《个人信息保护认证实施规则》背景下的认证制度实施*

刘懿阳
(中山大学法学院 人权法研究中心,广东 广州 510006)

摘 要:认证是数据跨境的主要合规路径,也是个人信息保护制度的有机组成。《实施规则》将一般情况下的个人信息保护认证和特殊情景下的个人信息出境认证"合二为一",对个人信息保护认证体系进行了整体性构建,明确了认证范围、认证依据、认证程序、认证标识等内容,在扩展认证范围、促进数据出境、明确侵权责任、推动国际互认等方面具有重大价值。个人信息保护认证制度实施需要政府、企业等多方主体共同参与,体现出数字时代公私合作的数据治理特征。

关键词:个人信息保护;数据跨境;认证;合作规制
中图分类号:D92;G203 文献标识码:A DOI:10.19358/j.issn.2097-1788.2023.01.008
引用格式:刘懿阳.《个人信息保护认证实施规则》背景下的认证制度实施[J].网络安全与数据治理,2023,42(1):61-66.

Implementation of the personal information protection certification system based on the Implementation Rules for Personal Information Protection Certification

Liu Yiyang
(Center for Human Rights Law Studies, Sun Yat-sen University, Guangzhou 510006, China)

Abstract: Authentication is the main compliance path of cross-border data and an organic component of personal information protection system. The Rules for Implementation "integrate" the personal information protection certification in general and the personal information exit certification in special situations, comprehensively construct the personal information protection certification system, and define the certification scope, certification basis, certification procedures, certification marks and other contents. It has great value in expanding the scope of authentication, promoting data exit, clarifying tort liability and promoting international mutual recognition. The implementation of the personal information protection and authentication system requires the participation of the government, enterprises and other parties, which reflects the data governance characteristics of public-private cooperation in the digital era.

Key words: personal information protection; cross-border data flows; certification; cooperative regulation

0 引言

随着《个人信息保护认证实施规则》(以下简称《实施规则》)出台,我国数据跨境认证制度实现了规则落地。"认证"是《个人信息保护法》第38条规定数据跨境流动的三种合规路径之一,除认证外,数据出境的合规路径还包括"安全评估"和"标准合同"。数据出境安全评估是一种具体行政行为[1],标准合同签订是一种私主体商事行为[2],专业机构认证则是一种第三方规制行为[3]。数据跨境认证是合作规制理论在数字时代的生动实践,体现出数字社会背景下数据治理的公私合作特征,《实施规则》为数据跨境认证的实施提供了现实方案。

除数据跨境处理外,《实施规则》同样适用于其他类型的个人信息处理活动。《实施规则》从认证范围、认证依据、认证程序、认证标识和认证责任等方面对个人信息保护认证规则进行了整体构建,在扩展认证范围、促进数据出境、明确侵权责任、推动国际互认等方面具有重要的实践意义。下面,

*基金项目:国家社会科学基金重大项目《互联网经济的法治保障研究》(18ZDA149)阶段性成果

本文将从规则要点、制度设计、实践意义三方面，对《实施规则》所规定的中国个人信息保护认证规则展开解读、评介与反思。

1 《实施规则》的要点解析

《实施规则》从认证适用范围、认证依据、认证模式、认证程序、认证标识、认证细则和认证责任七个方面对个人信息保护认证规则进行了整体构建，明确了认证的主体、对象、依据、流程等问题。下面，本文将从《实施规则》的重点内容展开分析。

1.1 认证范围

《实施规则》规定了对个人信息处理者开展个人信息收集、存储、使用、加工、传输、提供、公开、删除以及跨境等处理活动进行认证的基本原则和要求。从认证主体来看，凡是个人信息处理者皆可申请该项认证。从认证对象来看，认证涉及个人信息处理活动过程的产品、服务、管理体系。从认证内容来看，认证仅仅涉及个人信息，而不包括其他数据——例如《数据安全法》规定的核心数据和重要数据、《数据出境安全评估办法》规定的重要数据、《关键信息基础设施安全保护条例》规定的关键信息基础设施相关数据以及《个人信息保护法》规定的匿名化处理后的信息，此类非个人信息均不属于《实施规则》的认证内容。另一方面，认证是对个人信息处理的认证，个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等，同时也包括了数据跨境传输的处理活动。总体来看，《实施规则》规定的认证主体范围更明确，适用对象范围更广阔(包括产品、服务、管理)，内容界定范围更有针对性(仅限于个人信息)。

1.2 认证依据

《认证认可条例》是实施个人信息保护认证的根据之一，条例第 2 条规定了认证“是指由认证机构证明产品、服务、管理体系符合相关技术规范、相关技术规范的强制性要求或者标准的合格评定活动”。最新版本的 GB/T 35273《信息安全技术 个人信息安全规范》和 TC260-PG-20222A《个人信息跨境处理活动安全认证规范》是《实施规则》所规定的认证依据。前者是由市场监管总局与国家标准化管理委员会联合发布的国家标准，在《个人信息保护法》实施以前就对企业数据合规建设提供重要依据和规范指南；后者是由全国信息安全标准化技术委员会组织制定和发布的技术规范，同样可以作为认证依据。根据规定，凡个人信息处理者均需要满足前一种规范的要求，而开展跨境数据传输的个人信息处理者还应当符合后一种规范的要求。

1.3 认证程序

“技术验证+现场审核+获证后监督”是《实施规则》提出的个人信息保护认证模式。按此模式，认证机构在对认证委托人提交的认证委托资料进行审查过后，决定是否受理并向委托人及时反馈，受理后将确定认证方案并告知委托人。具体认证程序如下：

(1)技术验证：据此方案，技术验证机构实施技术验证，并向认证机构和认证委托人出具技术验证报告。

(2)现场审核：在收到技术验证报告之后，认证机构将对个人信息处理者实施现场审核，并向认证委托人出具现场审核报告。

(3)获证后监督：根据认证委托人提交的委托资料、技术验证机构出具的技术验证报告、认证机构掌握的现场审核报告和其他相关资料信息，认证机构将进行综合评价，最终决定认证申请是否通过。对符合认证要求的个人信息处理者颁发认证证书。在有效期内，认证机构将采取适当方式、以合理监督频次，对已获认证的个人信息处理者进行持续监督。

综上所述，《实施规则》以认证前资料审查、认证中能力审核、认证后持续监督的事前、事中、事后全过程规制模式对认证程序作出了具体规定，其流程如图 1 所示。

1.4 认证证书

认证机构将对符合认证要求的认证委托人颁发认证证书，有效期为 3 年。在此期间，认证委托人可向认证机构提出变更委托，对已获认证的个人信息处理者相关资料进行变更，也可申请将认证证书暂停、注销；到期后，认证委托人需要延续使用的，应在有效期届满前 6 个月内提交申请。获证后，认证委托人将受认证机构的持续监督，监督过程中若已获证的个人信息处理者不再符合认证要求，认证机构应当及时对认证证书予以暂停直至撤销。认证证书既不是行业许可证，也不是营业执照，而是一种资质认证，体现出认证机构对于认证委托人个人信息保护能力的肯定评价。

1.5 认证责任

《实施规则》规定，认证机构、技术验证机构、认

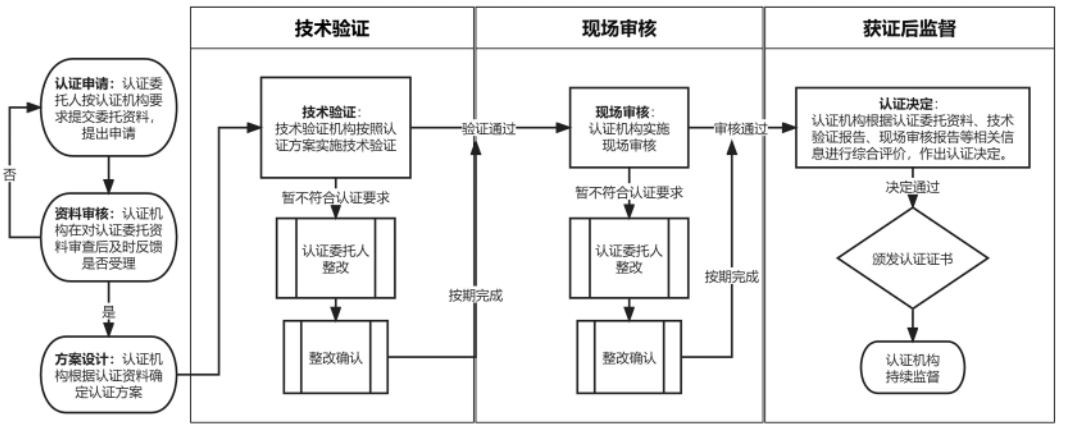

图 1　个人信息保护认证流程图

证委托人分别对各自的认证和验证结论、认证委托资料的真实性和合法性负责。针对认证机构的责任，《认证认可条例》第 73 条规定了“认证机构未对其认证的产品实施有效的跟踪调查，或者发现其认证的产品不能持续符合认证要求，不及时暂停或者撤销认证证书和要求其停止使用认证标志给消费者造成损失的，与生产者、销售者承担连带责任。”也就是说，若认证机构对个人信息主体造成损失则需承担连带责任，这意味着认证机构在个人信息保护认证工作实施过程中担负着持续的监督和审查义务，面临着重要的认证责任。

总体来看，《实施规则》将认证实施的适用范围界定在“个人信息”内容，依据国家标准和相关技术规范开展认证工作，提出了事前事中事后全过程规制的认证程序，公布了认证证书和认证标志，明确了认证的主体、对象及其责任。但《实施规则》的具体落实仍待认证机构对认证实施程序进行进一步的细化，认证机构在实践过程中所制定的科学、合理、可操作的认证实施细则才是《实施规则》方案真正落地的“最后一公里”。

2《实施规则》的制度设计

个人信息保护认证制度的上位法依据是《个人信息保护法》和《认证认可条例》。

《个人信息保护法》对认证制度的规定在第 38条和第 62 条均有体现。第 38 条对于跨境流动的个人信息提供了出境认证的合规路径；第 62 条第(四)项对个人信息开展认证服务，推进个人信息保护社会化服务体系建设作了规定。此次《实施规则》的出台标志着《个人信息保护法》中认证工作的具体实施有了明确依据，为数据出境中的“认证”路径提供了有力支撑，同时也对个人信息保护社会化服务体系建设提供了有效保障与落地方案。

如前所述，《实施规则》明确了认证的依据为 GB/T 35273《信息安全技术 个人信息安全规范》与 TC260－PG－20222A《个人信息跨境处理活动安全认证规范》，前者面向一般情况下的个人信息保护认证，后者则应对于特殊情景中的个人信息跨境认证。也就是说，《实施规则》是将个人信息保护认证和个人信息跨境认证“合二为一”。两者区别在于，个人信息保护认证针对的是认证委托人对于个人信息保护的水平，认证结果是对委托人个人信息保护能力和资格的评价；而个人信息跨境认证针对的是委托人在个人信息跨境传输场景下的数据处理行为，认证结果是认证机构对于委托人具体数据处理活动的特殊认证。

《认证认可条例》第 2 条明确了认证的对象为“产品、服务、管理体系”，认可的对象则是“认证机构、检查机构、实验室以及从事评审、审核等认证活动人员的能力和执业资格”，认证制度主要适用于企业，认可制度则是对认证机构及其人员的监督机制。根据《认证认可条例》，认证是要证明产品、服务、管理体系符合“相关技术规范、相关技术规范的强制性要求或者标准”。申请个人信息保护认证的个人信息处理者应当符合 GB/T 35273《信息安全技术 个人信息安全规范》的要求；但如果要在个人信息出境时采信认证结论，还需针对个人信息出境场景增加认证要求，即还必须符合《个人信息跨境处理活动安全认证规范》的要求。这相当于，我国既

建立了通用的个人信息保护认证制度,又建立了针对数据出境场景的个人信息出境认证制度。后者是前者的补充,前者是后者的基础(如表 1 所示)[1]。

《认证认可条例》第十七条指出,“认证机构应当按照认证基本规范、认证规则从事认证活动。认证基本规范、认证规则由国务院认证认可监督管理部门制定;涉及国务院有关部门职责的,国务院认证认可监督管理部门应当会同国务院有关部门制定。”这实际上指出了认证认可监管思路——在专业领域涉及到国务院有关部门职责的,由国务院认证认可监督管理部门会同国务院有关部门共同管理。因此,这项工作既涉及认证认可监管部门,也涉及数据安全监管部门。上一轮机构改革中,国家认证认可监督管理委员会职责已划入国家市场监督管理总局。因此,数据安全认证这项工作,由国家市场监管总局和国家互联网信息办公室共同负责[4]。

认证制度是目前国际通用的一种的第三方审核制度,由独立于被规制对象的专业机构依据标准和技术规范,通过调查取证、审核检验,对产品、服务或企业的管理体系、人员能力等合规情况进行评价与认定,是国家质量基础建设工程的基础项目之一。

从制度设计之初来看,在市场规模较大、需要开展专业化的检测检验工作的领域,行政监管通常难以实现全面、有效的覆盖[5]。在此背景之下,政府可以利用市场的力量,借助第三方机构的私人资源和专业优势开展认证工作,这样不仅可以弥补传统规制的不足,还可以提高专业水平、降低政府成本,同时也符合社会多元主体的利益期待[6]。

从历史发展过程来看,认证机制的制度演进体现出“自下而上”的社会共治理念。欧盟数据认证制度就经历了“自我声明—第三方认证—政府监管下数据认证”的演进过程。GDPR 第 42 条确立了“经批准的数据认证制度”,强调了公私合作的治理理念。数据监管当局全程监督并有权“干预”整个认证过程和认证结果,能够有效克服第三方认证的机制缺陷[7-8]。

从我国实践历程来看,认证制度首次出现在我国网络安全工作领域,源于 2004 年 10 月的《关于建立国家信息安全产品认证认可体系的通知》。在此之前,政府对社会的治理,更多地采用行政许可手段。而在规划国家信息安全产品认证认可体系建设时,我国便明确了政事分开、发挥认证认可制度作用的原则,凡可以通过认证认可解决的检测、评审,原则上不再设立行政许可。《数据安全法》《个人信息保护法》发布施行后,建立科学高效的数据安全治理体系的任务便被提上议事日程,认证认可制度成为重要的数据治理手段[4]。

《实施规则》的出台进一步完善了我国的数据安全治理体系,明确了数据安全认证的制度安排和规范依据。不过,认证工作的开展是一个动态治理的过程,需要多方主体的共同参与,既依靠国家网信

表 1 《实施规则》的制度设计

	个人信息保护认证	数据跨境传输认证
《个人信息保护法》	第六十二条:“国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作:(四)推进个人信息保护社会化服务体系建设,支持有关机构开展个人信息保护评估、认证服务。”	第三十八条:“个人信息处理者因业务等需要,确需向中华人民共和国境外提供个人信息的,应当具备下列条件之一:(二)按照国家网信部门的规定经专业机构进行个人信息保护认证。”
《认证认可条例》	第二条:“本条例所称认证,是指由认证机构证明产品、服务、管理体系符合……标准的合格评定活动。”	第二条:“本条例所称认证,是指由认证机构证明产品、服务、管理体系符合相关技术规范、相关技术规范的强制性要求的合格评定活动。”
《实施规则》	第二条:“个人信息处理者应当符合 GB/T 35273《信息安全技术 个人信息安全规范》的要求。”(国家标准)	第二条:“对于开展跨境处理活动的个人信息处理者,还应当符合 TC260-PG-20222A《个人信息跨境处理活动安全认证规范》的要求。”(技术规范)
制度设计	对于个人信息保护资格和能力的一般认证	对于数据跨境传输行为和场景的特殊认证
认证标志	PIP ABCD	PIP CB ABCD

部门的统筹协调，也有赖于社会认证机构的持续监督。将来，依据《个人信息保护法》和《认证认可条例》，我国的认证工作沿着《实施规则》的制度设计徐徐展开，在社会多元主体的协同共治下，个人信息保护格局也将朝着共建共治共享的治理样态发展。

3 《实施规则》的实践意义

本次《实施规则》的颁布及时回应了个人信息保护和数据跨境流动的需要，对于数字时代的网络强国建设具有重大意义，体现出我国构筑数据法治体系以及推进国家治理能力现代化所作出的努力。《实施规则》在扩展认证范围、促进数据出境、明晰侵权责任和推动国际互认方面具有重要的实践意义。

3.1 扩展认证范围

《实施规则》是我国首个关于个人信息保护认证的专项制度，也是我国建立的第三种数据安全认证制度。此前建立的两种数据安全认证制度分别是App安全认证以及数据安全管理认证。其中，2019年3月发布的《移动互联网应用程序(App)安全认证实施规则》属于产品认证；2022年6月份发布的《数据安全管理认证实施规则》侧重于数据安全管理能力。本次建立的个人信息保护认证制度是以认证认可为手段证明个人信息保护能力的一种认证方式，适用范围最广。比如某机构提供数据脱敏服务，可以为这种服务申请一张个人信息保护证书，从而表明具备服务能力；某机构是产品供应方，则可以为其产品申请一张个人信息处理过程符合有关标准的证书；各机构也可以为自身管理体系申请个人信息保护证书，当前很有影响力的ISO 27701隐私信息管理体系认证便属于此类[4]。

3.2 促进数据出境

个人信息保护认证是《个人信息保护法》第三十八条规定的数据出境合规体系的三条路径之一。《实施规则》的出台是落实《个人信息保护法》跨境数据流动认证路径的重要举措，及时填补了我国数据出境制度的实施细则空白。经过安全评估后出境和利用标准合同出境有着各自特殊的适用条件和应用场景，而个人信息保护认证作为并列的法定出境机制之一，能够和前两者产生有效的机制协调和衔接，共同助力数据跨境安全、自由流动，促进数据出境[9]。

3.3 明晰侵权责任

认证机构为认证申请人颁发的认证证书将给企业提供履行个人信息保护义务的合规证明，有助于明晰个人信息侵权责任。根据《个人信息保护法》第69条规定，“处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任”。也就是说，若个人信息处理者能够证明自身已履行个人信息保护义务，对于个人信息损害不存在过错，就能够降低个人信息侵权损害赔偿的法律责任，减少企业数据合规风险。更为清晰的权责边界也将为个人信息侵权诉讼的展开奠定基础，为数字时代的个人信息权益提供更好的保护。

3.4 推动国际互认

《实施规则》将《个人信息保护法》个人信息出境的相关规定具体化和可操作化，有利于和国际数据跨境流动认证制度相接轨，为未来相关认证的国际互认奠定基础。认证是全球个人信息保护实践当中的通行做法，国际上常见的个人信息保护相关认证包括以欧盟《通用数据保护条例》(GDPR_为基础确立的个人数据跨境传输认证，与GDPR相关的ePrivacy认证，美国的TRUSTe认证机制和亚太经济合作组织APEC框架下的CBPR认证，以及卢森堡数据保护机关新近推出包含个人数据跨境传输场景的GDPR-CARPA认证机制[9]。

目前，认证机制应用于数据出境管理仍缺少足够实践，国际上认证认可结果的互认存在困难[10]。严格意义上，欧盟尚未建立专用于数据出境的认证制度。鉴于数据安全的敏感性，我国当前对国际互认秉持审慎态度[11]。以我国现行法律法规为依据，比较借鉴域外权威认证机制建立个人信息保护认证，一方面有利于全面、及时回应跨境数据治理的全球态势；另一方面也有利于务实推动中国数据治理规则的国际化实现[9]。《实施规则》构建的中国个人信息保护认证规则同时助力中国企业跨越数字鸿沟，共同构建可信任的国际数据跨境流动体系，为企业更好地融入全球商贸环境、开展国际贸易保驾护航。

4 结论

《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》(简称“数据二十条”)指出，要推动个人信息保护认证制度的建立，加强企业数据合规体系建设，引导企业通过认证提升数据安全管理水平，有序培育合规认证的第三方专业服务机构，积极参与认证评估相关国际规则和数字技术标准制定，促进数据合规安全有序流通利用。此

次《实施规则》的颁布,标志着中国个人信息保护规则体系与数据合规制度建设又向前迈出了一步,数据跨境的第三条路也被缓缓打通。在《个人信息保护法》和《认证认可条例》制度支撑下,《实施规则》从认证范围、认证依据、认证程序、认证标识和认证责任等方面对个人信息保护认证规则进行了整体构建,在扩展认证范围、促进数据出境、明确侵权责任、推动国际互认等方面具有重要的实践意义。

个人信息保护体系与数据跨境流动机制下的认证制度仍有诸多问题亟待澄清,认证制度的真正落地仍待合理可行的实施细则的制定与公布。比如,正在编制中的国家标准《信息安全技术个人信息跨境传输认证要求》拟明确个人信息跨境提供的安全原则、安全要求和认证规则,该标准是否能够成为个人信息保护认证的第三个依据,暂未有定论。又如,作为数据跨境传输机制适用的个人信息保护认证制度对于全球数据治理而言仍是一个新问题——即便各国已相继构建与之适应的法律体系。这意味着,《实施规则》的颁布仅是一个开始,在如何发挥认证的实际作用方面,仍需对实施细则展开深入研究[4]。

就个人信息出境认证而言,《实施规则》《数据出境安全评估办法》《个人信息出境标准合同规定(征求意见稿)》共同构成了《个人信息保护法》第三十八条规定的个人信息跨境传输的具体落地规则。三条合规路径原本在法律设计上是择其一即可使个人信息出境,但实践中考虑到某些重要个人信息的公共属性等,有可能使得这三种路径需重复适用才能满足合规要求。就个人信息保护认证制度体系化和实施合规性而言,认证机制的有效推行不仅需要满足《实施规则》的要求,还需要协调《实施规则》与其上位法《个人信息保护法》和《认证认可条例》之间的关系,同时需要满足《实施规则》所规定的相关技术规范、国家标准以及认证机构制定的实施细则的要求,实践层面的法律合规面临着相当大的挑战,个人信息保护认证规则体系化仍任重道远。

从合作规制理论视角来看,构建法治化的个人信息保护认证体制机制,不仅是保障数据安全的现实需要,而且是弥补数字时代政府规制缺陷的迫切需求。作为去中心化的第三方规制,数据安全认证是一种全新理念。第三方规制同政府规制、自我规制一道共同构成了完善的规制法体系。在“放管服”改革深入推进和国家治理能力现代化的背景下,需要政府、互联网企业、数据安全认证机构、网络用户、社会公众等多方主体开展公私合作治理,相互取长补短,协同完成保障数据安全并促进数据高效流通利用的公共任务[3]。作为共同治理的方案之一,个人信息保护认证规则在推动创新的同时,也向市场主体提供相应信息,使得企业根据认证规则锚定的基准向消费者展示其个人信息保护水平[12],从而促进数据可信流通利用体系建设,为市场交易提供低成本、高效率、可信赖的流通环境,在安全可信、包容创新、公平开放、监管有效的多方主体合作共治环境下推动数据要素更好地发挥价值。

参考文献

[1] 张凌寒.论数据出境安全评估的法律性质与救济路径[J].行政法学研究,2023(1):45-61.
[2] 赵精武.论数据出境评估、合同与认证规则的体系化[J].行政法学研究,2023(1):78-94.
[3] 刘权.数据安全认证:个人信息保护的第三方规制[J].法学评论,2022,40(1):118-130.
[4] 左晓栋.顺势而为——谈我国个人信息保护认证制度的设计[J].中国信息安全,2022(12).
[5] 孔祥稳.论个人信息保护的行政规制路径[J].行政法学研究,2022(1):131-145.
[6] 高秦伟.论政府规制中的第三方审核[J].法商研究,2016,33(6):24-33.
[7] 张继红.数据认证:模式选择与应用规范[J].中国政法大学学报,2021(2):64-77.
[8] 张继红.经设计的个人信息保护机制研究[J].法律科学(西北政法大学学报),2022,40(3):31-43.
[9] 吴沈括.个人信息保护认证的制度意义与实践价值[J].中国信息安全,2022(12).
[10] Hogan Lovells.Memorandum on building a common EU and UK Binding Corporate Rules(BCR) framework[EB/OL].[2022-12-12].https://www.privacylaws.com/events-gateway/events/bcr2022/.
[11] 许皖秀,左晓栋.把握我国实施个人信息出境认证的几个要点[J].中国信息安全,2022(12).
[12] 洪延青.个人信息保护认证:实现个人信息保护共同治理的方案[J].中国信息安全,2022(12).

(收稿日期:2023-01-05)

作者简介:

刘懿阳(1998-),男,硕士研究生,主要研究方向:数据法学、行政法学。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部