Scientific Research Publishing

Beijing Law Review, 2023, 14, 1250-1270
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

The Risk-Based Approach to Personal Data Protection and the Response of the International Trade Law

Yuhong Yan

School of International Law, China University of Political Science and Law, Beijing, China
Email: cu224014@cupl.edu.cn

How to cite this paper: Yan, Y. H. (2023). The Risk-Based Approach to Personal Data Protection and the Response of the International Trade Law. *Beijing Law Review, 14,* 1250-1270.
https://doi.org/10.4236/blr.2023.143067

Received: June 13, 2023
Accepted: September 8, 2023
Published: September 11, 2023

Abstract

Data processing and transferring activities by businesses often result in increased risks to the rights and freedoms of data subjects, whereas the prescriptive and right-based approach, the dominating approach employed by lawmakers, fails to protect personal data as expected due to its inherent defects in managing risks. Accordingly, the risk-based approach, which endows businesses to calibrate their obligations of protecting personal data in terms of risks to enhance compliance with the principles and rules of personal data protection law, is introduced to the national and regional legislation as well as the international trade law to better manage risks so as to enhance the effectiveness of personal data protection. This paper investigates the backgrounds, meanings, functions, and advantages of the risk-based approach to personal data protection, and its embodiments in the EU, US, and China legislation, as well as in the international trade law such as USMCA and WTO members' consolidated negotiating texts produced in the Joint Statement Initiative on e-commerce. The paper then explores the mysterious and complicated "necessary and proportionate" test inherently contained in the risk-based approach, and whether data localization measures could pass such a test.

Keywords

The Risk-Based Approach, The-Right-Based Approach, Personal Data Protection, "Necessary and Proportionate" Test, USMCA, WTO

1. Introduction

Data, including personal data, is crucial for economic activities and trade, not only because it is the means of production through which global value chains (GVCs) are organized and services are delivered, but also because it is a core as-

set that could be used and traded (López González & Jouanjean, 2017). Through data collecting, processing, and transferring activities conducted by businesses, data fosters or promotes the development of new products, processes, organizational methods, and markets, and can generate great economic and social values (Casalini & López González, 2019; OECD, 2016). On the other hand, globalization brings more data processing and transferring activities, and results in ubiquitous and multitudinous risks, among which security risks and privacy risks to personal data are the most common forms (OECD, 2016). For instance, many businesses have suffered from digital security incidents through which their consumers' personal data are stolen by hackers, while some businesses may secretly sell their consumers' personal data to a third party or misuse consumers' personal data going beyond the original purpose without receiving additional consent from consumers.

Having considered the scale and frequency of security and privacy risks, protecting the availability, integrity, and confidentiality of personal data have been priorities for lawmakers and regulators for a long time. Furthermore, when data subjects are endowed with more positive rights to the protection of their personal data (e.g., the right to be forgotten), other risks that may negatively affect the realization of those rights shall also be taken into account. This explains why some legislation such as EU Data Protection Directive 1995[1] and General Data Protection Regulation (GDPR)[2] refers to the wider term "risks to the rights and freedoms of data subjects" instead of the narrower term security risks or privacy risks. In either case, however, most of the legislation adopts the prescriptive and right-based approach to protect personal data.

The right-based approach, which treats data subjects as rational people and the key players in the protection of their personal data, provides a certain level of protection by endowing data subjects with a set of rights and putting in place principles and rules of personal data protection for businesses to comply with. The characteristics of the right-based approach also reveal some inherent defects of this approach to protecting personal data. For instance, data subjects are not always rational, so treating them as key actors in protecting their personal data may negatively affect the efficiency of protection. Also, this approach manages risks in a universal and inflexible way, which may lead to unsatisfactory outcomes because the level of protection it provided may be disproportionate to the risks presented.

In order to address the defects of the right-based approach, some national, regional, and international legislation started to introduce the risk-based approach to better manage risks confronting personal data. It's widely accepted that Articles 24 and 25 GDPR represent the adoption of the risk-based ap-

[1]Directive 95/46/EC of the European Parliament and the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (hereinafter Data Protection Directive 1995).

[2]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 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 (hereinafter GDPR).

proach in the national legislation. And Articles 19.8(3) and 19.15(2) of the United States-Mexico-Canada Agreement (USMCA) as well as WTO members' consolidated negotiating texts produced in the Joint Statement Initiative ("JSI") on e-commerce imply the potential of the risk-based approach to be widely adopted at international level. Nonetheless, this approach has not yet been studied systematically and carefully. This paper aims to make this contribution and is structured in five sections. Following Section 1, Section 2 serves as a starting point by discussing the notions of risk and the right-based approach. Section 3 studies the meaning, functions, and advantages of the risk-based approach, and its embodiments in the national and regional legislation. Section 4 studies the embodiments of the risk-based approach in international trade law, and discusses the mysterious and complicated "necessary and proportionate" test inherently contained in the risk-based approach, and whether data localization measures could pass such a test. Section 5 concludes.

2. Risk and the Right-Based Approach to Personal Data Protection

Section 1 briefly introduced several risks to the rights and freedoms of personal data. In everyday life, the terms risk, threat, and danger are usually used interchangeably, meaning the term risk is used in a loose way. The question is: what can be considered a risk that is covered by the law? Making clear this question is a prerequisite to understanding the risk-based approach. Also, since the risk-based approach is introduced to overcome the defects of the right-based approach, it's necessary to first specify the meaning, characteristics, and defects of the right-based approach so that we can better compare the similarities and differences between the two approaches.

2.1. The Meaning of Risk and Its Embodiments in Legislation

The International Organization for Standardization (ISO) provides an internationally agreed understanding of the term risk, which is helpful for understanding this term that is covered by the law. According to 3.1 ISO 31000:2018(en) Risk Management-Guidelines (hereinafter referred to as "ISO Guidelines"), "Risk means the effect of uncertainty on objectives." In the common language, businesses or individuals engage in activities to fulfill certain objectives. In this process, external or internal factors or the combination of both may lead to uncertainty in the fulfillment of the objectives, and risk is the possible positive or negative effect of uncertainty on the objectives (OECD, 2016). It could be deduced from ISO's definition of risk that privacy risk means the possible negative effect of uncertainty on the objective of protecting privacy, and risks to the rights and freedoms of natural persons means the possible negative effect of uncertainty on the objective of protecting the rights and freedoms of natural persons.

In the personal data protection legislation, not all forms of risks are covered by the law. For instance, the EU's GDPR focuses on the risks to the rights and

freedoms of natural persons, the US law focus on privacy risks, and China's Personal Information Protection Law (PIPL) focuses on security risks. Also, the contents of risk covered by law vary in the different legislation. A risk may either be defined in terms of possible negative effects or consequences or be expressed together with risk sources, potential events, or likelihood.[3] In the first case, the Consumer Privacy Bill of Rights Act of 2015 (CPBRA) proposed in the 114th US Congress and the American Data Privacy and Protection Act (ADPPA) proposed in the 117th Congress could serve as two examples. CPBRA explicitly defined privacy risk as the potential to cause emotional distress or physical, financial, professional, or other harm to an individual, and ADPPA defined the term substantial privacy risk in a similar way.[4] In the second case, recital 75 of the GDPR could serve as an example. Recital 75 not only expressed "the risks to the rights and freedoms of natural person" in terms of various possible negative effects (e.g., physical, material, or non-material damage), but also referred to a risk source (i.e., personal data processing activity) and several potential events (e.g., fraud).

To summarize, although ISO's definition of risk has been widely accepted, not all forms of risk are covered by the law, and the forms and contents of risk covered by law vary in the different legislation. Those differences reveal legal, historical, and cultural diversities among countries and regions.

2.2. The Right-Based Approach and Its Embodiments in the Legislation

The prescriptive and right-based approach is the dominating approach adopted by most lawmakers and regulators not only in the public domain of personal data protection but also in many other public domains. However, this approach has inherent defects when addressing risks with different severity and possibility.

2.2.1. The Right-Based Approach to Personal Data Protection

Before analyzing the defects of the right-based approach to manage risks in the domain of personal data protection, we should make clear the meaning of this approach and how it is adopted to protect personal data.

The United Nation's Statement on Human Rights Based Approach (hereinafter referred to as "the Statement") released in 2003 could serve as a starting point and shed some light on the meaning of the right-based approach. In the light of the Statement, rights-holders are the key actors instead of passive recipients in their own development. Accordingly, human rights are mainly realized through empowerment and participation. Meanwhile, enhancing duty-bearers' capacity of performing their obligations is the other side of the coin for right-holders to realize their human rights (UNSDG, 2003). Last but not least, the principles of

[3]Risk source means element which alone or in combination has the potential to give rise to risk. Event means occurrence or change of a particular set of circumstances, and an event can be a risk source. Consequence means outcome of an event affecting objectives. 3.4-3.6 ISO Guidelines.

[4]S.1158, 114th Cong. § 4 (g) (2015). H.R.8152, 117th Cong. § 2 (2022).

accountability[5] and rule of law guiding all of the programming and cooperation are also indivisible components of the right-based approach. That is, when duty-bearers fail to comply with the legal requirements, rights-holders should be entitled to sue duty-bearers for compensation in accordance with rules and procedures provided by law (UNSDG, 2003).

When it comes to the domain of personal data protection, it's not difficult to recognize that early practices such as OECD's Privacy Guidelines 1980[6] and EU's Data Protection Directive 1995, as well as some latest enactments such as GDPR and The California Privacy Rights Act of 2020 (CPRA)[7] all adopted the right-based approach, although data subject's rights, as well as businesses' obligations and responsibilities, may vary to a different extent. Since GDPR's adoption of the right-based approach has great spillover effects worldwide on how personal data could be protected in the era of big data, algorithms, profiling techniques, and free cross-border flows of data, this paper takes GDPR as an example to illustrate this point.

GDPR heavily relies on the right-based approach to protect natural person's fundamental rights and freedoms. To start with, data subjects are assigned a set of rights empowering them to realize such rights as the right of access, right to rectification, right to be forgotten, right to data portability, right to object, and automated individual decision-making.[8] Second, data subjects substantially participate in their personal data protection through a set of rules, among which explicit or implied consent by data subjects is one of the most important legal bases for personal data processing.[9] This is because GDPR follows the logic that data subjects are reasonable people, so if they get more information about data controllers and how their personal data will be collected and processed, they will have a better understanding of the risks and make an informed decision on whether or not to take the risks. In the meantime, even if data subjects have consented to the processing of their personal data, they are still in control of some rights, such as the right of access, right to rectification, and right to erasure. Third, GDPR, through the adoption of a so-called meta-regulation as well as the principle and rules of accountability, shifted the main obligations of protecting personal data from the Member States to data controllers, and entitle data subjects to an effective judicial remedy against controllers (Eduarda Gonçalves, 2020).

2.2.2. Defects of the Right-Based Approach to Risk Management

To start with, the right-based approach is based upon the assumption that indi-

[5]Accountability, as described by international soft laws, requires businesses to be accountable for complying with measures which give effect to other principles of personal data protection. e.g., Article14 Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereinafter Privacy Guidelines 2013), or Article IX APEC Privacy Framework (2015). Accountability in GDPR further requires controllers to demonstrate its compliance with other principles of personal data protection. Article 5.2 GDPR.

[6]OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

[7]The California Privacy Rights Act of 2020, Cal. Civ. Code § 1798.100 etc. (2020).

[8]Chapter III GDPR.

[9]e.g., Articles 6.1(a), 7, 8, 9 GDPR.

viduals are reasonable persons who could make an informed decision. This may be true in some cases. In the domain of personal data protection, however, it's hard for data subjects to understand the professional and tedious notice of how their personal data will be collected and processed. As a response, they may not be willing to spend time reading it but consent without any hesitation, leaving their consent to take the risks problematic. Although it's suggested that this problem could be solved through simplified notice or enhanced education, such solutions are either ineffective or too burdensome and costly for data subjects, businesses, and society (Cate, 2006).

Second, the principle of use limitation and other rules contained in personal data protection law indicate that, when subsequent processing goes beyond the purposes of collection or processing specified earlier on, additional consent is needed to legalize such processing. In circumstances where new techniques such as big data and algorithms are used, subsequent processing of personal data is quite likely to go beyond the existing purposes, so additional consent is needed. However, it's hard to trace the original great amounts of data subjects to re-acquire their consent in those circumstances, meaning that data subjects have lost control of their personal data (Gellert, 2016).

Third, although the right-based approach also aims to manage risks, it manages risks in a universal and inflexible way, so the level of protection it provided may be disproportionate to the risks presented. For instance, when the level of protection provided by law is higher than the risks presented, it will be burdensome for businesses to take high-standard measures to just manage low risks. Similarly, when the level of protection provided by law is lower than the risks presented, data subjects' rights will be derogated if businesses don't voluntarily take additional measures beyond the law to protect personal data.

Fourth, the right-based approach heavily relies on tort law to compensate data subjects' harms or damages, but there are at least two limits to such practices. One limit is that tort law provides a remedy only after data subjects are harmed. For some rights such as privacy, once they are harmed, they cannot be easily filled up. Another limit is that it's hard to quantify certain harms such as reputation to compensate data subjects whose rights are harmed. In these circumstances, the heart of protection lies in minimizing the negative impact of risks ex-ante.

Having considered the inherent defects of the right-based approach to personal data protection, the risk-based approach is introduced to the latest personal data protection law to better manage risks and protect personal data.

3. The Risk-Based Approach to Personal Data Protection

The risk-based approach, partly initiated in Europe's de-regulation campaign in the late twentieth century, has been widely adopted in various policy domains. When it comes to the domain of personal data protection, the terms risk, and the risk-based approach are also increasingly inserted into the relevant legislation, since the right-based approach falls short in managing risks threatening

data subjects' rights. Therefore, Section 3 explores the meaning of the risk-based approach in the domain of personal data protection, how it is embodied in national or regional law, and its advantages.

3.1. The Meaning of the Risk-Based Approach

At present, no personal data protection law has explicitly defined the term the risk-based approach, nor has there been a widely accepted definition of it. Despite that, the existing literature could help shed some light on the meaning and characteristics of this approach, and how this approach is embodied in national or regional law.

In 2014, Article 29 Working Party stated that the risk-based approach used in the Data Protection Directive 1995 and the proposed GDPR was concerned with strengthened obligations in response to risks resulting from personal data processing (Article 29 Data Protection Working Party, 2014). It further clarified that the risk-based approach is "not an alternative to well-established data protection rights and principles, but a scalable and proportionate approach to compliance". Some scholars share similar views with Article 29 Working Party. For instance, Milda Macenaite held that the risk-based regulation focused on "providing a model to achieve proportionate and adaptive strategy for regulatory enforcement" (Macenaite, 2017). Claudia Quelle described the risk-based approach adopted in GDPR as compliance 2.0 which goes beyond the tick-boxes compliance. As she puts it, "Controllers shall perform their obligations in such a way that is tailored to respect individuals' rights and freedom (Quelle, 2018)."

In 2014, the Centre for Information Policy Leadership, after studying various workshops' discussions about the risk-based approach, summarized the main findings about this approach (Centre for Information Policy Leadership, 2014). Since those findings got close to the full picture of the risk-based approach, this paper attempts to take a step further and defines the risk-based approach as a special compliance approach under which the businesses are endowed to calibrate their obligations of protecting personal data in terms of risks of different possibility and severity to enhance compliance with the principles and rules of personal data protection law.

At least three characteristics of the risk-based approach are revealed from this definition. First, endowing businesses to calibrate their obligations in terms of risks is an essential characteristic of this approach, which usually means businesses shall implement measures proportionate to the risks. However, it doesn't matter whether the risk-based approach is adopted to ensure a specific goal (e.g., security of personal data) or a general goal of personal data protection. Obviously, the risk-based approach manages risks in a contextual and flexible manner, differentiating it from the right-based approach which manages risks in a linear and universal manner. Second, the goal of the risk-based approach is to enhance compliance with the law instead of weakening it, demonstrating that this approach is not incompatible with the right-based approach. To be more specific, the risk-based approach is not a replacement but a supplement of the

right-based approach. Third, the risk-based approach reflects the risk prevention principle, because it aims to reduce the risks to an acceptable level before data subjects are harmed, instead of providing a remedy for them ex-post.

At first glance, the term risk-based approach looks similar to the terms risk management, risk regulation, and risk-based regulation. These terms, although look similar and may overlap in meanings and scopes, are different and independent terms.

First, pure risk management refers to risk analysis tools replacing principles of personal data protection which enables controllers to determine the most appropriate safeguards for each processing and to decide whether or not to take the processing at stake (Quelle, 2018). In practice, however, pure risk management is rarely applied. Instead, it's usually inserted into the risk-based or right-based approach and is applied together with the principles and rules of personal data protection to manage risks.

Second, risk regulation refers to governmental interference with market or social processes to control certain risks (Quelle, 2018). Compare to the risk-based approach, controlling risks is the goal of risk regulation, no matter what means is used, while controlling risks is the means of the risk-based approach to achieve the goal of personal data protection.

Third, risk-based regulation refers to a strategy employed by government agencies tasked with oversight and enforcement to score the risks posed by an organization's activities (e.g., data processing) to target enforcement action on the most problematic areas (Quelle, 2018). Compare to the risk-based approach, the risk-based regulation is narrower in scope because it is adopted by regulators, while the risk-based approach could be applied to businesses. When the risk-based approach is applied to businesses, it could be called the risk-based compliance.

3.2. The Risk-Based Approach in the National/Regional Legislation

In order to get the whole picture of the risk-based approach adopted by national and regional data protection law, we should not only focus on provisions embodying this approach but also understand it in context, which means that other explicit requirements (e.g., compulsory obligations or exemptions) contained in law should also be taken into account. Therefore, Section 3.2 explores whether the EU, US, and China have adopted the risk-based approach in their personal data protection law and if so, what Articles embodied this approach.

3.2.1. EU Data Protection Directive 1995 and GDPR

The Data Protection Directive 1995, the predecessor of GDPR, is one of the earliest enactments that embodied the risk-based approach to personal data protection. Article 17, by prescribing that the technical and organizational measures implemented by controllers to protect personal data must ensure a level of security appropriate to the risks represented by the processing and the nature of the

data to be protected, endowed controllers with discretions to calibrate their obligation in terms of risks. Also, having considered that additional measures or exemptions are needed to respond to risks of specific possibility and severity, Article 20 required the Member states, after receiving the notification from controllers, to prior check data processing operations when there are specific risks to the rights and freedoms of data subjects, and Article 13 exempted the Member States from guaranteeing data subjects' right of access if there is no privacy risk to data subjects.

GDPR further enhances the risk-based approach in three aspects. First, Article 24, by requiring controllers to implement appropriate technical and organizational measures to ensure that processing is performed in accordance with GDPR, systematically expands the controller's discretion of calibrating their obligations in terms of risks from ensuring personal data security to ensuring compliance with GPDR (Macenaite, 2017). Also, Article 25 requires controllers, after taking into account the risks and other factors, to implement appropriate measures by design and by default to achieve compliance with the GDPR. Second, GDPR initiates more obligations related to risks for controllers to perform, improving the legal certainty of the risk-based approach in certain circumstances. For instance, Articles 34.1, 35, and 36 require controllers to take additional measures when there are high risks, and Articles 27, 30, 33, and 34 exempted controllers from taking certain measures when risks are low, or high risk is no longer likely to materialize. Third, compared to the Data Protection Directive 1995 which heavily relied on the Member States to protect data subjects' rights and freedoms, GDPR shifts this obligation to controllers who are considered to be more capable of and experienced in managing risks (Eduarda Gonçalves, 2020).

It's worth noting that, Article 17 of the Data Protection Directive 1995 as well as Articles 24 and 25 of GDPR are characterized as meta-regulation or meta-regulatory approach, under which the technical and organizational measures required to protect the rights and freedoms of data subjects are quite extensive, far beyond the explicit requirements prescribed in the GPDR. In other words, controllers may implement supplemental measures going beyond the GDPR to protect personal data if GDPR falls short in managing risks (Quelle, 2018). For instance, when processing is likely to lead to high risks, and additional obligations explicitly required by Article 35 of the GDPR is not enough to protect the rights and freedoms of data subjects, controllers should, in line with Article 24 and 25, implement additional measures that are proportionate to the risks. However, controllers are not allowed by GDPR to use the risk-based approach to derogate data subjects' rights in any circumstances.

3.2.2. The US Privacy Law and Proposed Legislation

In the US, personal data is protected mainly through the consumer's privacy rights approach for a long time. Since there is at present no overarching statute on consumer's online privacy rights protection at the federal level, most personal

data in the commercial field are protected mainly through self-regulation of businesses, unless it is special personal data that falls into the scope of sectoral statutes (EPIC, 2023). Meanwhile, The Federal Trade Commission (FTC) plays an important role in protecting the consumer's privacy rights. The FTC's mandates include the power to enforce certain federal laws and issue rules under the law, and the power to prohibit unfair and deceptive activities (EPIC, 2021). In addition, when a business's data processing activities breach consumers' online privacy, consumers' privacy rights can be remedied through common law.

The US is facing a data privacy crisis in the last decades. Data privacy scandals of large and powerful companies such as Facebook incurred many criticisms of the US approach to personal data protection. It's argued that since the US approach to personal data protection is sector-specific which only covers a few types of data and uses of data, many other types of data are not protected by law at all. Also, businesses that are not prohibited from taking the self-regulatory approach to personal data protection in the commercial field, in the absence of legal obligations and responsibility, fail to protect personal data as they asserted. Further, FTC's power to privacy regulation is restricted by law, and it provides remedies after consumers are harmed by unfair and deceptive practices (EPIC, 2022).

A few states took the lead in reforming privacy laws and have enacted their state-level comprehensive privacy acts in recent years, among which California, Virginia, and Colorado are the earliest states. To date, twenty-three states have enacted or introduced state-level general privacy bills, although some of them are not active yet (Lively, 2022). At the federal level, continuous efforts are made to pass a comprehensive privacy bill, and dozens of privacy-related bills are proposed through the halls of Congress (Fazlioglu, 2022). Pertaining to the bills proposed in 117th Congress, the bipartisan-sponsored bill ADPPA, which is moved to the House of Representatives in August 2022 for the vote for the first time, has many wondering if it will make the federal comprehensive privacy act into reality.

An overview of the US privacy law and proposed legislation demonstrates that the risk-based approach has not yet been widely and fully adopted by law. For instance, while Colorado Privacy Act is one of the few state-level comprehensive privacy bills that adopt the risk-based approach, it limits this approach to ensuring the security of personal data instead of ensuring compliance with wider obligations through meta-regulation.[10] It is until the proposed ADPAA that the risk-based approach with a general goal of personal data protection may be adopted by the US privacy laws.

As prescribed by section 103(a)(4) of ADPPA, a covered entity and a service provider shall establish, implement, and maintain reasonable policies, practices, and procedures that implement reasonable training and safeguards to promote compliance with all privacy laws applicable to covered data they collect, process, or transfer and mitigate privacy risks ("privacy by design"). And section

[10]Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1305 (2021).

208(a)(1) requires a covered entity or service provider to establish, implement and maintain reasonable administrative, technical, and physical data security practices and procedures to protect the covered data against unauthorized access and acquisition ("data security and protection of covered data"). Although the two sections don't clearly require the covered entity to calibrate the obligations in terms of privacy risks, it implies this requirement if we keep reading the next subsections. Also, sections 103(b) and 208(a)(2) provide that, the aforesaid obligations shall correspond with or be appropriate to certain factors relating to the covered entity or service provider and activities engaged by it, covered data, and individuals related to covered data. These factors to be considered undoubtedly reflect risks of different severity and possibility thus implying the insertion of the risk-based approach. Also, in order to improve the legal certainty of the risk-based approach under certain circumstances, ADPAA proposed additional requirements for a covered entity or service provider to comply with when there may be high privacy risks, such as specific requirements for data security and privacy impact assessments for large data holders.[11]

What calls for special attention is that ADPAA proposes that the covered entity or service provider shall take into account the cost of implementing requirements of privacy by design and data security in relation to the risks and nature of the covered data.[12] It suggests that when the cost of implementing the aforesaid requirements outweighs the benefits of data protection, the covered entity or service provider may be allowed to deviate from those requirements. This reflects a substantial difference between the US and EU personal data protection legislation: personal data protection is a fundamental right in the EU, so controllers are not allowed derogate data subject's rights, even if they are endowed to calibrate obligations in terms of risks; personal data protection is consumer's privacy right in the US, so businesses may be allowed to derogate consumer's privacy right if the cost of personal data protection in relation to risks outweighs the benefit of personal data protection and the overall welfare to the society.

3.2.3. China's Personal Information Protection Law

After several years of discussion, China's Civil Code and the omnibus Personal Information Protection Law (PIPL) both entered into force in 2021, under which personal information is deemed as personality rights and interests and is protected through private and public law approaches. PIPL is comprised of eight chapters, including general and special rules on different types of personal information processing, rules on providing personal data across borders, individuals' rights and processors' obligations in personal information processing activities, departments with personal information protection duties, legal liability, and other provisions.

Among seventy-four Articles in PIPL, only Articles 51 and 64 explicitly mention the term risk, and Article 51 constitutes a general provision of the risk-based ap-

[11]H.R.8152, 117th Cong. § 207(c), 208(b), 301(c) (2022).
[12]H.R.8152, 117th Cong. § 103(b)(5), § 208(a)(2)(F) (2022).

proach to personal data protection. In terms of the preamble of Article 51, personal information processors shall take measures to ensure that their personal information processing activities are in compliance with laws and administrative regulations based on the purpose and means of processing, the categories of personal information to be processed, the impact on personal rights and interests, and the potential security risks, among others, and shall prevent unauthorized access to, as well as breach, tampering or loss of any personal information. And paragraphs (1) to (6) list six types of measures for processors to comply with, including formulating an internal management system and operational procedures. Article 64 requires departments with personal information protection duties, when it finds relatively high risks in personal information processing activities, to hold interviews with processors or to request them to entrust a professional institution to conduct compliance audits of the personal information processing activities.

Chapter three of the PIPL together with other relevant provisions contained in Cybersecurity Law (CSL) and Data Security Law (DSL) are shaping China's layered approach to regulating risks from the cross-border flows of personal data. First, data localization measures apply to specific personal information and fields (e.g., financial information and government procurement), Online platform operators holding the personal information of more than 1 million users and newly listing on foreign markets, processors who process certain amount of personal information, and critical information infrastructure (CII) operators. If it's necessary to provide the foresaid personal information outside the mainland of the P.R.C, security assessment, cybersecurity review or other requirements prescribed by law shall be followed.[13] Second, for other personal information or personal information processors that do not fall within the above circumstances, the conditions for exporting personal information are similar to GDPR, that is, to obtain personal information protection certification or to conclude a contract with a overseas recipient in accordance with the standard contract formulated by the national cyberspace department.[14]

3.3. Advantages of the Risk-Based Approach

With respect to the meaning and characteristics of the risk-based approach and in combination with its embodiments in national or regional personal data protection legislation, at least three categories of advantages could be deduced from the perspectives of businesses and data subjects.

3.3.1. Advantages for Data Subjects

It's important to note that, the accountability principle does not replace other substantive data protection principles but aims to make them work better

[13]e.g., Articles 38, 40 of PIPL; Article 37 of CSL; Article 7 of Cybersecurity Review Measures of 2022.

[14]Article 38 of PIPL. It should be pointed out that regardless of the rules on exporting personal information stipulated by laws and regulations, personal information processors should inform data subjects of exporting their personal information overseas and obtain their separate consent, unless otherwise stipulated by laws and regulations.

(Quelle, 2018). Therefore, approaches to personal data protection are critical for the fulfillment of accountability and personal data protection. While the right-based approach stipulates business's compliance obligations in a universal and inflexible way, which may easily lead to tick-box compliance and thus make accountability and personal data protection meaningless, the risk-based approach endows businesses to calibrate their obligations in terms of different risks even if additional risk management requirements are not prescribed by law, which could better protect data subject's rights.

In particular, the risk-based approach could help address accountability problems in areas where new technologies such as profiling, big data, and algorithms are used and the prescriptive and right-based approach does not work (Macenaite, 2017). This is because, since laws usually lag behind technologies and practice, there may be grey areas where the legislation doesn't explicitly impose in advance certain compliance obligations on businesses, undermining the efficiency of personal data protection. Under the risk-based approach, however, businesses always need to be responsible for ensuring and demonstrating compliance with the law. Therefore, accountability is enhanced and personal data could be better protected.

3.3.2. Advantages for Businesses

By endowing businesses to calibrate their obligations in terms of different risks under different contexts, businesses are able to allocate more resources to address risks with higher possibility and severity, and fewer resources to address risks of lower possibility and severity. It could greatly reduce their burden of compliance obligations while increasing their risk management efficiency (Centre for Information Policy Leadership, 2014). Also, the risk-based approach could be served as a legal basis for reducing a business's administrative or civil responsibilities that cause harm or damage to the data subject's rights, if they have properly performed the risk-based compliance obligations. This does not contradict the idea that the risk-based approach cannot be used to derogate data subjects' rights.

4. The Response of the International Trade Law to the Risk-Based Approach

A few international soft laws such as Article 15 of the OECD's Privacy Guidelines 2013 suggest having in place a privacy management programme embodying the risk-based approach to enhance privacy protection. And regional trade agreements entered into force recently such as USMCA, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), and the Regional Comprehensive Economic Partnership (RCEP) set the rules of personal data protection which require parties to adopt or maintain a legal framework to protect users' personal data. Among these agreements, USMCA and the US-Japan Digital Trade Agreement embody the implied adoption of the risk-based approach in their rules of personal data protection. Also, since cybersecurity issues

and privacy issues are overlapping in ensuring the security of personal data, and the rules of cybersecurity contained in these two agreements explicitly encourage contracting parties and their enterprises to employ the risk-based approach to identify and protect against cybersecurity risks, the two agreements explicitly adopt the risk-based approach to protect the security of personal data. In addition, some WTO members proposed the risk-based approach to personal data protection at the JSI on e-commerce, indicating the potential of this approach to be widely adopted at the plurilateral level. Section 4 first explores the risk-based approach in the context of international trade law and then discusses the "necessity and proportionate" test inherently contained in the risk-based approach.

4.1. The Risk-Based Approach under International Trade Law

Since USMCA and the US-Japan Digital Trade Agreement share similar provisions on the risk-based approach, this paper takes the relevant provisions in USMCA as examples to explain the adoption of the risk-based approach under regional trade agreements.

4.1.1. Implied Adoption of the Risk-Based Approach in the Rules of Personal Data Protection

USMCA, which entered into force in July 2020, is a substitute for the North America Free Trade Agreement (NAFTA). The structures and contents of the USMCA are quite similar to CPTPP except for a few numbers of articles such as articles on personal information protection.

Paragraph 3 of USMCA Article 19.8 Personal Data Protection reads:

The Parties also recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented.

The phrase "ensuring compliance with measures to protect personal information" indicates that USMCA does not mean to interfere with contracting parties' personal data protection regimes. And the phrase "ensuring any restriction… are 'necessary and proportionate' to the risks presented" has two-fold meanings: 1) the contracting parties are encouraged to calibrate their restriction on cross-border flows of personal data in terms of the risks presented; and 2) the restriction should be "necessary and proportionate" to the risks presented. Although this phrase doesn't explicitly mention the risk-based approach, it in fact encourages contracting parties to apply this approach to protect personal data, because this voluntary obligation is consistent with the essential characteristic of the risk-based approach. This point is also in line with OECD's view in an early explanatory document (OECD, 2013). Compared to the risk-based approach in the national and regional personal data protection practices, however, the risk-based approach in this provision is limited to the domain of cross-border personal data flows.

4.1.2. Explicit Adoption of the Risk-Based Approach in the Rules of Cybersecurity

Paragraph 2 of USMCA Article 19.15 Cybersecurity reads:

Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.

This provision explicitly encourages contracting parties and their enterprises to employ the risk-based approach to protect against cybersecurity risks. Although cybersecurity and personal data protection are two different issues, they are overlapping in protecting the security of personal data: cybersecurity refers to "a measure for protecting computer systems, networks, and information from disruption or unauthorized access, use, disclosure, modification or destruction" (Wylde et al., 2022). and protecting individuals' personal data from unauthorized access, use, disclosure, modification or destruction is also an indispensable part of personal data protection. As Christopher Kuner et al. put it, "privacy depends absolutely on security, as a result, all modern data protection principles include an obligation to protect security (Kuner et al., 2017)." Therefore, it's safe to conclude that USMCA also encourages the adoption of the risk-based approach to protecting the (cyber)security of personal data. In other words, contracting parties are not encouraged to take measures that are unnecessary and disproportionate to risks to the (cyber)security of personal data.

4.1.3. Proposals on the Risk-Based Approach at the JSI on E-Commerce

A like-minded group of WTO members issued joint statements on advancing discussions on e-commerce and other three topics at the 11th Ministerial Conference in 2017. As regards the JSI on e-commerce, participants have submitted several versions of textual proposals for discussing six main themes: enabling electronic commerce, openness and electronic commerce, trust and digital trade, cross-cutting issues, telecommunications, and market access. According to the updated consolidated negotiating text, the risk-based approach is also embodied in proposals relating to personal data protection and cybersecurity.

In paragraph 3 of the proposals titled "Personal information protection/Personal data protection", the US proposed that:

The [Parties/Members] recognise the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented (WTO, 2021).

In paragraph 3 of the proposal titled "Cybersecurity", the US and the UK proposed that:

Given the evolving nature of cybersecurity threats, the [Parties/Members]

recognise that risk-based approaches may be more effective than prescriptive [regulation/approaches] in addressing those threats. Accordingly, each [Parties/Members] shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on [open and transparent industry/consensus-based] standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.

If we compare the two proposals carefully with their counterparts in USMCA, we'll find most of the contents remain the same except for one substantial difference: the risk-based approach in Article 19.15 of USMCA refers to the approach that relies on consensus-based standards and risk management best practices, while the risk-based approach proposed under the JSI on e-commerce is a less strict one because it relies on open and transparent industry standards and risk management best practices (WTO, 2021).

4.2. The Mysterious and Complicated "Necessary and Proportionate" Test

As mentioned above, the risk-based approach has been inserted into the rules of personal data protection and cybersecurity under some of the international trade agreements and has the potential to be widely adopted at the plurilateral level in the future. A contracting party of the foresaid agreements is encouraged to comply with the following obligations: any restriction to the cross-border flows of personal data taken to ensure compliance with measures to protect personal data is "necessary and proportionate" to the risks presented. Although those obligations are voluntary, contracting parties are suggested to consider whether and how to insert the risk-based approach into their personal data protection regimes so as to make them work more efficiently. In practice, since a data localization measure is faced with doubts about its efficiency and necessity in protecting personal data, this paper takes this measure as an example to discuss whether it is "necessary and proportionate" to the risks.

4.2.1. The Meaning of the "Necessary and Proportionate" Test

Under constitutional and administrative law, the "necessary and proportionate" test is composed of two elements of the principle of proportionality. The principle of proportionality is basically comprised of three principles: adequacy, necessity, and proportionate *stricto sensu*. Adequacy focuses on whether there is a rational connection between the measure and the aim pursued. Necessity means among all of the measures that could equally achieve or contribute to the achievement of the aim pursued, only the least restrictive measure is necessary. Proportionate *stricto sensu* (also referred to as balancing principle) means the benefits gained through fulfilling the aim should be proportionate to the harm to the human rights of others or public interests. Compared to the necessity principle which focuses on how to minimize harms caused by the means to the rights, proportionate *stricto sensu* focuses on whether it is necessary to achieve

the aim through the least restrictive means so as to protect rights and enhance overall social welfare (Barak, 2012).

The principle of proportionality in constitutional and administrative law serves as an important reference for interpreting the necessity test and proportionate test in international trade law. For instance, the WTO dispute settlement body's interpretation of the necessity test contained in Article XX GATT, Article XIV GATS, and Article 2.2 TBT manifest that the necessity test in international trade law also focuses on whether there is a reasonably available measure that could equally achieve the goal pursued but is less restrictive to international trade.[15] However, the rules of personal data protection under international trade agreements don't require the measures chosen to be necessary to achieve the goal pursued but require any restrictions on cross-border flows of personal data to be necessary to the risks presented. Therefore, the necessity test herein should be interpreted as focusing on whether there is a reasonably available measure that could equally manage risks as the measure in question, but is less restrictive to the cross-border flow of personal data. If the answer is yes, the measure in question is unnecessary, and vice versa.

As regards the proportionate test, similar to the proportionate *stricto sensu in* constitutional and administrative law, the proportionate test herein focuses on whether the harms cased by the restriction on the cross-border flows of personal data is proportionate to the benefits gained from it.

4.2.2. Whether the Restriction Caused by a Data Localization Measure Is "Necessary and Proportionate" to Risks

The nature of the risk-based approach shows that a measure implemented in accordance with this approach (e.g., Article 24 GDPR) is quite possible to be "necessary and proportionate" to the risks presented. This brings us to a question: whether a data localization measure implemented to protect the security or privacy of personal data will always be unnecessary or disproportionate to risks?

This paper establishes a theoretical model, **Figure 1**, to answer this question. In **Figure 1**, line 1 means that the restriction caused by the measure embodying the risk-based approach is always "necessary and proportionate" to the risks, and line 2 means that a data localization measure causes a universal level of restriction, regardless of risks of different severity. Line section A means as regards the same low risk, the restriction caused by a data localization measure is higher than the measure embodying the risk-based approach and thus is unnecessary and disproportionate to risks. Line section B means as regards the same high risk, although the restriction caused by a data localization measure is lower than the measure embodying the risk-based approach, it's less efficient in

[15]See e.g. Australia-Certain Measures Concerning Trademarks, Geographical Indications and Other Plain Packaging Requirements Applicable to Tobacco Products and Packaging, Appellate Body Report, WT/DS435/AB/R, WT/DS441/AB/R, 9 June 2020; European Communities-Measures Prohibiting the Importation and Marketing of Seal Products, Appellate Body Report, WT/DS400/AB/R, WT/DS401/AB/R, 22 May 2014; China-Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products, Appellate Body Report, WT/DS363/AB/R, 21 Dec. 2009.

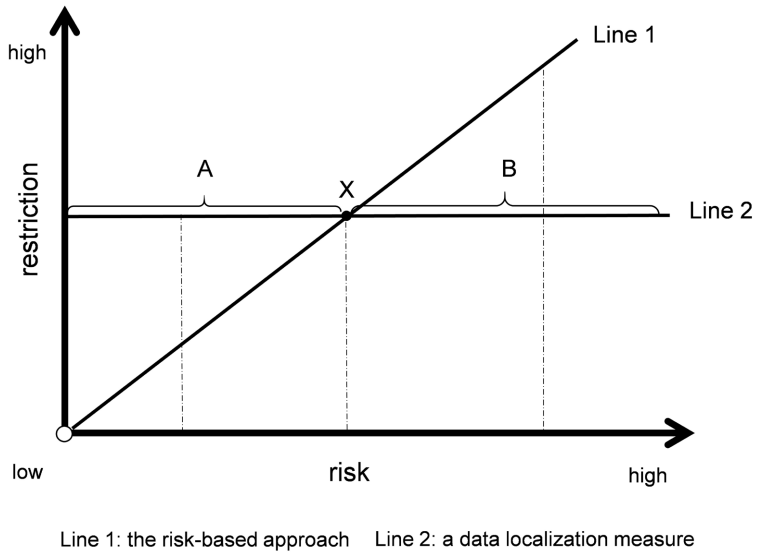

Figure 1. Relationships between Approaches, Risk, and Restriction. Source: the author self-organized.

managing risks and thus is not necessary or proportionate to risks. Point X means as regards a specific risk, the data localization and the measure embodying the risk-based approach can equally manage the same risk and cause the same level of restriction, and thus the data localization measure is necessary and proportionate to the risks. In summary, a data localization measure, although much more restrictive than other measures, may be necessary and proportionate to risks.

And then how do the adjudicators decide whether a data localization measure is necessary and proportionate to the risks? A risk management tool may be introduced to address this problem. In fact, risk management is not only an important part of the risk-based approach, it could also be used to assess the efficiency and necessity of any measure implemented to protect personal data. However, since different risk management tools may lead to different conclusions, risk management tools, standards, and best practices that are more widely accepted and applied shall be used by adjudicators to determine the necessity and proportionality of the measure in question. Therefore, the existing international standards on risk management such as ISO Guidelines shall be taken into account. Also, countries could cooperate together to foster more widely accepted risk management standards and best practices to improve the certainty of the "necessary and proportionate" test.

5. Concluding Remarks

In the public domain of personal data protection, although the prescriptive and right-based approach is necessary for establishing a certain level of protection for data subjects that cannot be undermined, some inherent defects of this approach make its risk management inefficient and thus decrease the efficiency of personal data protection. In order to better manage risks, various risk-related

tools such as risk management, privacy or data protection impact assessment, risk regulation, and risk-based regulation have been employed to protect personal data. Although these tools look similar to the risk-based approach, they are concepts with different meanings and functions. The risk-based approach, without replacing the existing right-based approach, works as a supplement that endows businesses to calibrate their obligations of personal data protection in terms of different risks, so as to improve the efficiency of risk management and to enhance compliance with the principles and rules of personal data protection law.

At the national and regional levels, the risk-based approach is increasingly being introduced into the legislation, although the coverage of this approach may range from protecting the security of personal data to more general personal data protection. Also, different nature of personal data protection leads to different approaches to and level of it: since the EU treats personal data protection as a fundamental right, businesses are not allowed derogate data subject's rights in any case; since the US treats personal data protection mainly as consumer's privacy right, businesses may be allowed to derogate such a right if the cost of personal data protection in relation to risks outweighs the benefit of personal data protection and the overall welfare to the society; since China treats personal data protection as personality rights and interests, it protects personal data through private and public law approaches.

At the international level, the risk-based approach has been inserted into some of the international soft laws and regional trade agreements and has the potential to be widely employed at the plurilateral level in the future. This paper finds that it's hard, if not impossible, for a data localization measure to pass the "necessity and proportionate" test that is inherently contained in the risk-based approach. However, since this test is a soft obligation, it would not pose substantial challenges to contracting parties' existing personal data protection regimes. Nonetheless, it gives contracting parties an opportunity to reconsider the necessity and proportionality of a data localization measure and relevant measures in managing risks and thus makes their personal data protection law work better.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Article 29 Data Protection Working Party (2014). *Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks (14/EN WP 218)* (p. 2).

Barak, A. (2012). *Proportionality: Constitutional Rights and Their Limitations* (p. 356). Cambridge University Press. https://doi.org/10.1017/CBO9781139035293

Casalini, F., & López González, J. (2019). *Trade and Cross-Border Data Flows* (p. 8). OECD Trade Policy Papers No. 220.

Cate, F. H. (2006). The Failure of Fair Information Practice Principles. In K. J. Winn (Ed.), *Consumer Protection in the Age of the "Information Economy"* (pp. 343-375). Routledge.

Centre for Information Policy Leadership (2014). *A Risk-Based Approach to Privacy: Improving Effectiveness in Practice*. https://www.huntonak.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf

Eduarda Gonçalves, M. (2020). The Risk-Based Approach under the New EU Data Protection Regulation: A Critical Perspective. *Journal of Risk Research, 23,* 140-143. https://doi.org/10.1080/13669877.2018.1517381

EPIC (2021). *What the FTC Could Be Doing (But Isn't) to Protect Privacy—The FTC'S Unused Authorities*. https://epic.org/wp-content/uploads/2021/10/EPIC-FTC-Unused-Authorities-Report-June2021.pdf

EPIC (2022). *Hearing on Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors*. https://epic.org/documents/hearing-on-big-data-privacy-risks-and-needed-reforms-in-the-public-and-private-sectors

EPIC (2023). *The US Sector-Specific Federal Privacy Laws*. https://epic.org/issues/privacy-laws/united-states

Fazlioglu, M. (2022). *US Federal Privacy Legislation Tracker*. https://iapp.org/resources/article/us-federal-privacy-legislation-tracker

Gellert, R. (2016). We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection. *European Data Protection Law Review, 2,* 481-492. https://doi.org/10.21552/EDPL/2016/4/7

Kuner, C. et al. (2017). The Rise of Cybersecurity and Its Impact on Data Protection. *International Data Privacy Law, 7,* 73-75. https://doi.org/10.1093/idpl/ipx009

Lively, K. T. (2022). *US State Privacy Legislation Tracker*. https://iapp.org/resources/article/us-state-privacy-legislation-tracker

López González, J., & Jouanjean, M. (2017). *Digital Trade: Developing a Framework for Analysis* (p. 10). OECD Trade Policy Papers No. 205.

Macenaite, M. (2017). The Riskification of European Data Protection Law through a Two-Fold Shift. *European Journal of Risk Regulation, 8,* 512-524. https://doi.org/10.1017/err.2017.40

OECD (2013). *Supplementary Explanatory Memorandum to the Revised Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

OECD (2016). *Managing Digital Security and Privacy Risk* (pp. 7-17). OECD Digital Economy Papers No. 254.

Quelle, C. (2018). Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach. *European Journal of Risk Regulation, 9,* 506-507. https://doi.org/10.1017/err.2018.47

UNSDG (2003). *Human Rights Based Approach to Development Cooperation towards a Common Understanding among UN Agencies*. https://unsdg.un.org/resources/human-rights-based-approach-development-cooperation-towards-common-understanding-among-un

WTO (2021). *Electronic Commerce Negotiations Updated Consolidated Negotiating Text-September 2021* (INF/ECOM/62/Rev.2).

Wylde, V. et al. (2022). Cybersecurity, Data Privacy and Blockchain: A Review. *SN Computer Science, 3,* 127. https://doi.org/10.1007/s42979-022-01020-4