PHRG
PEACE HUMAN
RIGHTS GOVERNANCE

Volume 6, Issue 1, June 2022

Tracing the Expansive Effect of the GDPR in the Third Countries. The Cases of Russia, Ukraine and China

Stanislav Gubenko

Research Articles*

DOI:

10.14658/pupj-phrg-2022-1-4

How to cite:

Gubenko S. (2022) 'Tracing the Expansive Effect of the GDPR in the Third Countries. The Cases of Russia, Ukraine and China', *Peace Human Rights Governance*, 6(1), 79-96.

Article first published online

June 2022

*All research articles published in PHRG undergo a rigorous double-blind review process by independent, anonymous expert reviewers

PADOVA UP

PHRG 6(1), June 2022

Tracing the Expansive Effect of the GDPR in the Third Countries. The Cases of Russia, Ukraine and China.

*Stanislav Gubenko**

Abstract

This research aims at analyzing the “expansive effect” of the General Data Protection Regulation (GDPR) in three non-EU case countries, i.e. Russia, Ukraine and China, to understand how the GDPR provisions affect, or are affected by, the interaction with three non-EU legal systems. The recently adopted GDPR, being a set of comprehensive data processing rules and penalties for violating data protection regulations, has set a very high standard for the other states in developing their own data protection regulations, but at the same time, the GDPR has brought about a wide range of compliance challenges. Due to the extraterritorial character of the General Data Protection Regulation, these challenges regard not only the EU member states but also any organisations around the world engaged in professional or commercial relations with the European Union. Therefore, there is a gap in understanding the interplay between the newly-built European data protection system and the legal systems outside the EU, which this research seeks to cover.

Keywords: *GDPR, General Data Protection Regulation, Russia, Ukraine, China, personal data.*

* University of Luxembourg, email: stanislav.gubenko@uni.lu

Introduction

With the adoption of the 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 the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and its entry into force in May 2018, the European Union obtained a powerful instrument of personal data legal protection (European Parliament 2016). The General Data Protection Regulation (later on, the GDPR) gave Europe a set of comprehensive data processing rules and a set of penalties for violating data protection regulations. The standards set by the GDPR are, from one side, serve as a paragon for various states in developing their own data protection regulations, but, from the other side, the GDPR brings about a wide range of compliance challenges. Due to the extraterritorial character of the General Data Protection Regulation, these challenges regard not only the EU member states but also any organisations around the world engaged in professional or commercial relations with the European Union (European Parliament 2016).

The exterritoriality of the GDPR automatically enabled the interaction of the European regulation with non-EU legal systems, as, according to Article 3 of the GDPR, this Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union (European Parliament 2016).

As, based on the Article 3 EU GDPR, the activity of a vast number of non-EU organisations all over the world falls under the competence of the new European data protection regulation, non-EU states face the need to adapt to the GDPR in order to ensure smooth and efficient professional and commercial activity of the local organisations working with the EU.

This research aims at analyzing the “expansive effect” of the GDPR provisions on non-EU countries, i.e. Russia, Ukraine and China, to understand how the GDPR provisions affect, or are affected by, the interaction with three non-EU legal systems. Russia, Ukraine and China were not chosen occasionally. These case countries represent three very different legal and political contexts and can provide a comprehensive outlook on the argument under consideration and, therefore, ensure a sound basis for comparative analysis.

In the process of preparation for the research, it was discovered that due to the novelty of the GDPR, extensive scientific literature on the impact of the GDPR on the third countries was almost absent, although there have been some studies on separate aspects of the impact of the GDPR on the third countries (Qiu 2019)In the years directly succeeding the GDPR's entrance into force, there was substantial confusion on how exactly personal data processors and ordinary people should adapt to the new regulation. Many questions were arising, while the answers were often insufficient, so a looming gap needed to be bridged. This research attempts to clearly illustrate what this implementation gap is and provide policymakers with some practical insights about the interaction of the GDPR with the third countries' legal systems.

The current research was carried out in three main phases: first, the readers will be provided with some important historical background of the right to privacy and of the right to have one's personal data protected, second, an overview of Russian, Ukrainian and Chinese systems of personal data protection will be presented. At this stage, relevant legal provisions, judicial decisions and legal/business literature will be analysed to build a picture of the structure of each country's data protection regulation. In the second part of the research, the aim will be to understand how the three non-EU regulations of personal data protection correlate with the GDPR provisions and whether there is any conflict between the GDPR and the legal systems of each country.

The results of these parts of the research will lay the groundwork for the third phase of research. In the third phase, country-by-country analyses of personal data protection in bilateral relations will be conducted. Here the practical interaction of the EU legal system of personal data protection interacts with Russian, Ukrainian and Chinese systems of personal data protection will be examined. The aspects under consideration of such interaction largely depend on a specific context but can generally be divided into several main groups: political, economic and digital, with some exceptions. As for Ukraine, it was decided to consider the following topics: the EU Commission adequacy decision of Ukrainian privacy and data protection legislation; the GDPR in relation to the country's agreement of association with the EU; European Neighbourhood Policy: Eastern partnership, Horizon 2020, EU Twinning projects in Ukraine, TAIEX; science and tech partnership. Most of these topics can be analysed only in relation to Ukraine, as, for example, neither Russia nor China has concluded an association agreement with the EU, and neither of these two countries has strived to obtain the EU Commission adequacy decision, as Ukraine has done. As for Russia, a chapter will be dedicated to EU bilateral and regional cooperation programmes with

Russia; Social media (Yandex, Telegram, Vkontakte) in relation to the GDPR; Russia-EU financial relations. The Chinese section of this part of the article will cover the following topics: specific cooperation programs on personal data protection; personal data protection in Sino-EU trade relations and bilateral cooperation on science and technology; Chinese digital platforms and personal data protection. The cases of AliBaba, TikTok and WeChat; Personal data protection issues in the Beijing Winter Olympics 2022.

This part of the work will imply documentary research, using both primary and secondary sources. Primary sources are represented by official documentation of various kinds, such as EU and national statements and declarations, international agreements, data protection regulations of single organisations. Secondary sources include but are not limited to scientific articles and monographs, and social media. The sources are consulted in their respective languages (English, Russian, Italian, Ukrainian and Chinese).

Apart from this, a coverage of some general issues related to the expansive effect of the GDPR in the world will be provided. These issues include the impact of the GDPR on the sphere of scientific research and international trade. Then, the issues of the GDPR jurisdiction and enforceability will be contemplated on. Here it will be sought to answer the question of the perspectives and challenges of the GDPR implementation abroad by looking both at the EU and international legal practice and consulting relevant secondary sources.

In the final part of the article, the conducted work will be summarised and relevant conclusions will be given.

1. Main Part

1.1. Privacy and Personal Data Protection in Russia, Ukraine and China in Historical and Linguistic Perspectives

First and foremost, the privacy and personal data protection will be considered from a historical and, to some extent, also linguistic perspective. This will contribute to understanding the reasons of difference in the expansive effect of the GDPR from country to country.

The Right to Privacy is thought to be first introduced by Samuel D. Warren and Louis D. Brandei in 1890 (Brandeis and Warren 1890). Authors deeply analysed the legal and historical backgrounds of the ‘incipient’ right to privacy or “the right to be let alone”. As the authors put it, “It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is" (Brandeis and Warren 1890). But Warren and Brandeis based their reasoning only on the Western reality (for instance, American). If one looks at the evolution of the right to privacy, one may see that the Western World mainly led it. In 1948 the Universal Declaration of Human Rights was adopted, and the Right to Privacy was included in it (United Nations 1948). In 1970, the first law in personal data protection in the world was adopted in Hessen, Germany (Feldman and Stepanova 2020). In 1980 OECD published the guidelines on data protection, and in 1981 the Council of Europe adopted the Data Protection Convention, also known as Convention 108 (Council of Europe 2018). Convention 108 was modernised in 2018 as a result of long 7-years work and negotiations and obtained a name of Convention 108+ (Council of Europe 2018).

As it can be seen, the history of the right to privacy and the right to personal data protection is strongly associated with the Western world. So, the right to privacy is thought to be first introduced by American lawyers Warren and Brandeis in 1890. They claimed to have built up the concept of a right to privacy partially on English case law. However, according to them, the right to privacy had been already previously expressed in a French law of the year 1868. As for the right to personal data protection, it was formulated by another American scientist Alan Westin in 1970. The emergence of the right to have personal data protected was tightly connected with the development of computer technology, which, as we know, was actively led by the United States in the second half of the 20th century.

But what about Russia, Ukraine and China? The reasonable question arises of whether there are roots of privacy and personal data protection in non-Western countries. Now it will be sought to trace the origins of the right to privacy and of personal data protection in Russia, Ukraine and China. This will allow to understand better why personal data protection regimes are so different and how the three legal regimes under consideration should be approached when the expansive effect of the GDPR abroad is analysed.

If one looks at the Chinese cultural, historical and linguistic background, it can be see that, according to Lo Chung-Shu, professor of philosophy at the West-China University, the word "right" is basically not present in Chinese tradition (Sun 2020). Instead, in the Confucian tradition, we find that "the basic ethical concept of Chinese social and political relations is to fulfil obligations to neighbours, rather than claim rights. Mutual obligations are regarded as the fundamental Confucian thought" (Lo 2018). The word "right" is thought to have come to the Chinese language in the second half of the 19 century when Chinese writers adopted the works of a Japanese scholar who studied Western public law (Lo 2018). In Chinese, the word "right" is composed of two characters (权利), the first of which means "power", while the second means "interest". So, the "right" is perceived as "power and interest": Going further, it may be seen that the word "freedom" was introduced by the translators of Western academic works in 1903 and that the word "freedom" in Chinese (自由) means "self/one's own and reason" (personal reasons). The Chinese translation of the word "privacy" is "隐私", which means "hide" and "private". However, according to Cao Jingchun, in Chinese "隐私" has negative connotations, and "it was initially common for Chinese to misunderstand privacy as relating to shameful secrets" (Denton et al. 2018). As Cao Jingchun puts it, "most people consider privacy matters to be shameful to talk about publicly and do not want to disclose them. Therefore, when their privacy is invaded, they prefer to ignore the invasion if it is bearable; or sometimes choose to solve the problem themselves rather than going to court" (Denton et al. 2018).

The brief overview of the concepts of "right", "freedom" and "privacy" in China demonstrates that the Chinese perception of privacy and personal data protection may be significantly different from the Western one. Although partially based on the Western concepts, mainly because of their linguistic adoption, Chinese concepts of "right", "freedom", and "privacy" have different cultural and historical backgrounds. The Chinese translation of these words, though being commonly accepted, does not entirely depict their initial English meanings. Deep understanding of Chinese cultural, linguistic and historical backgrounds of the concepts of privacy, rights and freedom is not within the scope of this article, but it would be definitely helpful to analyse these three concepts in-depth for the sake of better understanding the expansive effect of the GDPR.

As for Russia and Ukraine, these two countries will be discussed together and further specifications for each country will be given in the next part of the conclusions. The decision not to separate Russia from Ukraine was made because for a very long time, Russia and Ukraine were a part of the same state - the USSR. If we look further, a substantial territory of modern Ukraine made part of the Russian Empire, and, even further in history, Kyiv was thought to be the "Mother of Russian cities". For this reason, consideration of Russian and Ukrainian contexts together in our case is deemed to be generally acceptable.

Some elements of the right to privacy, i.e. the secrecy of correspondence, can be seen in the Postal Charter of 1857 and Telegraph Charter of 1876 of the Russian Empire. The Criminal Code of 1903 introduced a ban on the intervention by the state officials who carry out justice to personal and family life of the citizens. The Constitution of the Russian Soviet Federative Socialist Republic of 1918 did not give much space to human rights. It only referred to the prohibition of exploitation, the right of egalitarian land use, the liberation of labour of the masses from under the yoke of capital (Constitution of the RSFSR 1918*)*. For the first time, a chapter dedicated to the rights and obligations of citizens appeared in the Constitution of the USSR of 1936. It should be noted that the adoption of the Constitution occurred right before the Great Terror when Joseph Stalin launched a large-scale repression campaign. The Soviet totalitarian regime was eliminating those scarce elements of human rights which were present before. The human rights issues were raised again only after the death of Stalin; however, the concept of rights was in a very underdeveloped form. With the dissolution of the Soviet Union, human rights received much more attention than before. The Russian and Ukrainian human rights frameworks got a new chance for development but in somewhat different directions.

1.2. Correlation of Russian, Ukrainian and Chinese Regulations of Personal Data Protection with the GDPR Provisions and Practical Interaction of the EU System of Personal Data Protection with Russian, Ukrainian, and Chinese Data Protection Systems

After giving a brief historical and linguistic background, the findings are presented of the analysis of how Russian, Ukrainian and Chinese regulations of personal data protection correlate with the GDPR provisions, whether there is any conflict between the GDPR and the legal systems of each country and how the EU legal

system of personal data protection interacts in practice with Russian, Ukrainian and Chinese systems.

1. Russia.

Mandatory data localisation in the Russian Federation, introduced in June 2018 by the "Yarovaya Law" (or the Yarovaya package - Russian federal laws №374-FZ and №375-FZ), is deemed to be the main cornerstone of the interaction between the GDPR and the Russian data protection regime (The State Duma of the Russian Federation 2016). The contradiction occurs in case Russian telecommunication operators store information about EU data subjects on their servers without the consent of the data subject himself and without a court decision to provide this data to the Russian law enforcement bodies. In such case it is impossible to avoid the violation of the General Data Protection Regulation, as, according to article 5 GDPR "data must be kept in a form that does not permit the identification of an individual for a longer period than necessary for the purposes of data processing, meaning that the personal data have to be deleted or anonymised as soon as possible" (European Parliament 2016).

Data protection issues are always covered in the EU-Russia cooperation projects, although not always covered extensively. We may hypothesise that the degree of awareness about the GDPR of the Russian side is perhaps shallow, as the GDPR, being foreign to the Russian legal reality, is not well-known by most Russian citizens, and the lack of explanation of the GDPR in the considered legal documents on bilateral cooperation is evident. This puts under question the extent to which the GDPR is actually influencing EU-Russian relations. Another thorny question is the enforceability of the GDPR in relation to its "extraterritoriality principle". At the moment there are no relevant legal cases in this regard, so the ways to see how the GDPR provisions are being implemented in the EU-Russian relations are substantially limited.

*2. **Ukraine**.*

First, the rights to privacy and personal data protection outlined in the Ukrainian Law "On personal data protection" and in the Ukrainian Constitution, are much less defined than those in the GDPR. This may create confusion in interpretation. The Ukrainian mechanism of cross-border transfers of personal data is very similar to the mechanism of adequacy decisions of the GDPR - if Ukraine recognises an adequate level of personal data protection of a country, then the cross-border transfer is endorsed (Kobrin et al 2020). However, while Ukraine views the EEA member states as ensuring adequate levels of personal data protection, the European Commission has not issued an adequacy decision for Ukraine yet, so there are barriers for transfers of personal data from the EU to Ukraine.

Ukraine aspires to become an EU member state and strives to contribute to the integration with the European Union, also in the field of data protection. With the adoption of the GDPR, it became a key standard for Ukraine in approximating its data protection legislation to the European one. In fact, the traces of the GDPR in the EU-Ukraine relations are omnipresent. It is seen both from the efforts Ukraine puts in reforming its legislation according to the European standards with the help of the EU Twinning and TAIEX projects and from the Eastern Partnership and Horizon 2020. Having decided to integrate into Europe, Ukraine has been persistently working on enhancing its data protection regulation capacity, which is one of the obligations imposed on Ukraine in the EU-Ukraine Association Agreement. Although by now, the Ukrainian legislation on data protection has not been reformed yet, Ukraine has made significant steps in the GDPR direction. Although the COVID-19 pandemic significantly impeded the implementation of the reforms of the data protection regime, the Ukrainian Parliament Committees on human rights and digital transformation, the Office of the Ombudsman, and the Twinning Ombudsman Ukraine Project have been working on elaborating the approaches for the approximation of the Ukrainian legislation on personal data to the new EU Regulation 2016/679.

3. China.

In 2017 the Chinese Cybersecurity Law introduced mandatory data localisation. However, unlike the Russian Yarovaya law, the Chinese Cybersecurity Law does not provide any further information on the period of storage of personal data. At the same time, a "security assessment" has to be conducted for personal data to be sent from China abroad. The difficulties may occur in case an EU supervisory authority, following the GDPR provisions, requests a China-based processor of personal data to provide personal data of an EU data subject, and the Chinese security assessment for some reasons will not permit the overseas transfer of this data (Zhong 2021).

The analysis of the bilateral EU-China cooperation programs showed that although officially personal data protection is deemed important by both the EU and China, bilateral cooperation directly focusing on personal data protection is practically absent. The analysis of the personal data protection issues in EU-China trade relations showed no observed impact of the GDPR on Sino-EU trade, while the analysis of the bilateral cooperation on science and technology revealed the concerns of the European Union about "the potential for Chinese state-controlled enterprises and institutions to transfer data or intellectual property from Europe to China" (Yojana 2021). Moreover, the European Commission recently proposed China's complete exclusion from participation in Horizon 2020 and other sensitive research projects for not sharing core values of the European Union (Yojana 2021). The analysis of personal data protection issues in the operation of Chinese digital platforms showed that although in general, all three considered platforms (AliBaba, TikTok and WeChat) adapted their privacy policies to the European users, there have been some legal complaints and even litigations concerning alleged violations of the European data protection rules. Furthermore, the analysis raised several important questions concerning the possible impact of the Chinese digital governance system on the treatment of the EU data subjects' personal data. Finally, the expansive effect of the GDPR was analysed by looking at the personal data protection issues in the Beijing Winter Olympics 2022. Here the substantial influence of the international sport community represented by the WADA, IOC and IPC on the privacy and data protection standards (in some cases including the GDPR) was noted. However, the analysis revealed some challenges in the interaction between the Chinese data protection regime and the European regime framed by the GDPR.

1.3. Analysis of the Relationship between the Influence of the GDPR and the Level of the overall Influence of the EU on a Single Country

Although, as it was stated previously, cultural, historical, and linguistic backgrounds are of high importance when analysing the expansive effect of the GDPR, it is also deemed no less important to define the relationship between the influence of the GDPR and the level of the overall influence of the EU on a single country. In other words, the question arises of whether the GDPR may have an independent effect on a country, or it produces only a lateral effect of the EU influence on this country.

In the case of Ukraine, we see that the EU-Ukrainian relations are very close. Ukraine is interested in absorbing European experience in various areas and aims at joining the EU in the future. Ukraine is an active participant in various cooperation programs with a very wide scope - from personal data protection to the fiscal area. Reaching an adequate level of personal data protection is crucial for Ukraine to join the European Union. So, Ukraine views the reformation of the national data protection regime according to the GDPR standards not as an end in itself but as a means to achieve a bigger goal.

Unlike Russia and China, the Ukrainian case provides us with an example of a comprehensive impact of the GDPR. In fact, in the case of Ukraine, we see the deep expensive effect of the GDPR in most of the considered fields. Here the GDPR can be seen not as a temporary foreign element which is introduced simply due to some coercive circumstances, such as in the case of the Winter Olympics 2022 in Beijing, when Beijing is bound to comply with the international regulation on personal data protection, but the expansive effect of the international regulation is only temporary. Ukraine is incorporating the GDPR, together with other European practices, on a state scale. This can be viewed as the main difference from the Russian and the Chinese cases.

The explanation for this phenomenon is rather simple and intuitive. Ukraine, although being historically at the crossroads between the East and the West. Western Ukraine has historically been culturally closer to Europe than to Russia, and in different periods of history was under Polish and Austrian administration, while Eastern Ukraine, on the contrary, generally felt closer to Russia than to Europe. In 2014, following the Euromaidan and the Ukrainian crisis, Ukraine officially chose the ‘European way’. The country signed the Association Agreement and launched the process of gradual European integration. Nowadays, Ukraine views the EU as its key partner and, what is very important, this is an unbalanced partnership. Ukraine perceives the EU as a role model rather than an equal partner, and the EU, as it has been seen in this article, often performs a role of a 'teacher' in relations with Ukraine. This political imbalance is deemed crucial for understanding the expansive effect of the GDPR in a broad context.

Russia, along with Ukraine, has also been historically close to Europe. Furthermore, some territories of the modern European Union previously made a part of the Soviet Union and earlier of the Russian Empire. However, as for the last seven-eight years, it can be seen that the main focus of Russian foreign policy is not directed at the EU. In fact, in 2013, the Russian government claimed the so-called "pivot to Asia", which meant prioritising the relations with the People's Republic of China. In the recent period, Russian relations with the European Union were badly affected by the Ukrainian crisis. In fact, after the well-known Crimean incident in March 2014, the European Union decided to freeze the assets of the Russian citizens found responsible for the misappropriation of Ukrainian state funds (European Council 2021). The EU imposed comprehensive sanctions on economic relations with the Russian Federation in certain sectors. The further aggravation of the EU-Russian relations was provoked by the EU disapproval of a series of alleged human rights violations in Russia. Summing up, the state of the EU-Russian relations is far from satisfactory, and it needs to be considered when analysing the impact of the GDPR on Russia.

As it has been seen, Ukrainian and Russian contexts in which we seek to measure the expansive effect of the GDPR, significantly differ from each other. They are also very different from the Chinese context. Unlike Ukraine, China does not view the EU as a key role model, providing a development framework and standards. Unlike Ukraine and Russia, China has never historically been at the crossroads between the East and the West and has sought to construct and promote its own development model. This becomes especially evident now when we observe the "shift in global power to the East" (Karaganov and Suslov 2018). As we see, China is playing an increasingly significant role in transforming the global political and economic order. It proposes the Non-Western IR theories (Acharya and Buzan 2009). These IR theories may vary between each other but are mainly united by the proposal of the alternative international order, not based on the traditional Western approaches to IR. For example, the moral realism IR theory of Yan Xuetong, claims that the Chinese global leadership, guided by the traditional Chinese notion that the moral values of righteousness and benevolence are above the legalistic Western values of equality and democracy, and the Chinese values "can, by all means, transcend the hegemonic values of the United States" (Yan 2013). As it can be observed, China's role has been shifting from the norm-taker to the norm-maker. China is becoming an increasingly "responsible state", it is taking the "responsibility to protect" (R2P), but also promoting its own values in the world and proposing an alternative to the Western values, as, for instance, in Sino-African relations[1]. Here, among others, a substantial change in the Chinese paradigm towards human rights can be observed. In the last years the country has been gradually integrating in the global human rights legal order, and, as Zhang, Y., and Buzan, B. (2019) stated, China has been moving "from a human rights pariah state to an active participant and shaper of global human rights governance" (Zhang and Buzan 2020). An essential aspect of the Chinese norm-making agenda is connected to China's development reorientation. China has successfully moved from "the world's factory" to an active participant and shaper of the global and European economy. China is proposing its economic development models and strives to build an economic system satisfying both its financial and political ambitions. In the process of China's economic norm-making and development reorientation, Europe has been playing an increasingly important role. In 2013 Europe became the second largest recipient (after Asia) of Chinese investments, while Asia's share decreased substantially. Most of the Chinese investments in Europe went through the "One Belt, One Road" initiative, and thanks to the Chinese investments, many European countries got a new chance for development.

So, we may see that the geopolitical balance in the case of the EU-Chinese relations is completely different from that of EU-Ukrainian and EU-Russian relations, and it may be argued that the degree of the GDPR impact on a country is to some extent dependent on this balance.

Another relevant indicator of the difference between the three contexts is the fact that, unlike Ukraine and Russia, China did not officially express its decision to obtain the adequacy decision from the European Commission. Moreover, although the Chinese data protection regime is currently undergoing a huge transformation, it is still completely different from the European one and, as we have seen, the question arises about the future impact of this transformation with regards to the GDPR. The question is whether the new coming Chinese law on personal data protection (the Personal Information Protection Law - PIPL) can be fully implemented in the case of far-reaching surveillance and exposure of a wide range of personal data to the state authorities. This is deemed especially important

1 The term's definition coincides with the one given at the 2005 World Summit of the United Nations General Assembly.

for the topic of our research considering that the PIPL is largely based on the GDPR and if the answer to the second question will be negative, then the overall credibility of the Chinese new coming data protection system can be questioned. This should be considered when analysing the interactions between Chinese and European data protection systems and the expansive effect of the GDPR.

Overall, it may be generally argued that historical and political contexts play a crucial role in evaluating the expansive effect of the GDPR, and it would be incorrect to consider the expansive effect of the GDPR out of the country context.

Conclusions

In the final part of this article, it will be sought to draw some general conclusions from the conducted research and to answer the key question of the research, i.e. if there is an expansive effect of the General Data Protection Regulation outside the EU and, what is probably even more important, what are the factors determining this expansive effect.

As for the practical interaction of the GDPR with the non-EU legal systems, the research revealed an important implementation gap. Being a European regulation, the GDPR is enforced on the territory of the EU through national data protection authorities. The national data protection authorities of the EU countries are responsible for ensuring compliance with the GDPR on their national territories and for dispensing justice in case of violations. The situation becomes much more complicated when we seek to analyse the GDPR enforcement mechanism in non-EU countries. As we have seen, there is no authority officially responsible for the enforcement of the GDPR in non-EU countries. Moreover, we do not find any legal cases regarding the violations of the GDPR in the third countries (GDPR Enforcement Tracker 2021).

The analysis of the GDPR influence on EU-Ukrainian, EU-Russian and EU-Chinese relations showed that there is no mechanism of the GDPR enforcement abroad. Indeed, if the legal cases and complaints regarding violations of the European data protection regulation are examined, it is seen that the punishment for breaching the GDPR is possible or in case one deals with a European company, or with a foreign company with branches in Europe (for example, TikTok, which has the European branch in Dublin, Ireland).

The findings of this article have confirmed the preliminary hypothesis that there is a gap in the implementation of the GDPR in EU foreign relations. In fact, putting together the vagueness of the GDPR enforcement mechanism abroad and the absence of legal cases concerning violation of the GDPR by the third countries, it may be concluded that there the enforceability gap indeed exists.

While a comprehensive expansive effect of the GDPR is clearly observed in most of the areas considered in the Ukrainian case, the impact of the GDPR in Russia and China is rather sporadic and uncertain. Referring to one of the previous conclusions here above, it can be claimed that the effect of the GDPR may positively correlate with the general state of bilateral relations between countries, the closeness of legal and political systems, and the country's orientation in foreign policy.

As for Ukraine, the traces of the GDPR in the EU-Ukraine relations are omnipresent. It has been seen both from the efforts Ukraine puts in reforming its legislation according to the European standards with the help of the EU Twinning and TAIEX projects and from the Eastern Partnership and Horizon 2020. It has been observed that the digital transformation and cybersecurity of Ukraine are among the key loci of the EU-Ukraine programs of bilateral cooperation, and this broadens the influence of the European data protection regime and urges Ukraine to respect the GDPR. Having decided to integrate into Europe, Ukraine has been persistently working on enhancing the capacity of its data protection regulation, which is one of the obligations imposed on Ukraine in the EU-Ukraine Association Agreement. Although, by now, the Ukrainian legislation on data protection has not been reformed yet, Ukraine has made significant steps in the GDPR direction.

As it has been said before, unlike Ukraine, Russia is not striving to integrate with Europe and adapt its data protection regulation to European standards. At the same time, data protection issues are always covered in the EU-Russia cooperation projects, although not always covered extensively. In this regard, much research work is needed to assess if these rules are followed in practice and what can be the challenges of the GDPR implementation in the EU-Russian relations. In fact, by looking only at the legal basis of the Russia-EU cooperation programmes, it seems difficult to find out to what extent the GDPR is implemented in them. However, taking into consideration that usually data protection issues, and the GDPR in particular, are not developed extensively in the legal documents on the EU-Russian bilateral cooperation, we may guess that the degree of awareness about the GDPR of the Russian side is rather low. In fact, the General Data Protection Regulation, being foreign to the Russian legal reality, is not well-known by most Russian citizens, and the lack of explanation of the GDPR in the aforementioned legal documents does not contribute to raising the understanding of the Russian side of the ways to comply with the European data protection regulation. This puts under question the extent to which the GDPR is actually influencing EU-Russian relations.

Talking about China, we have seen that the influence of the General Data Protection Regulation on China substantially varies depending on specific aspects under consideration. On the one hand, the general comparison of the Chinese and European data protection systems suggests the existence of significant differences in the two systems. At the same time, the new coming Chinese Personal Data Protection Law, which is expected to be adopted shortly, greatly mirrors the GDPR and may potentially contribute to easing some of the existing contradictions between the two systems. Although officially personal data protection is deemed important by both the EU and China, bilateral cooperation directly focusing on personal data protection is practically absent. It was especially visible in the bilateral trade relations and sci-tech cooperation. Therefore, judging from the official documentation on the EU-China bilateral trade, the GDPR has no observed impact on Sino-EU trade. At the same time achieving a common framework on personal data protection is a stumbling stone in Sino-EU cooperation on science and technology. As for the personal data protection issues in the operation of Chinese digital platforms, although they, in general, adapted their privacy policies to the European users, there have been some legal complaints and even litigations concerning alleged violations of the European data protection rules. Finally, the analysis of the personal data protection issues in the Beijing Winter Olympics 2022, revealed a series of controversies. In particular, the necessity to comply with the GDPR requirements is coupled with the Olympics host city's obligation to comply with the host country's data protection legislation, which also regards international data transfers. In this regard, a range of possible challenges for Beijing may be expected since the Chinese data protection regime substantially varies from the European regime framed by the GDPR.

References

Конституция РСФСР 1918 г. (Constitution of the RSFSR 1918). Retrieved September 21, 2021, from http://www.hist.msu.ru/ER/Etext/cnst1918.htm

Федеральный закон от 06.07.2016 N 374-ФЗ "О внесении изменений в Федеральный закон 'О противодействии терроризму' и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности" (Federal Law of 06.07.2016 N 374-FZ «On *Amendments to the Federal Law 'On Countering Terrorism' and certain legislative acts of the Russian Federation in terms of establishing additional measures to counter terrorism and ensure public safety")*. (2016). Retrieved September 16, 2021, from http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=201078&fld=134&dst=100132&rnd=214990.3492213126493249&#WltHAjSUhyDRzdrE

Acharya, A., & Buzan, B. (Eds.). (2009). *Non-Western International Relations Theory: Perspectives On and Beyond Asia (1st ed.)*. Routledge. https://doi.org/10.4324/9780203861431

Brandeis, L., & Warren, S. (1890). The right to privacy. *Harvard law review*, *4*(5), 193-220.

Council of Europe. (2018). *Convention 108 and Protocols*. Data Protection. Retrieved September 21, 2021, from https://www.coe.int/en/web/data-protection/convention108-and-protocol

Council of Europe. (2018). *Convention 108+: The modernised version of a landmark instrument—Newsroom*.https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108

Denton, S., Pauwels, E., He, Y., & Johnson, W. (2018). *Nowhere to Hide: Artificial Intelligence and Privacy in the Fourth Industrial Revolution*. Wilson Center.

Feldmann, T. A.-J., & Stepanova, O. (2020). *In a nutshell: Data protection, privacy and cybersecurity in Germany*. Lexology. https://www.lexology.com/library/detail.aspx?g=c9f86639-8e64-433f-b1d7-bee9430eaa50

European Council. (2021). *EU restrictive measures in response to the crisis in Ukraine*. Retrieved September 20, 2021, from https://www.consilium.europa.eu/en/policies/sanctions/ukraine-crisis/

GDPR Enforcement Tracker. *List of GDPR fines*. Retrieved April 4, 2021, from https://www.enforcementtracker.com

Karaganov, Sergei, and Suslov Dmitry. (2018). *A new world order: a view from Russia*. Russia in Global Affairs.

Kobrin, A., Korchynskiy, D., & Nekrutenko, V. (2020). *Ukrainian GDPR: The reality and future of privacy legislation in Ukraine* [IAAP]. https://iapp.org/news/a/ukrainian-gdpr-the-reality-and-future-of-privacy-legislation-in-ukraine/

Lo, C.-S. (2018). *A Confucian approach to human rights*. UNESCO. https://en.unesco.org/courier/2018-4/confucian-approach-human-rights

Qiu Y. (2019). 试析 *GDPR* 影响下奥运赛事承办方跨境传输个人数据的合规义务 ——以 *2022* 年北京冬奥会为例 *(A tentative analysis of the compliance obligations of the organizers of the Olympic Games in cross-border transmission of personal data under the influence of GDPR: Taking the 2022 Beijing Winter Olympics as an example).* 体育科学 (Tiyu Kexue), 7, 80-91.

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), OJ L 119, 4.5.2016, p. 1–88. ELI: http://data.europa.eu/eli/reg/2016/679/oj.

Sun, S. (2020). *A Commentary on Lo Chung-shu's Human Rights Philosophy.* China Human Rights. http://www.chinahumanrights.org/html/2020/MAGAZINES_0407/14965.html

United Nations. (1948). *Universal Declaration of Human Rights.* Retrieved September 21, 2021, from https://www.un.org/en/about-us/universal-declaration-of-human-rights

Yan X. (2013). *New Values for New International Norms.* China Int'l Stud., 38, 15.

Yojana, S. (2021). *EU says it can exclude China from EU research projects.* University World News. https://www.universityworldnews.com/post.php?story=20210217080942426

Zhang, Y., & Buzan, B. (2019). China and the Global Reach of Human Rights. *The China Quarterly, 241*, 169 - 190.

Zhong, L. (2021). *GDPR* 影响下我国涉欧企业的数据合规路径 *(The influence of the GDPR on the data compliance path of the Chinese companies operating in Europe).* 科学猫 (Kexue Mao). http://www.scicat.cn/1/jingjilunwen/20210421/4958765.html