T/ZS 0270-2022《数据知识产权质押服务规程》团体标准解读

——基于团体标准与法律的互动

龙佳芩

（中国计量大学）

摘　要：《数据知识产权质押服务规程》作为全国首个数据知识产权质押团体标准，也是首次从标准层面支持了数据知识产权。在法律层面，数据知识产权概念尚未明确提出，但数据知识产权质押所涉及的个人信息保护与处理、企业数据保护与利用、国家数据安全与发展在现有法律中已有规定。团体标准与法律具有互动性，数据知识产权质押团体标准的制定和实施有利于倒推数据知识产权及其质押的专门立法，同时，该团体标准也受现有法律约束，对该团体标准的解读必须与所涉现有法律保持一致。

关键词：数据知识产权，质押融资，团体标准，数据法规

DOI编码：10.3969/j.issn.1674-5698.2023.03.017

Interpretation of Association Standard, *T/ZS 0270-2022 Data intellectual property pledge service regulations* —— Based on the Interaction of Association Standards with the Law

LONG Jia-qin

（China Jiliang University）

Abstract: As the first data intellectual property pledge association standard in China, T/ZS 0270-2022, Data intellectual property pledge service regulations supports data intellectual property rights from the standard level for the first time. Although the concept of data intellectual property rights has not yet been clearly put forward at the legal level, the protection and processing of personal information, the protection and utilization of enterprise data data, and the development of national data security involved in data intellectual property pledges have been stipulated in existing laws. Standards and laws are interactive. The implementation of the association standard can promote the special legislation of data intellectual property rights and its pledge, and the interpretation of the association standard for data intellectual property pledge must be consistent with the relevant existing laws.

Keywords: data intellectual property, pledge financing, association standards, data regulations

---

基金项目：本文系2021年国家社会科学基金一般项目“网络数据知识产权保护与治理研究”（项目编号：21BFX100）、2022年度互联网法治重点研究课题“我国网络数据知识产权治理与保护研究”研究成果之一。

作者简介：龙佳芩，硕士研究生，研究方向为知识产权法、标准化法。

1 引言

2022年3月16日，浙江省产品与工程标准化协会发布了全国首个数据知识产权质押团体标准《数据知识产权质押服务规程》，该标准由浙江省知识产权研究与服务中心、杭州高新技术产业开发区（滨江）市场监督管理局、浙江大数据交易中心有限公司等多家单位共同起草，于3月30日正式实施。该标准的制定响应了数字经济发展下知识产权强国战略、数字经济发展战略的要求——我国《知识产权强国建设纲要（2021–2035）》和《“十四五”国家知识产权保护和运用规划》均提出要构建数据知识产权规则，鼓励开展各类知识产权质押融资。该标准规范了数据知识产权质押服务中的采集、脱敏、存证、存储、评估、融资、处置等各环节，为数据质押流程中存在的数据权属、数据价值、数据安全问题的解决提供了有效途径，促进了市场主体对数据资产转化的认可。在该标准的应用下，各企业、银行、大数据交易中心等主体逐渐认可并使用企业数据融资新方式，如：杭州高新区（滨江）已有5家企业进行了数据知识产权质押，累计获融资两千万元。

然而，由于数据知识产权概念尚未被法律明确认可，该团体标准在具体解读与应用过程中必须考虑与法律的衔接、互动问题。一方面，该团体标准相对于现有立法具有开创性，一定程度能够起到立法推动作用。我国法律尚未明确规定数据能否纳入知识产权，但数据通过一定技术处理后能够具有市场价值，存在法律可保护的财产性利益是立法和司法实践已经确定的。利用团体标准对数据知识产权及其质押先行确定、试点实践，既能够有效、灵活、及时响应数据创新要求、对接数字经济市场需求，又能在较大范围实验数据知识产权及其质押的可行性以倒推相关立法。另一方面，虽然法律目前尚未对数据知识产权有所定义，但对与其相关的信息、知识产权、质押等概念都有具体规定，该团体标准的解读和应用必须与现有相关规定衔接、协调。该团体标准本身的制定就依据了大量的现有涉数据法律规范，其内容及应用必须遵循现有涉及数据处理的法律规范。数据内容涉及到个人信息、企业信息、政府信息，现有法律如：《民法典》《个人信息保护法》《数据安全法》《网络安全法》《著作权法》《反不正当竞争法》等，对于个人信息安全与处理、企业数据的保护与利用、国家数据的安全与发展都有相关规范，数据知识产权质押必然涉及到个人信息、企业数据、国家数据的保护与利用问题，故数据知识产权质押团体标准的内容也不得违背现有的涉数据保护与利用法律规范。

2 核心定义的法律背景

《数据知识产权质押服务规程》关于数据、数据知识产权、质押三大核心词的定义均紧密联系现有法律法规。首先，关于数据的定义，2021年出台的《数据安全法》首次从法律层面对此做出明文规定，本团体标准直接援用该定义：一方面，从数据存在形式角度，该定义范围较大，规定数据包括电子或非电子形式；从内容角度，该定义强调数据和信息的关系，规定数据是对信息的记录。其次，关于数据知识产权，虽然法律法规尚未有数据知识产权的明确定义，但本团体标准强调只有加工后形成的数据产品和服务才具有财产权益，单纯收集、存储的数据并不在知识产权范围内，正是对知识产权现有法律法规的呼应——无论是《著作权法》对作品要求独创性，还是《专利法》对发明创造要求新颖性，均体现知识产权法所认可的知识产权客体必须具备达到一定程度的智力投入，而单纯通过各种方法收集、存储数据尚未达到该程度，故标准将其排除在数据知识产权范围外。最后，关于质押的定义，《民法典》对知识产权中财产权出质有明确规定，本团体标准与《民法典》关于质押的规定保持相当程度的一致性：在质押效果上，与《民法典》担保债权效果一致，当债务不履行时产生优先受偿权；在质押方式上，规定为“将数据知识产权移交给债权人占有”，且在标准第十章“融资”10.3规定数据知识产权质权人应当与出质人签订质押合同，可见，标准对数据知识产权质权设立采取的是“书面质押合同+质押登记”要件模式，这与《民法典》第444条规定的知识产权中财产权出质应当办理出质登记的要求以及《民法典》体系化规定的权利质权应当订立书面质押合同的要求保持一致。

3　核心技术内容的解读

《数据知识产权质押服务规程》包括范围、规范性文件、术语和定义、基本要求和七大质押环节5个部分，重点内容是对于数据采集、脱敏、存证、存储、评估、融资、处置七大数据知识产权质押基本流程的具体规定（如图1所示），核心技术内容主要包括源数据采集、数据脱敏、数据哈希存证以及数字信封加密存储，该4项核心技术内容均应当基于法律与标准结合的方式进行分析和解读。

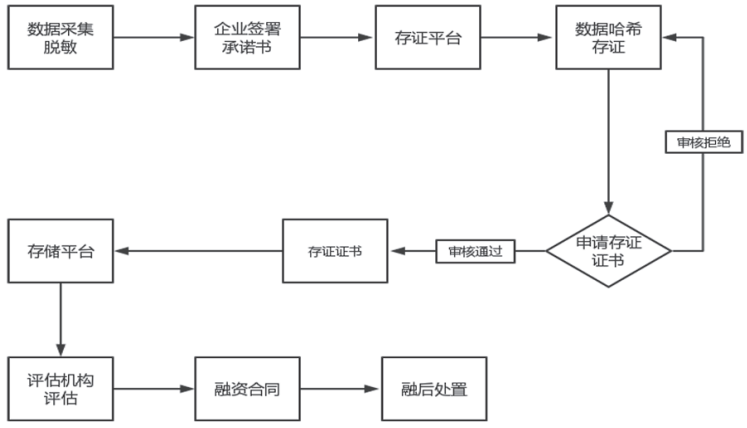

图1　数据知识产权质押流程

3.1　源数据采集

数据采集方式包括源数据采集和非源数据采集，源数据又称原始数据，是终端用户所产生的、未经过处理的数据，非源数据就是经过处理后的数据。当前，由于数据加工尚处于新兴阶段且对已加工数据的再次利用存在不正当竞争纠纷争议，数据知识产权所涉数据的采集通过源数据采集更可取，具体方式包括：端上数据采用埋点方式采集；物理数据通过传感器来进行自动识别和数据提取；主观性数据通过用户调研或访谈的方式收集；其他平台数据通过其他平台提供的规范API接口服务采集；数据库数据采用库库对接的方式采集。

上述几种源数据采集方式都直接针对用户个人信息，直接关系用户个人信息权益、隐私权；虽然该团体标准在“采集”一章主要详细规定的是上述采集方式，没有明确针对数据采集与个人信息保护进行规定，但通过上述采集方式进行数据采集时，也需要遵守关于处理数据采集与个人信息保护利益冲突的规范。该团体标准在“采集”一章5.6条明确规定数据采集过程要符合GB/T 35273的规定，GB/T 35273规定了个人信息的收集必须遵守合法性原则、最小必要性原则、个人信息保护政策（强调个人信息处理者的告知义务）、自愿性原则和授权同意规则，这5项基本规则是《民法典》《个人信息保护法》中个人信息权益保护规范的重要内容，GB/T 35273在操作标准层面将其具化、贯彻（见表1），前三者从采集者（经营者）角度出发，后两者从被采集者（用户）角度出发。根据表格，该团体标准仅对最小必要性原则内容有所涉及，其他4项基本规则并未列明，但在具体采集数据时是必然要遵守5项基本规则，合理平衡数据采集者与个人信息主体的两方利益。

3.2　数据脱敏

数据采集环节主要强调的是与个人信息保护之间的协调，但采集后形成的海量数据集与国家数据安全、企业数据利益保护的协调也凸显出来。数据采集后的数据脱敏不仅是针对公开后极易导致个人名誉受损或歧视性待遇等的个人信息，还针对公开后会损害国家利益、商业利益的信息。

我国对于敏感信息的概念尚未统一，现对于敏感信息的规定都集中在个人信息领域，但实质上对于敏感信息不应当仅限于个人信息范围。GB/T 35273–2020中3.2条对“个人敏感信息”进行了概括式定义，并通过附录进行类型列举，《个人信息保护法》一脉相承，在第二十八条通过“概括式+列举式”方式规定了“敏感个人信息”，个人敏感信息成为我国学者重要的研究对象，但在相关文献中常常将敏感信息混同于个人敏感信息甚至隐私信息。从语义学的角度来看，“个人敏感信息”是个人信息领域的“敏感信息”，其范围应当比“敏感信息”的范围小。从比较法的角度来看，欧美都对敏感信息进行了概念界定（见表2），均认为敏感信息包括但不限于公开后会不利于自然人人身、财产安全的个人信息[1]。从现有文献来看，我国学者对“敏感信息”的内涵和外延也并未限定在个人信息领域，如有学者基于相关裁判事例的考察研究政府信息公开中的

“敏感信息”界定，认为政府信息公开领域的“敏感信息”为不符合国家秘密标准、但公开后可能会影响到行政机关正常执法的政府信息[2]。

综上，敏感信息是指被泄露或不当披露后会对信息主体产生某些不利影响，包括但不限于个人隐私、商业秘密等信息，但依法规定的公开信息和保密信息除外。

敏感信息的泄露将会对个人利益、企业利益甚至社会及国家安全造成巨大威胁，通过数据脱敏技术有利于解决数据安全与数据利用的冲突问题。数据脱敏技术通过采取一定方法消除所采集的原始环境数据含有的敏感信息部分内容，并且保留下目标环境业务所需数据部分内容，其既能够保障数据中的敏感数据不被泄露又能够保证数据可用性的特性[3]，有利于平衡数据涉及的多方利益。该团体标准在“脱敏”一章的6.2条也明确规定，脱敏后的数据要符合《民法典》《个人信息保护法》《数据安全法》《网络安全法》《关键信息基础设施安全保护条例》等法律法规，不得侵犯任何国家、个人和实体的合法权利，这也是强调利用数据脱敏技术，在发挥数据价值的同时，保障数据所涉的其他主体的合法权利。

表1 个人信息收集基本规则

内容 / 名称	采集者（经营者）角度： 合法性、最小必要性、告知义务	被采集者（用户）角度： 授权同意、自愿性
民法典	第1035条第1款规定了处理个人信息应当遵循合法、正当、必要原则，不得过度处理	第1035条第1款第1项以及第1036条规定了授权同意规则及其3种例外：法律、行政法规另有规定的，合理处理该自然人自行公开或者其他已经合法公开的信息，为维护公共利益或该自然人合法权益合理实施的其他行为
个人信息保护法	第5条规定处理个人信息应当遵循合法、正当、必要和诚信原则；第6条进一步规定了最小必要原则。第17到第18条规定了个人信息处理者的告知义务及其例外：原则上处理个人信息前是需要以显著方式、清晰易懂语言真实、准确、完整、及时地向个人告知的，但法律、行政法规规定应当保密或者不需要告知的情形除外，紧急情况无法及时告知的应当在紧急情况消除后及时告知	第13到第16条规定了授权同意规则及其6种例外：原则上处理个人信息应当取得个人同意，但为订立、履行合同所必需，为履行法定职责或义务所必需，为应对突发公共卫生事件或紧急情况下为保护自然人生命健康和财产安全所必需，为公共利益实施新闻报道，合理处理个人自行公开或者其他已经合法公开的个人信息，法律、行政法规规定的其他情形，这6种情形是不需要取得个人同意的
GB/T 35273–2020	本国家标准第5章专章规定了个人信息的收集，其中5.1规定了合法性原则，5.2规定了最小必要原则，5.5规定了个人信息控制者应真实、准确、完整告知个人信息主体	5.3规定了自愿性原则，5.4规定了授权同意规则，5.6规定了授权同意的11种例外包括：为履行法定义务的，与国家安全、国防安全直接相关的，与公共安全、公共卫生、重大公共利益直接相关的，与刑事侦查、审判等直接相关的，为保护自然人生命、财产等重大合法权益的，个人自行公开的个人信息，合法公开披露的个人信息，维护产品或服务运行所必需，新闻单位为新闻报道所必需，学术研究机构为公共利益或学术研究所必需
T/ZS0270–2022	本团体标准“采集”一章第5.5涉及到最小必要原则，即数据采集内容应与企业经营范围具备直接相关性	

表2 国外敏感信息定义

国家	规范	敏感信息定义
美国	1987年计算机安全法案（CSA)	将“敏感信息”（sensitive information）定义为一旦丢失、滥用、未授权访问或修改将会对国家利益、联邦计划的执行或个人隐私产生不利影响的任何信息，但不属于总统令或国会法案规定的为维护国防或外交政策利益而需要保密的信息，故也称“受控非密信息”
	2010年13556号总统令	涉及个人隐私、安全、专属的商业利益和执法调查等的信息都属于受控非密信息的范畴
欧盟	2015 年3月发布的关于欧盟委员会安全的2015 /443决议	将敏感的非保密信息界定为，由于生效中的条约或法案的规定，或者由于其自身的敏感性，欧盟必须加以保护的信息或资料，包括但不限于工作秘密; 公开后会影响公共利益、个人隐私、商业利益、法律程序和建议、审查调查和审计目的的信息; 个人数据
英国	《处理公务类信息: 确保安全分类更简便、清晰和安全》的指南	列举了“公务敏感信息”，包括敏感的公司信息，非常敏感的个人信息，关于有争议和非常敏感事项的政策研制和给领导的建议，商业或市场敏感信息，可能扰乱执法或破坏司法案件的调查和民事或刑事诉讼信息，敏感的外交事务或国际谈判

数据脱敏主要包括三大基本过程，分别是脱敏对象识别、脱敏方案执行以及脱敏效果对比（如图2所示）。脱敏技术仅针对敏感信息进行操作，首先就必须从采集所得数据中确定敏感数据的范围，利用自然语言处理、知识库、算法规则中的特征密度计算、特征词提取、命名实体识别等方式智能识别出需要进行脱敏的对象[4]。常用的具体脱敏方案有仿真、数据替换、加密、加减值、数据截取以及数据混淆等，在识别出敏感数据后，数据处理者根据实际需求针对脱敏对象选择并执行脱敏方案。具体脱敏方案执行完毕后，显示脱敏前后的数据进行对比，检测实际脱敏效果，根据实际效果选择是否重新脱敏或叠加使用其他脱敏方案，当然仅对外公开完成脱敏后的数据。

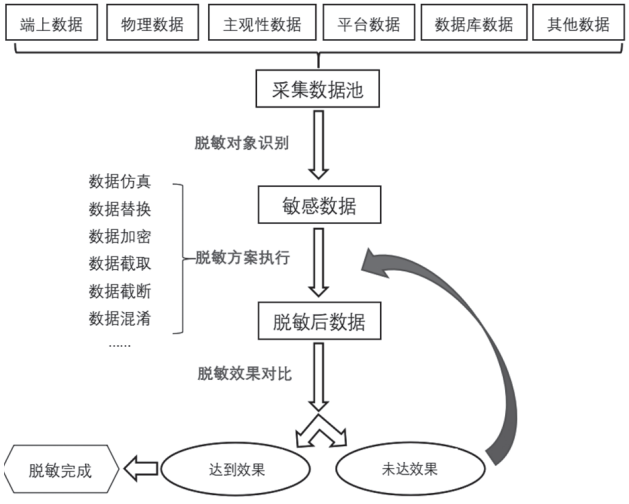

图2 数据脱敏基本过程

3.3 数据哈希存证

脱敏后的数据将上传至浙江知识产权区块链公共存证平台，并且同步到市场监督管理局、杭州互联网法院等机构单位。该存证采用哈希函数（Hash Function）运算技术，有利于检测后续使用时数据的真实性、完整性。哈希存证技术将脱敏后数据压缩成短的、长度固定的字母和数字组成的字符串，即哈希值[5]，由于每个中文、每个字母甚至每个标点的改变都会影响哈希值发生变化，故只要对应哈希值不同，则表明原始输入的数据也不同[6]。通过哈希存证技术，一方面有利于保证数据在后续使用中的真实性、完整性，一方面也有利于防止数据篡改。

本团体标准7.4条规定，数据哈希存证如满足审核条件，将颁发存证证书，那么，该存证证书的效力是什么？一方面，该团体标准是浙江省产品与工程标准化协会发布的，是市场主体根据数字化环境下所产生的新的标准需求所制定的，不具有行政性，虽然具有很强的适应性和灵活性，但缺乏社会普遍认可和采信。另一方面，数据知识产权尚未在法律层面得到明确认可，对于其数据知识产权是同著作权一样遵循自动取得原则——自完成采集、脱敏后公开即自动取得，还是同专利或商标一样必须经过专门行政程序进行注册登记确权，尚无定论，在相关涉数据纠纷中对于数据产品法益主体的证明缺乏证据材料，但目前学术理论界、司法实践界对加工数据具有受法律保护的利益几乎都是认可的，采纳认证证书作为法益主体证明材料不失为一种可取之法。2018年9月，最高人民法院《关于互联网审理案件若干问题的规定》中第11条首次对以区块链技术进行存证的电子数据真实性作出明确规定，由此区块链存证的法律效力得到确认。2021年4月，成都某公司起诉广州某公司未经许可在其运营的音乐平台上向公众提供涉案歌曲的在线播放和下载服务，该案中法院采信了由第三方版权服务平台出具的《区块链存证证书》作为有效权属证据[7]。《浙江省知识产权区块链存证平台数据资产存证证书》运用区块链技术取证、存证，具有可信且不可篡改特征，同时该存证在上传至存证平台的同时已同步上传至杭州互联网法院，平台所有数据内容都可通过法院平台查询、核验，若无相反证据推翻其真实性，应予确认并采信其真实性，以有效保障数据资产主体的合法权益。

3.4 数据信封加密存储

数据哈希存证与数字信封加密存储都是在数据保管阶段所采取的措施，前者主要针对哈希值与数据资产的“数–数”唯一性，后者主要针对数据知识产权主体与数据资产的“人–数”唯一性。数字信封综合利用了对称加密技术与非对称加密技术的优势[8]，其功能类似于纸质信封，纸质信封保证只有收件人才能阅读信的内容，数字信封采用成熟的密码技术保证只有授权方才能获取数据资产的内容[9]，即数据资产主体通过加密算法将数据资产进行加密封锁，并获得唯一私钥，数据安全存储平台可查看数据的前十条概述，对于其他数据，无私钥

或企业授权，任何主体都无权查看。

将数据资产进行数字信封加密，赋予数据资产主体唯一密钥，这是知识产权排他性的体现，也是在促进数据资产流通的同时对数据资产主体的合法权益的保护。基于劳动价值理论、创新激励理论等原理证成数据资产主体对所加工数据享有的可受法律保护的权益，将满足要求的数据纳入知识产权保护框架，该权益客体具有无形性，通过一定技术手段来补强对其的排他性保护是数字化时代的应然之义。

4 结 论

团体标准属于市场型标准，直接被法律援引的功能不大，但能够在立法尚未对新兴事物做出明确规定前迅速地做出反应，为后续立法铺路。由于公信力等原因，法律通常只援引政府型标准而不会援引团体标准这种市场型标准[10]，但无论相对于政府型标准还是法律，团体标准的制定更加灵活、高效，稳定性要求程度更低。数据知识产权质押是在数据价值深入发掘、数据利用技术不断提高的背景下产生的，符合数字经济发展和市场经济发展的要求，在尚无法律法规以及政府型标准对数据知识产权质押进行规定时，通过市场主体制定的团体标准对该规范空白进行填充，有利于适应新时代下的市场需要，对市场活动实践起到指导、规范作用，在市场实践中不断探索、明晰数据知识产权的构成标准及其质押的流程标准，以科学、技术和经验的综合成果为基础为数据知识产权入法奠基[11]。

法律是团体标准的制定依据，对团体标准的制定、理解、适用都应当避免与法律规定出现矛盾和抵触[12]。根据数据知识产权质押团体标准，整个质押流程包括七大基础环节，在数据流通环节中，涉及的不只是数据资产主体一方的利益，还涉及到被采集数据主体、国家等多方利益，对于该团体标准的解读和技术实施必须结合《民法典》《个人信息保护法》《网络安全法》等多部法律规定，保证各方利益的协调和平衡。同时，标准应充分把握数据与知识产权的相同点和不同点，针对相同点，数据知识产权质押团体标准内容本身应当与现有知识产权法律体系以及知识产权质押法律规定相符，可以直接通过现有规范内容进行解读；针对不同点，应当结合数据特性，在不与现有规范发生冲突的情况下，可以进行有利于数据知识产权质押的创造性解读。

参考文献

[1] 于洁,栗琳. 英国敏感信息管理及对我国的启示[J]. 情报理论与实践, 2021,44(7):184–190.

[2] 赵剑文. 政府信息公开中“敏感信息”的界定——基于相关裁判事例的考察[J]. 太原理工大学学报(社会科学版), 2021,39(5):39–47.

[3] 唐迪,顾健,张凯悦,等. 数据脱敏技术发展趋势[J]. 保密科学技术, 2021(4):4–11.

[4] 张宁池,朱小娟,张宇,等. 互联网商业模式下大数据脱敏方法的探究与研究[J]. 行业应用与交流, 2021,40(1):150–154.

[5] 刘颖. 电子银行风险法律问题研究[M]. 北京: 法律出版社, 2016:45.

[6] 罗恬漩. 民事证据证明视野下的区块链存证[J].法律科学(西北政法大学学报), 2020(6):65–72.

[7] 王婧. 法院采信存证证书作为有效权属证据[N]. 法治日报, 2021–10–12(010):1–3.

[8] Prasanna S,Gobi M. Performance analysis of distinct secured authentication protocols used in the resource constrained platform[J]. ICTACT Journal on Communication Technology,2014,5(1) : 904–906.

[9] 张小红,涂平生. CP–ABE与数字信封融合技术的云存储安全模型设计与实现[J]. 计算机应用与软件, 2016,33(9):313–319.

[10] 周宇. 法律引用团体标准规则的探索[J].电子知识产权, 2022(3):4–19.

[11] 柳经纬. 论标准对法律的支撑作用[J]. 厦门大学学报(哲学社会科学版), 2020(6):152–162.

[12] 王雅君. 刍议标准与法律的交互关系[J]. 中国质量与标准导报, 2021(2):65–67.