.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the Republic of Korea under the Personal Information Protection Act.* https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf

38 BlankRome. (2022, January). *The BR Privacy & Security Download.* https://www.blankrome.com/publications/br-privacy-security-download-january-2022

39 European Court of Justice (2020). *Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. Request for a preliminary ruling from the High Court (Ireland).* https://curia.europa.eu/juris/liste.jsf?num=C-311/18

40 Cory, N., Castro, D., & Dick, E. (2020, December 3) *'Schrems II': What invalidating the EU-US privacy shield means for transatlantic trade and innovation. Information Technology and Innovation Foundation.* https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic/

41 The White House (2022). *Fact sheet: United States and European Commission announce Trans-Atlantic Data Privacy Framework.* https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

- specific monitoring and review mechanisms.[42]

While many of the details still remain unclear, the US and European Commission have represented that the next steps will be to translate the agreement in principle into legal documents.[43] And the tendency will continue. According to the European Commission's Data Act, which was published on February 23, 2022, digital platforms like Amazon and Microsoft must set up safeguards against illegal data transfers to non-EU governments,[44] thus pushing the development of national legal arrangements in the sphere. The developments will be keenly followed by a number of tech giants like Meta, which is at risk of a suspension order being slapped on its EU-US data transfers following a long-running complaint that's still grinding through the EU's GDPR enforcement procedures.[45] Google, whose analytics product has been hit with warnings by DPAs around the bloc over illegal transfers of personal data, should be also added to the list.[46] In this regard should be also mentioned Microsoft, whose cloud-based productivity suite 365 is under GDPR review by German DPAs that's further complicated by the data transfers issue, to name three high profile examples.[47]

Conclusions

This study shows that the problem of personal data protection in contemporary conditions has the same origin and requires the same solution — to maintain an optimal balance between human rights, society, and the state. The means of establishing a balance of rights is a legal regime for the protection of personal data that is based on certain principles common to all democratic states, regardless of the specific features of their legal systems. This set of principles constitutes a body of good information practice: there should be no personal data processing systems in which the existence of personal data processing is secret: the person must be notified about the processing and use of their personal data, provided with the opportunity to know what information their personal data contains, be informed about why such data is cultivated, and how it is used. People should also be able to prevent the use or dissemination of their personal data for purposes they have not agreed upon and given the opportunity to make corrections or additions to their personal data. In addition, all organizations that process or use data in a form that allows identification of an individual should be required to take measures against the misuse of personal data, and personal data should only be used for the purposes for which it was collected.

With regard to the example of the UK's withdrawal from the European Union, it can be stated that the British legal regime still maintains a certain dependence on the EU and its legal order, since, as a non-member country, it does not have the ability to influence decisions made in the Union. In addition, in principle, Brexit has complicated the cross-border activities of digital platforms in

[42] European Commission (2022). *Trans-Atlantic Data Privacy Framework*. https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100

[43] TrustArc Privacy Intelligence (2022). *New EU-US Agreement: Trans-Atlantic Data Privacy Framework*. https://trustarc.com/blog/2022/03/25/trans-atlantic-data-privacy-framework/

[44] Chee, F. Y. (2022, February 4). EU aims to tighten curbs on data transfers to non-EU governments — EU document. *Reuters*. https://www.reuters.com/business/eu-aims-tighten-curbs-data-transfers-non-eu-governments-eu-document-2022-02-03/

[45] Lomas N. (2022, August, 11). Facebook avoids a service shutdown in Europe for now. *TechCrunch*. https://techcrunch.com/2022/08/11/facebook-europe-shut-down-delay/

[46] Lomas N. (2022, February, 10). France's privacy watchdog latest to find Google Analytics breaches GDPR. *TechCrunch*. https://techcrunch.com/2022/02/10/cnil-google-analytics-gdpr-breach/

[47] Lomas N. (2022, February, 15). Public sector bodies' use of cloud services probed in joint EU data protection enforcement. *TechCrunch*. https://techcrunch.com/2022/02/15/edpb-cef-public-sector-cloud/

both jurisdictions, since the uniform legal regulation within the EU for all member states has been replaced by a dichotomy in the form of the presence and interaction of the relevant legal norms of both the UK and the European Union, which must now be followed, and which may contain mutual contradictions.

In legally regulating data protection, the UK is forced to obey the EU's legal order and is dependent on the will and legal prescriptions of the Union's institutions, primarily with respect to the need to receive an adequacy decision from the European Commission. However, even after the adoption of such a decision, the legal order of the United Kingdom will still be under the EU's constant control with respect to the assessment of the level of adequacy of its system of personal data protection and ensuring sufficient data-sharing, which casts doubt on the stability and predictability of relations in this area, thus shifting the degree of influence in the co-regulation to the EU's supranational authorities. This is also confirmed by the examples of other third countries, in particular South Korea and the United States, demonstrating the importance of strengthening and developing European integration mechanisms that can successfully overcome the reverse of integration, not only minimizing the negative consequences of disintegration, but also strengthening international integration and additionally influencing the legal orders of states that are not part of the integration entity.

References

1. Babynina, L. O. (2021). Torgovoe soglashenie mezhdu ES i Velikobritaniej: Mezhdu kondicional'nost'ju i suverenitetom [Trade and cooperation agreement between the EU and the UK: Conditionality versus sovereignty]. *Sovremennaja Evropa*, (2), 5-16. http://dx.doi.org/10.15211/soveurope220210516
2. Beck, E. J., Gill, W., & De Lay, P. R. (2016). Protecting the confidentiality and security of personal health information in low- and middle-income countries in the era of SDGs and Big Data. *Global Health Action, 9*(1), 32089. https://doi.org/10.3402/gha.v9.32089
3. Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review,* 107(1), 19-35.
4. De Hert P., & Papakonstantinou, V. (2017). The rich UK contribution to the field of EU data protection: Let's not go for "third country" status after Brexit'. *Computer Law & Security Review, 33*(3), 354-360. https://doi.org/10.1016/j.clsr.2017.03.008
5. Eisenmann, T., Geoffrey, P., & Van Alstyne, M. (2011). Platform envelopment. *Strategic Management Journal, 32*(12), 1270-1285. https://doi.org/10.1002/smj.935
6. Entin, M., & Galushko, D. (2021). O pravovykh posledstviyakh Brekzita (na primere zashchity personal'nykh dannykh) [On the legal consequences of Brexit (on the example of personal data protection)]. *Sovremennaya Evropa, 105*(5), 45-55. http://dx.doi.org/10.15211/soveurope520214555
7. Fabbrini, F., Celeste, E., & Quinn, J. (Eds.) (2021). *Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty*. Hart Publishing.
8. Kira, B., Sinha, V., & Srinivasan, S. (2021). Regulating digital ecosystems: Bridging the gap between competition policy and data protection. *Industrial and Corporate Change, 30*(5), 1337-1360. https://doi.org/10.1093/icc/dtab053
9. Martirosjan, A. Z. (2021). Realii cifrovogo suvereniteta v sovremennom mire [Realities of Digital Sovereignty in the Modern World]. *Mezhdunarodnaja Zhizn*, (3), 28-35. https://interaffairs.ru/jauthor/material/2483
10. Mingers, J., & Standing, C. (2018). What is information? Toward a theory of information as objective and veridical. *Journal of Information Technology, 33*(2), 85-104. https://doi.org/10.1057/s41265-017-0038-6
11. Nicolaïdis, K. (2017). The political mantra: Brexit, control and the transformation of the European order. In F. Fabbrini (Ed.), *The Law & Politics of Brexit.* Oxford University Press.

12. Nitecki, J. Z. (1985). The concept of information-knowledge continuum: Implications for librarianship. *The Journal of Library History (1974-1987), 20*(4), 387-407. http://www.jstor.org/stable/25541654
13. Prosser, W. L. (1964). *Handbook of the Law of Torts*. West Publication Corp.
14. Resta, G. (2011). The new frontiers of personality rights and the problem of commodification: European and comparative perspectives. *Tulane European and Civil Law Forum, 33*, 49-57.
15. Voigt, P. & von dem Bussche, A. (2017). *The EU general data protection regulation (GDPR). A practical guide*. Springer.
16. Voss, W.G. (2019). Obstacles to transatlantic harmonization of data privacy law in context. *Journal of Law, Technology & Policy, 2*, 405–463.
17. Voss, W.G. (2020). Cross-Border data flows, the GDPR, and data governance. *Washington International Law Journal*, 29(3), 485-532.
18. Walker, R. (2015). *Success with big data: From data and analytics to profits.* Oxford University Press.

Information about the authors:

Mark L. Entin — Dr. Sci. in Law, Professor, Head of European Law Department, MGIMO-University, Moscow, Russia.
entinmark@gmail.com
ORCID: https://orcid.org/0000-0001-9562-8340

Ekaterina G. Entina — Dr. Sci. in Politics, Associate Professor, Director of Mediterranean Studies Centre, Faculty of World Economy and International Affairs, HSE University, Moscow, Russia.
e.entina@hse.ru
ORCID: https://orcid.org/0000-0003-4198-4870

Dmitriy V. Galushko — PhD in Law, Associate Professor, Department of Legal Regulation of Economic Activity, Financial University, Moscow, Russia.
galushkodv@gmail.com
ORCID: https://orcid.org/0000-0001-9562-8340

Сведения об авторах:

Энтин М. Л. — доктор юридических наук, профессор, заведующий кафедрой европейского права Московского государственного института международных отношений (МГИМО-Университет) МИД России, Москва, Россия.
entinmark@gmail.com
ORCID: https://orcid.org/0000-0001-9562-8340

Энтина Е. Г. — доктор политических наук, доцент, директор центра средиземноморских исследований Факультета мировой экономики и мировой политики Национального исследовательского университета «Высшая школа экономики», Москва, Россия.
entinmark@gmail.com
ORCID: https://orcid.org/0000-0003-4198-4870

Галушко Д. В. — кандидат юридических наук, доцент, доцент департамента правового регулирования экономической деятельности Финансового университета при Правительстве Российской Федерации, Москва, Россия.
galushkodv@gmail.com
ORCID: https://orcid.org/0000-0002-4484-9423