Open Journal of Legal Science 法学, 2024, 12(5), 3297-3304
Published Online May 2024 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2024.125468

Hans汉斯

我国个人数据出境法律规制的优化进路研究

刘珂颖[1]，李新航[2]

[1]郑州大学法学院，河南 郑州
[2]郑州大学国际学院，河南 郑州

收稿日期：2024年3月28日；录用日期：2024年4月19日；发布日期：2024年5月31日

摘 要

构建统一和完备的个人数据出境法律规制体系对于维护我国国家安全和数字安全、深入参与国际数字贸易合作具有举足轻重的意义。我国在立法层面初步形成了个人数据出境监管规则框架，但规范体系分散，具体监管规则细化程度较低，导致司法实践偏离立法旨意。本文基于比较法的视域，借鉴欧盟及美国成熟的规制模式经验，对现有个人数据出境监管路径提供优化建议。我国应推动构建统一的个人数据出境规则体系，细化和健全具体监管规则，设立专门数据监管机构，并加强企业合规性指导，为数字经济有序发展提供坚实的制度支撑。

关键词

个人数据出境监管，数据跨境，数据安全，数据合规

Research on the Optimization Approach of the Legal Regulation of China's Personal Data Export

Keying Liu[1], Xinhang Li[2]

[1]Law School, Zhengzhou University, Zhengzhou Henan
[2]International College, Zhengzhou University, Zhengzhou Henan

Received: Mar. 28th, 2024; accepted: Apr. 19th, 2024; published: May 31st, 2024

Abstract

Building a unified and comprehensive legal regulatory system for the cross-border transfer of

文章引用: 刘珂颖, 李新航. 我国个人数据出境法律规制的优化进路研究[J]. 法学, 2024, 12(5): 3297-3304.
DOI: 10.12677/ojls.2024.125468

personal data is of paramount importance in safeguarding our national security, digital security, and deepening participation in international digital trade cooperation. While China has preliminarily established a framework for regulating the cross-border transfer of personal data at the legislative level, the regulatory system remains decentralized, with low levels of specificity in the detailed regulatory rules, leading to deviations from legislative intent in judicial practice. This paper, from the perspective of comparative law, draws on the mature regulatory models of the European Union and the United States to provide optimization suggestions for the existing regulatory pathways for the cross-border transfer of personal data. China should promote the establishment of a unified system of rules governing the cross-border transfer of personal data, refine and strengthen specific regulatory rules, establish specialized data regulatory agencies, and enhance guidance on corporate compliance, thereby providing solid institutional support for the orderly development of the digital economy.

Keywords

Personal Data Exit Supervision, Cross-Border Data, Data Security, Data Compliance

1. 个人数据出境的基本内涵

1.1. 个人数据的概念及分类

1.1.1. 个人数据与个人信息

“数据”是指描述事物特征、属性或关系的事实或信息的符号表示，通常以数字、文字、图形等形式存在，以便存储、处理和传输。在数字经济时代，数据活动已经超越商品、服务、资本等传统生产要素，成为驱动数字贸易发展的新型驱动力[1]。

在信息网络时代，个人数据具有区分与识别自然人的特定功能，与每个个体紧密联系。国际上对于“个人数据”这一概念没有统一的表述，根据法域、场合不同，涵盖个人信息、个人隐私等多种表达。欧盟在《通用数据保护条例》(以下简称“GDPR”)中对“个人数据”的定义予以延续，并进一步阐述了何为“可识别的自然人”。[1] 我国《网络安全法》第七十六条第五款中采用了“个人信息”的概念，将其定义为能够单独或与其他信息结合识别个人身份的信息。[2] 鉴于二者概念在立法层面之同一的指向性，本文不再对其作区分，并统一使用“个人数据”之表述。

1.1.2. 个人数据的分类

基于不同的标准，个人数据的分类也不尽相同。根据个人数据所体现的社会功能不同，可以将个人数据分为身份数据、健康数据、位置数据、生物特征数据、社会特征数据等；依据个人数据控制主体不同，可以将其分为企业控制的个人数据、政府专职部门控制的个人数据、社会成员控制的个人数据[2]。根据数据对国家安全的影响程度不同，我国《网络安全管理条例(征求意见稿)》将个人数据划分为一般数据、重要数据与核心数据，而《个人信息保护法》则采取了敏感个人信息和非敏感个人信息的划分方式。除此之外，还有动态个人数据和静态个人数据、原始个人数据和衍生个人数据等多种区分类别[3]。

[1]EU. General Data Protection Regulation, 2018, Article 4(1).
[2]《中华人民共和国网络安全法》第七十六条第五款。

1.2. 个人数据出境的概念

就严格厘清个人数据出境之内涵而言，其应属于个人数据跨境流动之子集，而其相对应的概念是个人数据入境。目前部分国家在立法中虽使用数据跨境流动之定义，实际上却仅规制数据出境的行为。国际上对个人数据出境的概念的界定有所区别。经济合作与发展组织(OECD)是最初提出“个人数据出境”这一概念的国际组织。OECD 认为，个人数据出境是指点对点的跨越国家、政治疆域的个人数据传输[4]。1980 年 OECD 正式提出个人数据出境是指个人数据在不同国家之间的自由流动。澳大利亚则认为个人数据无需转移，若由境外访问则可视为出境[5]。集合《信息安全技术数据出境安全评估指南(征求意见稿)》以及《个人信息和重要数据出境安全评估办法(征求意见稿)》，我国已基本明确了“个人数据出境”之概念，即“在中华人民共和国境内收集和产生的电子形式的个人信息和重要数据，提供给境外机构、组织、个人的一次性活动或连续性活动”[3]，并区分两类个人数据出境之情形，即个人数据向境外转移和境外主体访问国内存储的数据[6]。可见我国已从立法上明确了个人数据出境之范围，为个人数据出境监管提供了基本依据。

1.3. 个人数据的权利属性

界定个人数据的权利属性是构建个人数据出境监管体系、推进数字经济蓬勃发展的重要前提。个人数据是一项复合型权利。一方面，个人数据属于人格权的范畴。由前述可知，个人数据区别于非个人数据的关键在于其主体内容与人身密不可分，具有区分个人身份信息的特定功能，这也体现在人格特征的方面[7]。另一方面，个人数据具有财产权的属性。随着信息社会的发展，个人数据可以由个体所支配、使用，也可以被授权实现其金钱价值，从而具有财产权的性质[8]。

2. 我国个人数据出境治理现状

2.1. 个人数据出境的实践现状：以滴滴下架案为例

2016 年，滴滴全球股份有限公司(以下简称滴滴公司)于美国上市。2021 年，国家信息网络安全审查办公室对滴滴公司进行安全审查，发现滴滴公司存在未经用户允许收集客户的个人信息等 16 项违法行为，并对滴滴公司处以罚款。“滴滴出行”的用户以中国用户居多，如未能将这些个人信息恰当处理，造成信息泄露，我国的数据主权及至整体国家安全将面临严重的威胁。但是，与保护出境的个人数据安全的迫切现状相不对称的是我国仅在《个人信息保护法》中规定了信息处理主体务必采取措施保护个人信息在出境过程中的安全。

2.2. 个人数据出境立法概况

在个人数据出境立法领域，我国相对来说起步的时间较晚，但近几年呈现出拔节生长的态势。总体而言，我国通过《网络安全法》《数据安全法》和《个人信息保护法》奠定个人数据出境规则整体基调，形成了以数据出境安全评估制度为核心、以维护数据安全为目标的个人数据出境监管规则框架。

2.2.1. 《网络安全法》

2017 年颁布的《网络安全法》是规范个人数据出境问题的基础性法律文件，为从事个人数据出境业务的网络公司提供合规方向。《网络安全法》作为上位法，指引《个人信息和重要数据出境安全评估办法》(以下简称《办法》)的施行。《办法》将安全评估作为重要内容，详细规定了从适用范围到申报评估的全流程，明确了我国对待个人数据出境采取“境内部署 + 安全评估”的模式，表明了我国致力于预先化解个人数据出境过程中可能存在的安全风险的态度。

[3]《信息安全技术数据出境安全评估指南(草案)》第 3.6 条。

2.2.2. 《数据安全法》

2021 年开始实施的《数据安全法》明确了“数据”“数据安全”“数据治理”等重要概念，确定了“坚持安全与发展并重”的基本原则，规定了国家对于个人数据采取分级处理的措施。由此可见，《数据安全法》是一部立足于《网络安全法》的基础之上，对其中有关个人数据出境问题的规定进行了补充与完善，更加细致地着眼于符合当前我国数字化发展现状的个人数据安全治理的法律文件。虽然这一法律文件已搭建起我国数据治理的体系框架，但是仍需对其分支部分进行细化。

2.2.3. 《个人信息保护法》

《个人信息保护法》紧随《数据安全法》之后实施，着眼于保障个人信息权益和推动数字经济健康发展，与《数据安全法》的基本原则相呼应，充分结合我国国情，对个人数据流动问题作出了更为详细具体的规定。例如，对敏感和非敏感信息进行了区分，并对二者采取分类处理；效仿欧美的成熟做法，提出“单独同意”制度，以及提出再次告知的义务。《个人信息保护法》的出台，使得数据安全治理体系愈加趋近于周密，促进我国个人数据安全治理迈上新台阶。

2.3. 我国个人数据出境监管规则基本内容

2.3.1. 数据本地化原则

基于国家安全和个人隐私保护的考量，我国制定了数据本地化存储规则，要求数据服务器位于本国境内，即本国数据应存储于境内。我国《网络安全法》第三十一条规定了数据本地化的情形，即关键设施基础设施的运营者收集的数据一般应存储在境内。数据本地化并非将所有类型数据囊括其中，而仅针对直接影响国家安全的关键数据。

2.3.2. “单独同意”规则

从个人信息保护的角度出发，自然人主体的告知同意是数据处理者使用和传输个人数据的合法性基础[9]。为避免信息主体权益在数据跨境的过程中减损，我国《个人信息保护法》第 39 条明确将“单独同意”作为数据处理者向境外提供个人数据的前提条件。单独同意之所以区别于一般同意，在于信息处理者在就其信息处理行为取得信息主体同意的基础上，还需要告知信息接收者、信息处理内容及方式。

2.3.3. 安全评估制度

数据出境安全评估制度是我国个人数据出境监管体系的核心。根据数据本地化的强制性规定，一般情况下重要数据需存储于境内，自然人、企业或其他组织在符合一定条件的情况下，经由网信办进行安全评估后被准许向境外提供数据。在个人数据出境监管的场合，《个人信息保护法》以专章形式规定了个人数据处理者向境外提供个人数据时，需要满足的三类出境方式：即安全评估、专业机构认证、标准合同。[4]

3. 个人数据跨境规制模式比较分析

3.1. 欧盟模式

欧盟关于个人数据出境的法律规制主要由充分保护水平认定、提供适当安全保障及信息主体的明示同意三个方面组成。充分保护水平认定是指，符合欧盟所设置的数据安全标准的国家可以被列入白名单，白名单上的国家无需再参与进一步审查，即可与欧盟进行个人数据出境业务。但是，欧盟所设置的标准极为严苛，这一规定的适用范围受到限制。提供适当安全保障是指，对未得到充分保护水平认可的国家要求其对敏感信息采取额外的保护措施，这种保护措施可以是对信息主体使用假名。但是，对于基因数

[4]《个人信息保护法》第 40 条。

据，常规的去标识化处理并不能起到很好的保护效果。信息主体的明示同意是指，将信息主体的个人数据向第三国传输需征得其同意。然而，如此规定将导致高额的合规成本[10]。

3.2. 美国模式

相比之美国政府，美国的行业部门在保护个人数据安全出境方面占据着更为突出的地位，在个人数据出境方面提倡行业监管。当某一企业或个人滥用民众个人数据时，美国政府对待此种侵权行为的态度是谦抑且克制的[11]。相较而言，行业部门对个人数据安全出境负更重要的责任。例如，金融机构与其关联机构之间可以自由地传输信息主体的个人数据，但向非关联机构传输个人数据时务必获取信息主体的许可，并向其提供选退机制。虽然美国在行业内给予较充分的个人数据出境自由，但行业内仍存在，对个人数据自由出境造成限制的“隐性制度”。

3.3. 经验借鉴及启示

GDPR 作为在欧盟及至世界范围内公认的科学的数据保护法律规制，我国在构建个人数据出境的安全标准时可从中获取参考，尤其是在充分保护水平认定方面宜尽可能与欧盟标准相齐。对于使用敏感数据的信息利用主体，要求其对敏感数据采取特殊保护措施，全面保障敏感数据的安全。同时，也可以适当效仿美国的个人数据出境高度自由，并参照美国发展民间团体在个人数据出境过程中的安全保证作用。

4. 我国个人数据出境法律规制困境与不足

4.1. 外部规范体系松散、制度重叠

我国现有的涉及解决个人数据出境问题的法律法规存在部分矛盾之处。首先，在应当参与个人数据出境安全评估的标准方面，相关规定之间存在分歧。《个人信息保护法》规定了应当对涉及关键信息的基础设施运营者以及处理加工相当数量信息的处理者进行安全评估。但是，有别于《个人信息保护法》，后出台的《个人信息出境安全评估办法(意见征求稿)》则指出以是否具有“数据出境”行为而非是否为信息利用主体作为是否应当进行安全评估的判断标准。此外，关于自评估与安全评估的规定方面存在矛盾。《个人信息保护法》明确一般的信息处理主体不必须进行自我评估，而应当参与国家组织的安全评估。但是，一般的信息处理主体所加工的信息并未涉及国家安全问题，不宜将国家层面的安全评估作为个人数据出境的前提条件[12]。

4.2. 个人数据出境分级分类标准单一、规则细化程度低

由前所述，《网络安全管理条例(征求意见稿)》将个人数据划分为一般数据、重要数据与核心数据。如上的分类方式，在面临个人数据出境问题时，或将出现分类失灵的情况。在数据跨境传输的过程中，一般数据可能转为涉密程度更高一层级的重要数据，若仍依照该分类方式实行不同等级的保护，为涉密数据的出境设置较低的门槛，或许将对国家安全与数据主权构成威胁。因此，当个人数据出境后，应当重新订立一套符合个人数据出境特性的分类标准[13]。

此外，如上文所提及，当前仅《个人信息保护法》笼统地指出应当对出境的个人数据加以保护，缺乏更进一步的指示，未能明确具体措施，需要加以细化与延伸。

4.3. 独立数据监管机构缺位

目前我国尚未建立统一的数据监管机构，导致数据出境监管的领域存在执法权分散的情形。《数据安全法》第 6 条规定，“国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作”，我国形成了以网信部门为统领、各级政府及各行业主管部门负责各自管辖范围

内信息保护与监管事务的“1 + N”多层次数据管理机制。然而，该机制的弊端在于权责分散，难以形成事前监管、事后追责的全流程监管模式[14]。另外，分行业监管体系在实施过程中也会带来法律适用不统一、执法标准不一致的问题，实践中也难免存在重复处罚和相互推诿的情形。在追求效率的互联网时代，独立数据监管机构的缺位很可能导致企业在国际市场上处于竞争劣势，影响数字经济的高效运作与持续发展。

4.4. 企业个人数据出境合规机制尚不完善

随着数字产业经济发展日新月异，跨国公司在进行个人数据跨境传输及数字产业交易过程中，将不可避免地需要应对不同法域的多层数据监管规则。国际层面多数国家已通过立法确认数据权具有基本人权的地位，相关数据保护法规要求数据处理者承担起更多责任与义务[15]，企业数据出境合规压力随之凸显。一方面，多数企业合规意识淡薄、尚未构建起完善的内部数据合规管理体系。一系列数据监管法规的出台对数据安全和个人数据保护提出了更高的要求，企业不履行或未充分履行其数据合规自查义务将面临监管部门的高额罚款。另一方面，我国企业合规引导性机制尚存在不足。企业合规自查指引机制仍有待完善，亟须探索更为高效的方式引导企业健全和细化个人数据出境的自评估流程。

5. 我国个人数据出境法律规制路径的完善建议

5.1. 构建统一的个人数据出境规则体系

在司法实务工作中，可对告知信息主体的必要告知内容进行扩展延伸和统一规范，丰富“告知”的内涵与外延，充分平衡信息主体的隐私权、自决权与国家数据权之间的立场与关系。具体而言，现阶段《个人信息保护法》第十七条所规定的告知义务，仅包括姓名与联系方式等基本信息、处理意图与方法等具体信息，但仅履行通知上述信息的义务并不足以在个人数据出境的过程中保障其安全，应当将告知义务的适用范围扩展至包括但不仅限于个人信息处理者和境外信息接收方的姓名、联络方式、处理数据的目的等内容，使自然人数据出境的整个过程透明地向信息主体给予呈现。将告知义务进行上述扩展，有利于维护信息主体自身知情权，使得信息主体的个人数据出境后其权益也能得到充分保障，能够寻求救济措施[5]。有关个人数据出境的上位法与下位法之间应当密切配合，构成有机联系，彼此照应。例如，对上文提及的务必参与个人数据出境安全评估的标准问题，应进行统一规范，避免矛盾的存在。

5.2. 推进多元化分类标准，健全个人数据出境具体规则

一方面，我国需要推动建立起个人数据适应不同出境场合的多元化分类标准。首先，在《网络安全管理条例(征求意见稿)》所规定的分类方式基础之上，可将个人数据划分为一般数据、敏感数据与重要数据。对于一般数据允许放宽出境限制，以促进个人数据的自由流动，而敏感数据与重要数据可能转化为关乎国家数据安全的个人数据，此时对此二者的关注保护等级需要发生变化，应当在“知情－同意”方面作出限制，在安全评估方面加强把控[16]。

其次，也可依照地域标准对个人数据进行划分。海南自贸港对个人数据出境采取更为宽松的政策即属于采用这种以地域标准为划分依据的较为典型的情况。此外，还可按照个人数据产生的不同方式，将个人数据分为原始数据与衍生数据。建立起多元的分类方式有利于更具有针对性地保障个人数据安全，进而维护国家数据主权的安全。

另一方面，我国在细化个人数据出境安全评估规则方面需要持续发力。在采取前述具有针对性的个人数据分类标准的基础上，还需个人数据跨境的后续流程监管规则加以细化。对于出境后的个人数据应根据风险等级不同划分的诸如限制出境、备案后出境等进行分类监管，构建和完善个人数据的动态风险

防控机制[17]。针对附条件允许出境的个人数据，应加强对数据接收方的实时实地安全监控，并要求企业定期向网信办出具个人数据出境安全自评估报告并备案。

5.3. 建立专门的数据监管机构

为完善个人数据出境监管体系，建立独立的数据监管机构，不仅有利于对海量的个人数据实现统筹管理，更是我国进一步融入国际数据跨境管理体系的重要要求。如欧盟 GDPR 将一国设立统一的数据监管机构作为符合“充分性保护”的关键标准；亚太经合组织在其通过的“跨境隐私规则体系”中明确规定各成员国应当建立有独立执法权的隐私保护机构以实现保护公民个人隐私和数据权的目的。尽管《个人信息保护法》已规定由县级以上有关政府部门对个人数据负监管职责，但实践过程中各部门职能交叉、执法权分散。这要求在国家层面建立统一的数据监管机构，以达到覆盖数据传输全周期监督管理，统筹各方参与数据出境安全评估，更好地保障数据主体在数据出境流程中的合法权益。一方面，我国网信部门可以在原来的权责基础上扩大数据监管的权限范围，并开设独立的个人数据监管机构。另一方面，从企业层面而言，《个人信息保护法》虽要求互联网公司设立独立的数据管理机构，却遗漏了相应的惩罚措施，这将使其实施效果大打折扣。基于此，可以借鉴美国、欧盟等国家和地区的做法，设立专业的“数据保护官”，以监督企业处罚措施的落实。

5.4. 构建和完善企业个人数据出境合规体系

对于企业个人数据出境合规监管痛点，国家首先应发挥引导者的责任，加强政策扶持，激励企业加快数据安全自评估体系的建设。网信办可以提供公共服务产品，向社会发布企业个人数据传输国别指引，为我国企业作为数据处理者参与数据出境传输提供有力指导，降低数据合规成本与违规风险。此外，美国的行业自律模式也为我们提供了宝贵的经验，可以鼓励企业制定相关公司章程和开展数据安全自评估，以实现为行政监管提供补充的效果[18]。国家可以通过出台企业数据出境合规指南引导企业细化内部数据合规性审查规章，保障数据出境传输全流程安全。从管理体系而言，在公司内部设立专门的数据安全办公室，制定本公司数据安全管理规章，对现有数据处理方案进行优化；需要明确数据安全责任人，负责个人数据资产配置，授权数据管理人对个人数据进行运营管理。从管理技术的角度，引导企业利用技术手段对存储的个人数据进行安全检测与风险评估，确保数据在包括收集、存储、处理、传输、销毁的全生命周期均符合安全监管标准。

6. 结语

个人数据跨境流动是数字经济时代的重要议题，相关法律规制的完善和落实对维护个人权益、促进数字经济发展至关重要。通过对欧美经验的借鉴和我国先行数据规制框架的深入探究，为我国个人数据出境法律监管制度的改进提供有益启示和参考。首先，构建统一的个人数据出境规则体系应为重中之重，扩展告知义务内容，协调上位法与下位法，以确保法规之间的一致性和有效性。其次，推进多元化分类标准，健全个人数据出境具体规则，建立起适应不同出境场合的分类标准，并细化个人数据出境安全评估规则。第三，建立专门的数据监管机构，实现个人数据出境全流程监督管理，加强企业内部监管，推动企业建立完善的个人数据出境合规体系，强化技术手段保障数据安全。我国应与世界各国加强合作与交流，不断优化个人数据出境的法律规制体系，推动数字经济健康、可持续发展。

参考文献

[1] 资武成. 创新生态系统的数据治理范式: 基于区块链的治理研究[J]. 社会科学, 2021(6): 80-87.

[2] 项定宜, 毕莹. 大数据时代数据的类型化保护研究[J]. 重庆理工大学学报(社会科学), 2020, 34(6): 94-101.

[3] United Nations (2019) Digital Economy Report 2019. https://unctad.org/system/files/official-document/der2019_en.pdf

[4] Kent, A. (1990) Encyclopdia of Library and Informtion Science. Vo1. 45, Marcel Dekker, Inc., New York, 360 p.

[5] 沈玉良, 李墨丝, 李海英. 全球数字贸易规则研究[M]. 上海: 复旦大学出版社, 2008.

[6] 惠志斌, 张衡. 面向数据经济的跨境数据流动管理研究[J]. 社会科学, 2016(8): 13-22.

[7] 王利明. 论个人信息权的法律保护——以个人信息权与隐私权的界分为中心[J]. 现代法学, 2013, 35(4): 62-72.

[8] 姜程潇. 论数据双层结构的私权定位[J]. 法学论坛, 2022, 37(4): 119-126.

[9] 万方. 个人信息处理中的“同意”与“同意撤回” [J]. 中国法学, 2021(1): 167-188.

[10] 张继红, 蔡雨倩. 敏感个人信息跨境流动的国际规制[J]. 广西社会科学, 2023(7): 107-118.

[11] Goldman, D. (2006) I Always Feel Like Someone Is Watching Me: A Technological Solution for Online. *Hastings Communications and Entertainment Law Journal*, **28**, 353-408.

[12] 赫然. 个人信息跨境提供的规范分析与理论反思——以《个人信息保护法》第 38、39 条为视角[J]. 兰州学刊, 2022(3): 97-105.

[13] 齐爱民. 论大数据时代数据安全法律综合保护的完善——以《网络安全法》为视角[J]. 东北师大学报(哲学社会科学版), 2017(4): 108-114.

[14] 唐要家. 中国个人隐私数据保护的模式选择与监管体制[J]. 理论学刊, 2021(1): 69-77.

[15] Custers, B., van der Hof, S., Schermer, B., *et al*. (2013) Informed Consent in Social Media Use. The Gap between User Expectationsand EU Personal Data Protection Law. *Journal of Law and Technology*, **10**, 435-457. https://doi.org/10.2966/scrip.100413.435

[16] 陈峰, 王利荣. 个人信息“知情同意权”的功能检视与完善进路[J]. 广西社会科学, 2021(8): 106-111.

[17] 陈胜, 王可心. 数字经济时代个人信息跨境流动规制问题研究[J]. 中国商论, 2023(24): 44-47.

[18] 马其家, 李晓楠. 国际数字贸易背景下数据跨境流动监管规则研究[J]. 国际贸易, 2021(3): 74-81.