Dispute Settlement 争议解决, 2025, 11(11), 196-202
Published Online November 2025 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2025.1111360

Hans汉斯

数据跨境中个人信息与重要数据转化机制分析

黎颖茹

澳门科技大学，澳门

收稿日期：2025年10月19日；录用日期：2025年11月13日；发布日期：2025年11月21日

摘　要

随着信息科技发展，数据成为全球竞争中的战略资源与重要生产要素，其跨境流动在带来经济效益的同时，也对国家安全构成挑战。我国此前通过《网络安全法》《数据安全法》《个人信息保护法》及配套规定，构建了以安全为导向的强监管体系，涵盖维护国家安全与公共利益的数据出境管理制度，以及保护个人利益的个人信息出境监管制度。2024年3月《促进和规范数据跨境流动规定》(跨境新规)的实施，标志着我国数据跨境监管从严格管控转向“安全与便利兼顾”的阶段。该新规确立个人信息出境监管豁免制度，对特定情形下的数据出境安全评估、个人信息出境标准合同及个人信息保护认证给予出境前监管豁免。但因个人信息与重要数据的关系尚未明晰，二者转化条件及判断标准存在争议，监管豁免制度引发了对安全失衡的担忧。本文将通过梳理制度层面对个人信息与重要数据的关系定位及转化条件的相关规定，分析学界在二者转化机制研究中的未明晰之处，并借鉴域外经验，探讨可行的个人信息向重要数据的转化识别机制，以保障数据出境监管豁免制度在最大阈值内实现数据跨境流通自由，同时不触及国家安全保障红线。

关键词

数据出境监管豁免，个人信息，重要数据

Analysis of the Transformation Mechanism of Personal Information and Important Data in the Context of Cross-Border Data Flows

Yingru Li

Macau University of Science and Technology, Macau

Received: October 19, 2025; accepted: November 13, 2025; published: November 21, 2025

Abstract

With the advancement of information technology, data has emerged as a strategic resource and a

文章引用: 黎颖茹. 数据跨境中个人信息与重要数据转化机制分析[J]. 争议解决, 2025, 11(11): 196-202.
DOI: 10.12677/ds.2025.1111360

critical factor of production in global competition. While cross-border data flows generate significant economic benefits, they also present challenges to national security. China has established a robust regulatory framework centered on security through the "Cybersecurity Law", the "Data Security Law", the "Personal Information Protection Law", and their implementing regulations. This framework encompasses a data export control system designed to safeguard national security and public interests, as well as a supervision mechanism for personal information exports aimed at protecting individual rights. The implementation of the "Regulations on Promoting and Regulating Cross-Border Data Flows" in March 2024 signifies a pivotal shift in China's approach to cross-border data regulation—from a model emphasizing strict control to one that seeks to balance security with facilitation. The new regulations introduce an exemption mechanism for personal information exports, allowing pre-export regulatory relief from security assessments, standard contractual clauses, and personal information protection certification under specified conditions. However, due to the lack of clarity regarding the relationship between personal information and important data, uncertainties persist concerning the criteria for classification and the conditions under which such data categories may be converted. As a result, concerns have arisen about potential imbalances in the regulatory framework. This article aims to systematically examine institutional provisions concerning the definition and conversion criteria between personal information and important data, identify ambiguities in existing academic discussions on transformation mechanisms, and draw upon international regulatory practices to propose a feasible identification and conversion framework. The objective is to ensure that the regulatory exemption regime for data outbound flows facilitates maximum openness for cross-border data circulation while strictly adhering to the boundaries of national security.

Keywords

Exemption from Data Outbound Supervision, Personal Information, Important Data

1. 问题的提出

随着信息科技的高速发展，数据作为一种新兴的战略资源和重要生产要素，其在全球竞争中的重要地位毋庸置疑。数据跨境流动在为各国带来经济效益的同时，也对国家安全产生了前所未有的挑战。为了应对这一挑战，我国通过制定《网络安全法》《数据安全法》《个人信息保护法》及相关配套规定，构筑起旨在维护国家安全、公共利益的数据出境管理制度及旨在保护个人利益的个人信息出境监管制度[1]。这两种制度的确立充分彰显了数据规制体系成立之初，我国对数据出境以安全为导向的强监管态度。

2024 年 3 月，《促进和规范数据跨境流动规定》(下称跨境新规)颁布实施，这一新规的出台标志着我国数据跨境监管从过往的严格管控转向兼顾安全与便利的调整阶段。跨境新规确立了个人信息出境监管豁免制度，同时对特定情况下的数据出境安全评估、个人信息出境标准合同、个人信息保护认证予以一定条件下的出境前监管豁免。但由于个人信息与重要数据之间的关系尚未明晰，二者间的转化条件及判断标准尚存争议，数据出境监管豁免制度引发了各界对于监管豁免后可能导致的安全失衡的担忧。

本文将通过介绍制度层面对个人信息及重要数据的关系定位及关于二者转化条件的相关规定，分析学界对于个人信息及重要数据转化机制研究中尚未明晰之处，结合对域外经验的借鉴，探讨如何建立可行的个人信息向重要数据的转化识别机制，以保障数据出境监管豁免制度在最大阈值内实现数据跨境流通自由而不触及国家安全保障的红线。

2. 制度梳理及学界争议

(一) 理论基础：风险规制

风险规制理论源于上世纪中后期各国对于“不确定风险”的治理需求，其核心是通过构建“风险识别–风险评估–风险应对–风险监控”这一完整的系统性框架以实现安全与发展的动态平衡。风险预防原则最先应用于环境法领域，但近年来随着数字化经济的飞速发展，学界开始意识到数据在跨境流动过程中具备隐蔽性、传导性、不确定性等特点，并开始探讨风险理论在数据安全监管体系中的应用。

现有风险规制理论具有“风险识别精准性”、“风险评估多元性”、“风险应对比例性”、“风险监控动态性”等特点。风险识别精准性要求对风险源进行本质界定，明确区分潜在风险与现实风险，避免因泛化风险导致监管过度。风险评估的多元性反对通过单一指标进行片面评估，主张结合风险发生概率、影响范围、传导路径等多元因素构建多维度评估体系。风险应对的比例性原则要求规制措施与风险等级相匹配，在低风险领域应当简化规制以提高效率，在高风险领域则应当强化管控以保障安全。风险监管的动态性则强调风险是流动多变的，需要根据技术迭代、场景变迁等调整规制策略，避免静态规则与动态风险脱节[2]。

就本研究而言，从风险识别层面来看，数据出境监管豁免制度存在的核心安全隐患是个人信息与重要数据存在界定模糊的问题，而风险规制理论对于“精确定位风险源”的强调与本文探讨“个人信息向重要数据转化机制”高度契合，对于转化机制的探讨本质上是对数据风险源的识别过程。从风险评估层面来看，本文反对现有制度单纯以定量为标准判断个人信息与重要数据间的转化关系，与风险规制理论反对一刀切的规制模式，主张基于多元评估的理念直接呼应。从风险应对层面看，风险规制理论的比例原则要求规制措施需要兼顾安全与效率，数据出境监管豁免制度恰是这一原则的体现，本研究在此基础上讨论建立更为完善的转化机制的可能性则是为了避免豁免制度因风险误判导致的安全失衡问题。综上，风险规制理论与本研究高度契合，为后续研究提供坚实的理论基础。

(二) 现有制度对个人信息及重要数据的关系定位及其转化机制

纵观我国现有与数据相关的规范体系，法律作为层级更高的立法规范，并未对重要数据作出概念性界定，甚至于在《网络安全法》颁布实施以前，“重要数据”一词并不具备独立意义[3]。2017 年 6 月 1 日《网络安全法》正式施行，当中第 37 条提到“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储”，从该条对“个人信息和重要数据”的表述来看，将个人信息和重要数据作为两种独立的数据类型似乎更符合《网安法》的立法意图。随后为完善数据规范体系而颁布的包括《网络数据安全管理条例》等行政法规以及更低级别《数据出境安全评估办法》及一系列国家标准中，都对个人信息和重要数据的关系多采取“个人信息和(或者)重要数据”这种明确体现出二者独立性的表述。

虽然相关规定在文字表述上将个人信息和重要数据作为两种独立的数据类型来处理，但通过对规范条文的分析可发现，这种独立是具有相对性的，个人信息在满足特定条件时，可转化为重要数据。如《网络安全管理条例》第 28 条提出：“网络数据处理者处理 1000 万人以上个人信息的，还应当遵守本条例第三十条、第三十二条对处理重要数据的网络数据处理者(以下简称重要数据的处理者)作出的规定。”根据该条内容，数据处理者在处理 1000 万人以上个人信息时，同时承担个人信息保护及条例规定的重要数据安全保护义务，换言之，当处理的个人信息达到一定的量值时，数据处理者的身份将从“个人信息处理者”转化为“个人信息及重要数据处理者”，立法者虽未言明，但从其将第三十、三十二条所规定的重要数据安全保护责任置于第二十八条所涉的个人信息数据处理者承担可知，立法者认同、至少是不否认个人信息和重要数据在范围上存在着重叠的部分。由此可得出，在规范层面，个人信息和重要数据是相对独立的两种数据类型，但二者在特定情况下存在范围或内容上的重叠。而就二者重叠部分的识别，或

者说，个人信息向重要数据的转化方式，我国采用定量方式进行界定考量。

如前述《网络安全管理条例》第二十八条对定量个人信息处理者施以部分重要数据安全保护责任，说明一定量的个人信息对公共利益而言，其价值等于或不低于重要数据。其次，《数据安全技术数据分类分级规则》3.2 条注：“仅影响组织自身或公民个体的数据一般不作为重要数据”，该注明内容体现了现有规范虽认同个人信息一般不作为重要数据，但并非绝对。另外，《重要数据识别指南》对个人信息和重要数据的关系表述为：“重要数据不包括国家秘密和个人信息，但基于海量个人信息形成的统计数据、衍生数据有可能属于重要数据”，以上种种皆佐证了立法者对个人信息和重要数据的关系定位为相互独立，但在满足定量条件下个人信息可转化为重要数据这一观点。

然而，规范对为何以定量作为转化标准以及确定量的依据何在等一系列问题却未在立法过程中予以说明或解释，这也导致学界和实务界对于个人信息和重要数据的转化机制合理性存在一定争议。

(三) 学界争议

中科大教授左晓栋在 2022 年北京网络安全大会上指出，“批量个人信息是不是重要数据”是一个伪命题。左晓栋教授在大会上指出，个人信息和重要数据是两种独立并且无关联的数据类型，“我们只能说当个人信息符合某种特征时，其在某种情况下可能是重要数据，而不会说(个人信息)天然就是重要数据”[4]。左晓栋教授对于个人信息和重要数据的关系观点与立法机关观点大致相同，均认为二者存在独立性。但对二者的转化机制，与制度规范中单纯以定量方式判断不同，左晓栋教授对于二者的转化情形采用了更为严谨的“符合某种特征 + 符合某种情况”这一定性方式来进行转化判断，这一观点似乎比起单纯的定量判断更能保障数据安全。遗憾的是，左晓栋教授虽否认了定量判断，却未给出定性的具体判断标准。另外，根据左晓栋教授否认单一的定量判断而采用“符合某种特征 + 符合某种情况”定性判断的逻辑，是否可以认为，单条个人信息满足定性标准后也可能成为重要数据？如果答案是肯定的，满足定性标准的个人信息就会同时具备个人信息和重要数据双重身份，这似乎又与左晓栋教授“个人信息就是个人信息，重要数据就是重要数据”这一过于绝对的关系表述不相符。

中国法学会法制研究所研究员胡金瑞也认同个人信息和重要数据是两种独立的数据类型，但二者在满足一定条件下可以实现个人信息向重要数据的转化。根据刘金瑞研究员的观点，我国实行的是“以维护个人权益为目的的个人信息跨境监管制度和以维护国家安全及公共利益为目的的重要数据跨境安全监管制度”双轨并行的数据跨境管理制度，而这种双轨并行的制度模式说明了个人信息和重要数据是具有相对独立性的两种数据类型[5]。和立法机关相同的是，刘金瑞研究员也认同个人信息在达到一定量的条件下可以转化为重要数据，不同的是，立足于个人信息出境监管豁免视野下，刘金瑞研究员认为单纯以定量为判断标准是不够的，如果在个人信息监管豁免场景中，单纯以定量的标准判断是否应当进行安全评估，则会提高“少量信息经聚合分析后形成重要数据从而危害国家安全或公共利益”的风险。刘金瑞研究员认为，完善个人信息向重要数据的转化判断机制在个人信息出境监管豁免中尤为重要，《跨境新规》及其他法律法规、部门规章等所规定的定量标准不能满足保障国家安全及公共利益的要求。虽然如此，其与左晓栋教授一样，仅笼统提出应以定性为判断条件，并未就此展开讨论。

郭春镇、候天赐认为目前学界和实务界对于个人信息跨境流动的界定暂未达成一致，并提出应当基于“场景－风险”视角建立动态判定框架，在具体场景中判断信息跨境活动可能造成的风险[6]。但二者未对场景设计标准及判断条件给出具体方案。

另外，郭壬癸、胡延杰也在其研究中指出：“不论是企业数据还是个人信息，如果因聚合效应后可能危及整体层面的利益，也会构成重要数据”，但与前述学者不同，郭壬癸、胡延杰对于个人信息向重要数据转化定量判断并无异议，只是认为《数据出境安全评估办法》中所规定的数量阈值过低，容易造成非必要评估泛化及加重出境限制[7]。张建文则认为，之所以存在个人信息和重要数据之间的关系模糊

或转化机制不明晰，是因为重要数据法律制度尚未完善[3]。

学界对于个人信息和重要数据的关系似乎并无太多争议，主流观点都认同个人信息和重要数据具有相对独立性，在特定情况下存在交叉重叠，这也与法律规范及部门规章所表述的大致相同。而对于个人信息向重要数据的转化机制，学界对于现有的定量判断标准似乎不甚满意，但并未就具体改善方案提供有效意见。

3. 完善路径

(一) 必要性

我国现有制度仅以定量标准作为个人信息向重要数据转化的判断依据，这一判断标准具有合理性但并不全面。根据观察者网报道，一名澳大利亚学生通过某健身应用公布的信息成功定位到美军在多个地区的军事基地，这一信息的泄露被称为是“军事作战安全的灾难”。另外，2022 年滴滴公司的数据泄露案也证明了达到一定量的个人信息聚合后可能会形成重要数据这一事实。但是仅以定量为标准却无法满足特定情况下少量个人信息泄露对国家安全和公共利益造成的危害，例如对于某些诸如警察家属等身份特殊的群体而言，其身份具有现实意义上的特殊性，但又不具备法定意义上的特殊身份，其个人信息管理采用的是和普通群众同等的管理手段，对其出行信息等特殊信息进行聚合分析，仍有可能提取出重要数据。另外，对于如机要部门等特殊地点的人流信息等提取分析也可能得出重要情报。即便部分个人信息可以进行脱敏处理(如通过技术手段去标识化或匿名化处理等)，但脱敏后的数据仍可通过技术手段进行重新识别，且重识别后的数据与源数据相比契合度较高[8]。在这种情况下，仅进行定量标准判断个人信息是否构成重要数据显然是不能满足安全保障需求的。

另外，立足于《跨境新规》制定的个人信息出境监管豁免制度来分析，以定量标准豁免个人信息出境监管存在安全隐患。《跨境新规》第 5 条规定了四种豁免场景，其中第四项规定“关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供不满 10 万人个人信息(不含敏感个人信息)的”可免于安全评估、订立个人信息出境标准合同及通过个人信息保护认证。此外，第 7 条规定：“关键信息基础设施运营者以外的数据处理者向境外提供重要数据，或者自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息(不含敏感个人信息)或者 1 万人以上敏感个人信息”的，应当申报数据出境安全评估。这些规定从一定程度上放宽了个人信息跨境限制，但考虑到出境前的安全评估制度对于数据跨境流动监管而言是维护国家安全和公共利益的第一道、也是极其重要的一道防线，跨境新规单纯以定量方式来进行监管豁免或实行安全评估申报条件，显然无法达到维护国家安全及公共利益的要求，毕竟数据一旦出境并发生数据泄露，事中监管和事后补救都只是亡羊补牢的手段。

因此，鉴于定量方法无法覆盖在现实中在特定情况下少量个人信息经过技术分析可得出重要情报的情形，个人信息向重要数据的转化机制应当采用“定量 + 定性”的方法进行判断。

(二) 域外经验

(1) 美国

2024 年 2 月 28 日，拜登总统签署颁布了《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据的行政命令》(简称《EO14117》)，随后美国司法部于 2024 年 12 月 27 日颁布了《防止受关注国家及相关人员访问美国敏感个人数据和政府相关数据的规定最终规则》(简称《最终规则》)，以细化和落实该行政命令。这两套规则进一步限制了美国数据向特定国家的流动，体现了美国在数据跨境流动监管方面对特定国家/地区的严格态度和先进经验。

与一直以来奉行的数据自由流动政策不同，《最终规则》以《EO14117》为基础，对包括个人标识符、生物识别标识符在内的六种个人数据进行了敏感性识别，并对此设置了由 100 到 10,000 不等的处罚跨境流动限制监管的阈值，并将已通过匿名化、假名化或去标识化等脱敏处理后的信息也纳入计算阈值中。

另外，对于美国公职人员个人信息，包括但不限于现任或离任人员信息，均限制出境，并不设阈值要求。

《最终规则》对于个人信息出境不仅根据不同敏感程度的信息设置了不同的定量标准，还针对特定群体的个人信息设置了无条件出境禁止，如离任公职人员，其虽已丧失特殊身份，但仍被纳入出境限制范围中，这无疑更有利于数据安全防护，在最大程度上防止受关注国家和地区通过数据再识别、聚合分析等手段提炼重要情报。

《最终规则》采用的“敏感性分级 + 差异化阈值”的定量评估逻辑和“特殊身份 + 全周期保护”的定性评估延伸既提升了定量评估的精确性，又填补了对少量特殊个人信息聚合风险的监管空白。另外，《最终规则》采用“动态名单 + 定向管控”的监管模式，对受关注国家采取低阈值严管控的风险匹配管控逻辑可为我国提供一定借鉴，在定量维度上，美国的识别制度采取的是根据信息敏感程度的不同划分不同的阈值，相比于中国一刀切的定量方式，显然美国模式所构筑的安全防御网更具弹性；在定性维度上，美国模式不仅识别了在任公职人员，还将离任人员纳入其中，有效防范了相关人员在信息保密期离任后因个人数据外流造成的对国家安全的威胁，扩大了安全防御网的范围。但不可否认的是，《最终规则》具有地缘属性及治理排他性，“受关注国家”名单及对特定国家的严格管控措施本质上是基于政治博弈需求，与我国“安全与便利兼顾”的数据跨境治理目标相违背，且其对于离任公职人员信息不设阈值、无条件限制亦与比例性原则相悖，存在过度监管的嫌疑。

(2) 欧盟

欧盟 GDPR 采用以“敏感性–场景”为核心的双维度分类体系，将个人数据分为“普通个人数据”与“敏感个人数据”，其核心是“敏感性越高，保护强度越大”，并要求数据分类需要结合“处理目的与场景”等考量因素。GDPR 要求数据管理者在实行数据跨境前需要展开数据保护影响评估(DPIA)，评估指标包括数据敏感性、传输规模、接收国保护水平等，其核心是保障“风险与措施”满足比例性原则，比如敏感数据在跨境前需要额外签署补充协议等，DPIA 评估流程共分为九步，覆盖数据处理全周期，流程严谨、全程可追溯。在评估主体上，DPIA 要求评估过程需要咨询数据保护官、数据主体、技术专家等多元主体，以确保风险识别的全面性。

另外，GDPR 条文中对于敏感个人信息范围作出明确规定，并要求信息收集者在收集信息过程中满足最小化原则，即仅收集和处理为实现特定目的所必需的信息。在持有、控制数据过程中，数据处理者担负证明合规性的义务，需要对数据活动、类别、流转路径等信息进行详细记录，以作监管检查即合规证明的依据。另外，GDPR 及欧洲数据保护委员会(EDPB)指南中列明若干种需强制适用 DPIA 的情形。

欧盟对特定数据纳入强制评估范围，要求完成 DPIA 评估流程前不能进行数据处理，这一前置防控逻辑避免了先出境后评估导致的监管滞后问题，在数据处理活动开展前就完成了风险防控。另外，DPIA 通过“描述处理活动→评估必要性→识别风险→制定缓解措施”的标准化流程(EDPB“九步法”)，确保评估可追溯、可验证，避免了形式化评估带来的风险，且多元主体参与风险评估在确保专业性的前提下有效平衡企业与政府的合规成本。不同于美国模式，欧盟模式虽对数据出境设置了严密的评估体系，但其主要目的却是在于保护自然人权利与自由，其风险评估机制聚焦于个人信息泄露对用户的影响，对数据聚合后可能产生的危害国家安全的风险考量不足，且 DPIA 合规成本极高，对参与评估的主体也有较强的专业性要求。

(三) 中国方案

针对我国现有制度的不足，可结合美国及欧盟的模式，建立“敏感性分级 + 动态定量”的识别机制。

首先，针对敏感性分级部分，我国个人信息向重要数据转化识别存在困难主要是因为个人信息和重要数据存在界限上的模糊，数据处理者在进行数据跨境活动时容易陷入似是而非的尴尬境地。针对这一问题，可以借鉴美国设定分级阈值，纳入场景评估作为考量因素，通过制定以水平变数、垂直变数为横纵轴的量化式计分判断表格，将个人信息按照敏感性程度进行数据风险等级评分，如对与生物识别等相

关的个人信息给予高评分，消费记录等普通信息给予低评分，并结合行业特点、特殊身份等考量因素进行综合计分，达到预设分数标准即实现个人信息向重要数据的转化。制定表格式的指引有助于数据处理者及监管方清晰了然地判断个人信息的敏感程度及其是否存在转化为重要数据的可能，能有效提高识别准确性。数据处理者在申请数据出境豁免前可自行通过表格完成数据敏感性识别，提高豁免审批效率，而监管方则可以通过随机抽查的方式对申请处境豁免的数据进行抽样检查，这样既能保障数据安全，又能实现成本分摊，最大程度上平衡安全与效率。

其次，为进一步加强安全防御效力，可在量化计分评估的基础之上引入场景化风险评估机制，对具备特殊身份的主体及特殊区域相关信息进行关联分析可能性评估，结合“特殊身份主体清单”，并通过指定不同行业的操作指引，细化特定场景的转化规则。

另外，还可在借鉴美国模式的基础之上制定动态信任名单，根据中国与各国或地区在数据领域的合作模式、信任程度不同，制定动态信任名单，对不同国家和地区根据合作模式和信任程度采取不同的信任标准，并根据信任标准的不同设置不同的定量阈值门槛，在最大程度上实现数据跨境自由与安全之间的平衡。另外，为了便利数据传输者及时、清晰的了解定量标准及信任名单，在技术上可设计统一查询平台供数据传输者查阅。

除此之外，还可对《跨境新规》中的豁免制度制定特殊情况下的豁免除外条款，对于特殊情况下(如与数据接收国发生数据争端或某类人员因特殊情况在短暂时间内拥有特殊身份时)，可由有关部门宣布相关个人信息不适用豁免条款。对适用豁免制度豁免事前监管的数据加强事中和事后监管，加强事中、事后抽样审查，重点关注数据出境后的聚合风险。

4. 结语

本文通过对制度层面、学界争议、案例分析以及域外经验的综合探讨，得出个人信息与重要数据并非完全独立，二者在特定条件下存在转化关系的结论，这为数据跨境流动中的个人信息监管提供了新的视角，同时发现现有制度采取定量方式判断个人信息向重要数据转化虽存在一定合理性但不足以满足保障国家安全和维护公共利益的要求，这一再认识为我国完善相关制度和实践操作提供了理论支撑。基于上述分析，建立“定量 + 定性”识别机制显得尤为重要，这不仅有助于准确判断个人信息集合是否可能转化为重要数据，还能确保数据跨境流动的安全和效率。本文结合域外经验，建议参照美国模式制定一套具体完善的识别机制，明确不同敏感性个人信息合集的数量门槛和定性标准，为数据跨境流动中的个人信息监管提供明确的指导和依据，以最大程度实现数据跨境流动中自由与安全的平衡。

参考文献

[1] 刘金瑞. 数据跨境双轨制下个人信息出境监管豁免制度的适用与完善[J]. 财经法学, 2024(5): 23-40.

[2] 苏宇. 风险预防原则的结构化阐释[J]. 法学研究, 2021, 43(1): 35-53.

[3] 张建文. 对作为独立数据类型的“重要数据”的发生史与本体论考察[J]. 上海政法学院学报(法治论丛), 2025, 40(1): 53-64.

[4] 批量个人信息是重要数据吗? 左晓栋: 伪命题, 不应强行关联[N]. 南方都市报, 2011-07-04(01). https://m.163.com/dy/article/HBFI1SRP05129QAF.html?spss=adap_pc

[5] 刘金瑞. 我国重要数据认定制度的探索与完善[J]. 中国应用法学, 2024(1): 189-200.

[6] 郭春镇, 候天赐. 个人信息跨境流动的界定困境及其判定框架[J]. 中国法律评论, 2022(6): 86-106.

[7] 郭壬癸, 胡延杰. 重要数据出境安全评估制度的偏离与修正[J]. 科技与法律(中英文), 2024(1): 43-53.

[8] Wu, Z., Huang, Y., Wang, L., Wang, X. and Tan, T. (2017) A Comprehensive Study on Cross-View Gait Based Human Identification with Deep CNNs. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **39**, 209-226. https://doi.org/10.1109/tpami.2016.2545669