从保密到安全：数据销毁义务的理论逻辑与制度建构

赵精武*

目次

摘要 我国现行立法规定了自然人有请求信息处理者删除个人信息的权利，但这并不等于承认数据生命周期的最后环节是“删除”，因为“删除权”是“信息处理的合法性与必要性基础丧失”的必然结果，而“数据销毁”才是“数据归于消灭”的处理流程末端。数据销毁义务的理论基础在于信息保密方式的扩张，即从维持信息保密状态转向维持数据安全风险的可控性。在数据安全风险评估过程中，倘若义务主体无法保障暂时不使用的重要数据和个人信息处于安全状态，则应当采取适当的数据销毁范式降低数据泄露或非法复原的安全风险。在未来立法活动中，我国应当明确数据销毁义务的义务主体、销毁方式和销毁范围等具体制度内容，完成数据安全立法的“最后闭环”。

关键词 数据销毁义务 删除权 保密方式 数据安全风险评估 风险控制

* 北京航空航天大学法学院助理教授、法学博士。本文系国家广播电视总局部级社会科学研究项目“广电行业法治和治理体系建设研究”（项目编号：GDT2120）及中国科学技术协会2021年“高端科技创新智库项目——智能算法在社会治理中的挑战、机遇与发展对策研究”（项目编号：2021ZZZLFZB1207065）的阶段性研究成果。

一、问题的提出

为应对网络平台超范围收集个人信息、在后台私自收集个人信息、擅自向第三方主体共享个人信息等问题，《网络安全法》《民法典》《数据安全法》《个人信息保护法》等法律相继明确了信息处理者在信息收集、加工、更新、存储、删除等环节的个人信息保护义务和数据安全保障义务，〔1〕但针对数据生命周期的最后一个环节“消灭”，立法者并未提供足够明确且直接的义务性条款。虽然现行立法已经明文规定了自然人享有删除其个人信息的权利，而有关“删除个人信息的实际范围”“删除义务的履行主体是否包含业务合作第三方”“删除个人信息应当满足何种一般性要求”等具体问题并未得到真正解决。更重要的是，“删除个人信息”在名义上虽以权利性规范的形式得到立法者的认可，实践中自然人在请求信息处理者删除个人信息之后，却无从确认信息处理者究竟是否真正彻底删除个人信息以及删除信息的类型和范围，更遑论业务合作第三方主体所获取的个人信息是否已经被删除，法益保护目标的实现与否在很大程度上依赖于信息处理者是否真正履行相应的给付行为。国内外主流的 APP 在其隐私政策中明确了用户行使删除个人信息权利的适用条件和具体行使方式，但均是以自然人主动申请为前提，并没有详细提及用户如何自行注销账号或者 APP 运营者将如何为用户删除其个人信息。〔2〕由此可见，至少在商业实践层面，尚未形成个人信息删除的行业标准和商业惯例，其原因也很好理解：在“流量为王”的时代，网络平台活跃用户数量已经与企业经营状况和营利方式直接挂钩，账号信息和个人信息的删除势必会影响到信息处理者的经济效益，在现行立法尚未细化“删除权”具体内容的情况下，采用相对模糊的隐私声明条款更符合自身的商业利益。在此种立法背景下，不少学者开始尝试细化删除权的具体规则，或是主张以比例原则和公平原则作为删除权客体范围的认定标准，〔3〕又或是将删除范围解释为“信息处理的相关性和必要性不复存在”的个人信息，〔4〕抑或是基于删除权与被遗忘权的比较而将删除范围限定为“被自动化处理的、无意识生成的个人信息和数据”。〔5〕学理上的解释方案似乎正在为数据生命周期的末尾环节填补上最后的立法空白，但问题的核心却在于：“删除”真的是个人信息保护体系的最后一环吗？或者说，“删除”是否真的意味着个人信息归于消灭？

在《辞海》中，“删”即指消除，“除”即指去掉，若将其置于个人信息保护语境下，“删除”所对应的技术措施显然只要满足个人信息已被去除的效果即可，而销毁意味着数据生命的终结，二者的语义涵摄范围存在差异；同时，在《个人信息保护法》中，删除个人信息的适用情形是以信息处理者丧失合法处理个人信息的正当性基础为前提，删除的目的是满足“合法正当”之原则，而非直接对

〔1〕 如《网络安全法》第 43 条规定：“个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息。”《民法典》第 1037 条第 2 款规定：“自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权请求信息处理者及时删除。”

〔2〕 有学者在统计国内外 20 款 APP 隐私政策时发现，国内外 APP 运营者在隐私政策中有关个人信息删除权的内容较为简单，未能向用户提供明确具体的操作指引，且常常掺杂在冗长的文字表述中，难以轻易理解删除的方式和途径。参见徐磊：《个人信息删除权的实践样态与优化策略——以移动应用程序隐私政策文本为视角》，载《情报理论与实践》2021 年第 4 期，第 89—98 页。

〔3〕 参见余筱兰：《民法典编纂视角下信息删除权建构》，载《政治与法律》2018 年第 4 期，第 26—37 页。

〔4〕 参见满洪杰：《被遗忘权的解析与构建：作为网络时代信息价值纠偏机制的研究》，载《法制与社会发展》2018 年第 2 期，第 199—217 页。

〔5〕 参见王琰、赵婕：《大数据时代被遗忘权的现实逻辑与本土建构》，载《南昌大学学报（人文社会科学版）》2020 年第 6 期，第 103—111 页。

应数据生命周期的最后环节。2021年9月30日，工信部发布了《工业和信息化领域数据安全管理办法（试行）》，首次提出“数据销毁”的概念，其数据生命周期也未沿用现行立法常见的“收集、存储、使用、加工、传输、提供、公开、删除等”，而是表述为“数据收集、存储、加工、传输、提供、公开、销毁、跨境、承接、委托处理等”。事实上，不论信息处理者如何设计数据处理流程，都始终无法回避数据的“死亡问题”，数据销毁并非处于信息处理者经营自主权的范围之内，其是数据安全流程的必要环节，能够对大数据时代下信息主体所面临的权利问题做出积极的回应〔6〕。故而前述立法表述的变化也将新的数据安全问题置于立法者眼前：如何建构数据销毁义务？一方面，数据销毁义务的建构问题关系到个人信息保护义务内容的体系化，在明确数据销毁义务具体内容的同时也是在划定删除权的行使空间和保护标准；另一方面，数据销毁义务的建构问题亦是数据安全风险评估机制的重要内容之一，因为对于部分暂时不使用的数据，企业可以通过数据安全评估机制来确定是否继续保存，倘若安全风险较高且技术能力薄弱，企业则可以依照安全技术标准直接予以销毁。因此，在回答数据销毁义务的建构问题的过程中，还需要回答三个子问题：第一，在“删除”与“销毁”含义分离的前提下，数据销毁义务的理论基础应当如何理解？第二，数据销毁义务的适用条件是否仅限于个人信息保护？其适用情形、销毁方式、销毁范围等具体内容又当如何设计？第三，针对死者的个人信息、去中心化技术方案的数据处理等特殊场景，数据销毁义务是否存在例外情形或特殊规则？

二、数据销毁义务的理论基础

（一）数据销毁的技术方案与业务类型

在文义解释层面，《个人信息保护法》所规定的“删除权”通常被理解为从信息处理者的数据库中删除已经“过期”或自然人不愿再留存的个人信息，即达到了数据销毁的效果；但是在技术方案层面，“删除”和“销毁”并不是两个完全等同的概念。〔7〕数据销毁与数据删除具有典型的技术语境属性，数据销毁通常被视为数据安全业务流程的最后环节，直接目的是避免第三人通过数据复原、存储介质窃取等方式重新复原业已销毁的数据；而数据删除并不是数据安全业务流程的必备环节，而是数据处理者根据法定义务、业务需求等多种因素选择不再对外公开特定数据。现有的数据销毁技术方案大致可以分为两大类：一类是硬销毁，即直接对数据存储介质进行销毁，如直接对硬盘施加强磁场进行消磁，促使硬盘不再具备数据记录功能；另一类则是软销毁（也被称为逻辑销毁），即通过数据覆盖录入等操作方法进行数据销毁或数据擦除，如为了节省存储介质的开销，以最新的数据直接替换之前存储的数据，使其不再具有恢复可能性。但是这些数据销毁方式并不都是信息处理者的最佳选择，考虑到技术难度、经济成本以及销毁效率等因素，数据销毁行业常用的数据销毁方式主要包括覆写法、消磁法、剪碎法和焚毁法，〔8〕以便能够在短时间内彻底销毁留存的业务数据。需要说明的是，信息处理者自主销毁数据的直接动力并不是《个人信息保护

〔6〕 参见唐林垚：《〈个人信息保护法〉语境下“免受算法支配权”的实现路径与内涵辨析》，载《湖北社会科学》2021年第3期，第134—142页。

〔7〕 在团体标准《个人信息处理法律合规性评估指引》的“第1部分：概述和术语”中，3.4.1“个人信息处理”明确提及“个人信息处理的示例包括但不限于采集、存储、修改、检索、咨询、披露、匿名化、假名化、传播或以其他方式提供、删除或销毁”。该标准并没有选择将“删除”或“销毁”视为同一个技术操作活动。

〔8〕 参见森一科技：《数据销毁的几种方法》，载简书网，https://www.jianshu.com/p/c96a4e90658a，2021年9月30日访问。

法》所要求的“删除权”，而是出于提升数据质量和满足大数据应用的需求。在数据大爆炸的时代，数据质量的商业价值远高于数据数量，信息处理者需要在有限的存储空间内进行数据筛选，所以销毁的对象往往是业务活动中产生的无用数据、无效数据，而非涉及业务核心的用户个人信息。虽然我国国内尚未形成有关数据销毁的国家标准，但在该领域常以美国国防部的 DOD 5220.22 技术标准作为参考，〔9〕而该标准对数据清除（data clearing）和数据销毁（data sanitization）有着不同的界定方式。数据清除是指在重复使用存储介质前，需要彻底删除存储介质中的数据，且删除数据之前，存储介质所处环境也应当满足相当的安全保护等级，这是为了避免通过内存、缓冲区以及其他可重复使用内存读取先前存储的数据；而数据销毁则是由于存储介质所处环境无法提供相当的安全保护等级，需要对数据以及相关程序进行彻底销毁，两个概念的实质性差异在于是否需要对数据及其环境进行彻底的清理和销毁。而国际数据销毁联盟（IDSC）则将数据销毁定义为“永久且不可逆地删除或销毁存储在存储设备上的数据且使其不可恢复的过程”，主要包括物理销毁、加密擦除和数据擦除三种方式（参见下表 1）。〔10〕 在比利时的数据保护机构（L'APD）2021 年 3 月发布的《关于数据销毁和数据介质销毁技术的建议》（Recommendation on data sanitisation and data medium destruction techniques）〔11〕中，“数据销毁”的技术方案与数据保密要求密切相关，按照秘密、机密和绝密的分类标准（参见下表 2），“数据销毁”分别对应着数据清除（clear）、数据擦除（purge）和数据销毁（destroy）。由此可见，技术层面的“数据销毁”概念在本质上更关注的是这些业已清除的数据是否具备再次被获取或复原的可能性，如比利时监管机构针对《通用数据保护条例》（General Data Protection Regulation，以下简称“GDPR”）第 32 条规定删除义务，要求数据处理者应当评估个人数据类型以及泄露风险分级，并以此为依据，确定相应级别的数据销毁方式；并且，这些销毁技术的选择取决于个人数据的存储系统和格式。在比利时的监管机构看来，匿名化并不是欧盟立法者所追求的“足够安全且保密”的技术手段，故而需要通过数据销毁措施填补匿名化技术存在的问题。〔12〕

（二）数据销毁义务的理论基础与立法现状：信息保密方式的扩张

正如上文所述，数据销毁的技术方式多是以数据的不可复原和彻底灭失作为直接目标，且数据销毁的实际范围不仅仅是用户的个人信息，还包括企业的业务数据，数据销毁义务的销毁范围、销毁方式等具体内容明显有别于删除权的具体内容，〔13〕这也意味着数据销毁义务的理论基础同

〔9〕 该标准发布于 1995 年 1 月，在 1997 年 7 月进行修订，在 2006 年又重新发布了新版的 DOD 5220.22－M 标准。新标准中有关数据清除与销毁的内容寥寥无几，但是旧版的数据清除与数据销毁之区分对于当下关于数据销毁义务的内容理解仍具有一定参考价值。

〔10〕 参见 IDSC 官网，https://www.datasanitization.org/about-international-data-sanitization-consortium/，2021 年 9 月 25 日访问。

〔11〕 该文件仅针对整个存储介质销毁的技术，不涉及文件、目录或分区部分的特定擦除。Only techniques leading to “sanitisation” of the entire medium or to its destruction are discussed in this document. The specific erasure of files, directories or partitions is therefore not processed. 参见比利时 L'APD 官网，https://www.autoriteprotectiondonnees.be/publications/recommendation-n-03-2020-of-11-december-2020.pdf。

〔12〕 美国教育部在《数据销毁的最佳实践》（Best Practices for Data Destruction）中将数据销毁分为“数据清理”（clear）、“数据清除”（purge）和“数据销毁”（destory）三类：（1）数据清理是指清理所有用户在可寻地址存储位置中的数据，防止简单的非侵入性数据恢复技术；（2）数据清除是指采用物理逻辑技术的清理方法，即便采用最先进技术也无法恢复数据；（3）数据销毁是指删除数据且不可恢复的方法，但同时也导致存储介质的不可用。

〔13〕 《民法典》第 1195 条“……采取删除、屏蔽、断开链接等必要措施……”的表述，从法律术语统一性解释的角度来看，“删除”所要求的技术效果显然是以无法访问为直接目标。

表 1　IDSC 有关数据销毁方式的优势与弊端

数据销毁方式	优　　势	弊　　端
物理销毁	数据无法恢复	破坏存储介质(企业资产),无法再次利用或转售
加密擦除	快速有效	仍然允许数据保留在存储设备上,并且通常无法达到数据安全的合规性要求
数据擦除 (例如验证覆盖、生成防篡改证书、块擦除等)	数据销毁中最安全的保护形式,保留存储介质原有价值	需要企业为所有数据存储设备事前制定详细的擦除流程

表 2　L'APD 所划分的数据销毁技术方案

数据销毁技术所对应的技术方式		
清　　除	擦　　除	销　　毁
覆盖(标准化指令) 重置(恢复出厂设置)	覆盖(专用/集成化指令) 消磁 加密擦除	焚毁 粉碎 分解 消磁

样有别于删除权所依托的个人信息自决权益保护理论。在个人信息保护、数据安全和网络安全领域,相关法律法规确实尚未明文规定"数据销毁义务",甚至在《网络安全法》《个人信息保护法》《数据安全法》中均未存在过"销毁"这一表述,但这并不能成为否认数据销毁义务事实存在的直接依据,因为数据销毁义务存在的直接依据并非是学界主流观点所认可的"个人信息权益保护",而是保密义务在信息时代的内涵延伸。事实上,早在 2010 年的《保守国家秘密法》中就已经提及"销毁义务",〔14〕规定企事业单位应当严格按照国家保密规定销毁涉及国家秘密的载体,该义务的内核实质上仍然是保密义务,销毁乃是国家秘密"保密生命周期"的最后一个环节。在我国个人信息保护和数据安全监管的早期立法活动中,囿于信息技术水平尚处于早期发展阶段,立法者对于数据安全保护的认知主要还是以国家秘密、商业秘密等信息层面的保密义务为主,义务主体也是主要以"国家机关和涉及国家秘密的单位"为限。在此之后,大数据、云计算、区块链等信息技术的重大突破对立法目标和立法技术产生重大影响,以往隐藏于"隐私权"中的个人信息权益逐渐受到重视,"个人信息"开始独立于"个人隐私"之外并成为独立的民事客体。公法层面的保密义务仅以国家安全和社会公共利益为适用前提,〔15〕故而该义务无法适应私法层面自然人对于个人信息保护的利益诉求,以"国家秘密""商业秘密"等有限类型客体为保护对象的保密义务开始异化为数据安全保障义务和个人信息保护义务。一方面,"国家秘密"和"重要数据"两个概念在信息社会中内涵和外延发生偏离,传统意义上的"国家秘密"仅限于"一定时

〔14〕《中华人民共和国保守国家秘密法》第 21 条、第 22 条、第 25 条、第 34 条均有提及"国家秘密载体的销毁"。

〔15〕参见刘迎霜:《大数据时代个人信息保护再思考——以大数据产业发展之公共福利为视角》,载《社会科学》2019 年第 3 期,第 100 页。

间内只限一定范围的人员知悉的事项”，〔16〕而“重要数据”则是由国家机关制定重要数据目录予以确定，〔17〕但两者法益却存在着重叠，即两者均涉及国家安全和社会公共利益，这也是保密义务异化为数据安全保障义务的关键环节。因为“国家秘密”的存在形态是以特定内容的信息为基础，而“重要数据”的存在形态则是各行业各部门在业务活动中积累形成的“数据集合”，前者的保护方式显然无法直接沿用于后者的保护活动中，但在实际的保护逻辑层面却具有相似性，即“国家秘密”和“重要数据”均是以有限的传播和特定的处理权限为保障工具，保密义务的核心在于严格控制能够处理“国家秘密”的人员范围和时间节点，即“数据访问权限受限”，而数据安全保障义务的基础逻辑同样是限定数据访问权限，“数据分级分类保护制度”即是最佳例证。另一方面，国家秘密相关的保密义务与个人信息保护义务在客体层面存在显著的差异性，前者是以承载公共利益的国家秘密为限，后者则是以承载私法利益的个人信息权益为限，将基于个人信息自决权益的个人信息保护义务解释为保密义务的异化结果似乎存在逻辑关系断裂的问题。然而，需要说明的是，个人信息保护义务不单纯是私法利益保护的必然结果，该义务的理论基础还包括数据安全保障义务。《数据安全法》和《个人信息保护法》在法律效力层面相同，但在立法目标和调整范围层面，《数据安全法》囊括了所有类型的数据安全保护，“数据安全”指向“个人、组织的合法权益”和“国家主权、安全和发展利益”，调整范围显然囊括了个人信息的安全；而《个人信息保护法》则是在《数据安全法》的安全保障制度框架下建构的个人信息保护义务，该义务同样沿用了数据安全保障义务的保护逻辑，即自然人的个人信息应当以秘密的状态予以处理，不得超出约定的范围向第三方主体传输或是用于其他信息服务场景。更重要的是，个人信息的安全状态不仅关涉自然人的合法权益，同样也关涉社会公共利益和国家安全，如在跨境数据流程场景下，信息处理者需要经过安全评估或个人信息保护认证方可向境外提供数据。

综上所述，在我国现有立法资源中，数据销毁义务起始于国家秘密、国家安全信息的保密义务，在整个数据生命周期中，销毁是信息归于消灭的最后阶段，保密义务内含的“信息处理受限”之逻辑，要求数据销毁的直接结果是数据的不可复原和不可再次获取。而在信息社会中，涉及国家安全和社会公共利益的客体从“国家秘密”延伸至“重要数据”和“个人信息”，保密义务也随之异化为“数据安全保障义务”和“个人信息保护义务”。这种异化趋势导致数据销毁义务在理论基础层面发生变化：第一，在保护理念层面，为了适应客体范围的变化，信息安全的保护理念也从传统的“信息保密”转向“可控式数据安全”，数据销毁义务不再是单纯地导致“秘密/机密/绝密信息的消灭”，而是延伸至“数据的不可再次获取”。第二，在制度功能层面，数据销毁义务功能从早期“保障信息处于秘密状态”转向现在的“尽可能消除可控的数据安全风险”，重要数据的销毁是为确保仅有特定的法律主体能够获取这些数据，且在数据销毁之后无法通过其他方法予以复原，个人信息的销毁则是为了确保个人信息在废弃过程中意外泄露的风险处于可控状况。第三，在义务内容层面，基于保密目标的数据销毁义务是指国家秘密载体应当按照国家保密规定予以销毁的义务，任何组织或个人均无权私自销毁国家秘密载体，而基于数据安全保障义务的数据销毁义务则是指义务主体在数据生命周期最后阶段应当采取适当的销毁技术将数据安全风险控制在可接受的范围内。

---

〔16〕《中华人民共和国保守国家秘密法》第2条规定：“国家秘密是关系国家安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项。”

〔17〕《数据安全法》第21条规定：“国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。”

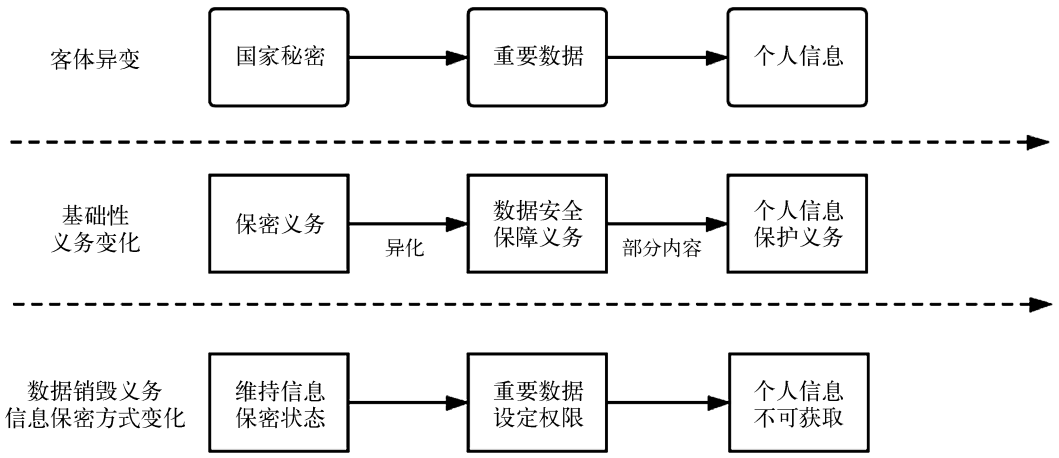

图 1

三、数据销毁义务的功能定位和制度建构

（一）数据销毁义务的功能定位

数据销毁义务的理论基础在于信息保密方式的异化，《保守国家秘密法》中的信息保密方式要求信息销毁的方式处于保密状态，并严格按照既有的销毁流程进行内容和载体的彻底清除；数据安全相关立法中的数据保密方式则是维持数据安全处于可控状态，既包括保障仅有法律授权主体才可以持有重要数据，也包括第三方无法获取已经销毁的个人信息。数据销毁义务的功能定位是以数据安全保障制度为依托，其目的是保障数据主体的数据控制权，防止数据被滥用、误用，〔18〕确保数据安全风险处于可控状况。换言之，对于义务主体而言，数据销毁不是为了保障数据安全的强制性义务，而以确认义务主体继续持有数据无法保障数据安全为前提，倘若义务主体现有的技术水平、内部管理制度能够保障可接受的数据安全，则义务主体可以选择继续持有这些数据，而非只能选择销毁这些数据。数据销毁义务的体系定位是与数据安全风险评估机制直接挂钩的，因为数据安全风险评估机制的基本逻辑是基于统一的安全指标和权重设置将数据安全风险可视化，数据（信息）处理者结合自身风险控制能力和安全技术水平选择适当的数据处理流程保障数据安全，不可复原和不可非法获取的数据销毁技术属于“兜底性”的数据安全处理方案。进一步而言，数据销毁义务的功能定位不应当仅仅理解为确保信息处理者删除个人信息的义务性规范，否则该项义务只不过是“删除权”所对应的个人信息保护义务的另一种类型而已，而是应当理解为全行业全领域在处理无用数据、超期数据、未授权数据、不安全数据时应当采取的技术处理方案。〔19〕具体而言，理解数据销毁义务的功能定位有必要厘清以下三个概念之间的体系关系：

第一，数据销毁义务与数据删除义务的区分。其一，数据销毁义务的履行能够确保信息处理者无法获得特定自然人的数字身份和行为轨迹。删除权的功能首先是确保自然人能够再次隐匿自己在网络空间的数字身份以及降低网络社会对个人信息的感知程度，而数据销毁义务也

〔18〕 参见唐林垚：《隐私计算的法律规制》，载《社会科学》2021 年第 12 期，第 118—119 页。

〔19〕 参见张继红：《大数据时代个人信息保护行业自律的困境与出路》，载《财经法学》2018 年第 6 期，第 57—60 页。

具有类似的功能定位，即通过焚毁法、覆写法等数据销毁技术达成“信息处理者不再控制自然人个人数据”的法律效果。〔20〕其二，数据销毁义务的履行应当是有限度地销毁部分个人数据，即应当是销毁、删除自然人姓名、电话、IP地址、职业等信息要素，而不是因为某一条或数据库中存储有特定自然人相关联的个人数据就要销毁、删除整条数据或整个数据库。〔21〕根据第一层次的功能定位，数据销毁义务既可以直接以技术手段实现个人数据从有到无的转变，也可以间接销毁、删除部分信息要素达成特定自然人身份的无法关联和无法识别，即仅清除、替换部分信息要素即可。其三，数据销毁义务的履行应当在平衡企业数据销毁成本和个人数据安全保护两种法益基础上进行。〔22〕数据销毁义务的具体内容不应当严格限定某一类或某几种技术方案，对于不同规模企业而言，从根源上销毁存储介质固然可以确保数据的不可再生，但对于中小企业而言，频繁地更换存储介质无异于增加额外的经济成本，故而数据销毁方式的选择应当交由信息处理者自身根据实际情况予以确定。〔23〕数据销毁义务的实现方式也应当满足数据安全保护的立法目标，对于敏感个人数据，这类数据的销毁应当采用不可再生、不可溯源的技术方案予以实现（如硬件焚毁等）；对于一般个人数据而言，这类数据则可以采取恢复成本高昂的技术方案予以销毁（如加密销毁、数据销毁等）。

第二，因法定事由而必须销毁数据的义务和按照安全技术标准销毁数据的义务。数据销毁义务的基本内涵并不是强制要求信息处理者必须销毁数据，而是指信息处理者在销毁数据时所采取的销毁流程和销毁技术措施应当满足数据安全的立法目标和安全技术标准。在《工业和信息化领域数据安全管理办法（试行）》第23条中，工业和电信数据处理者履行数据销毁义务主要包括“建立数据销毁策略和管理制度”“明确销毁对象、流程和技术等要求”以及“记录和留存销毁活动”三个层面的内容。数据销毁义务的制度目的是实现数据全生命周期的安全管理，满足立法层面所要求的“持续处于有效保护状态”和“合法利用状态”。因此，数据销毁义务不可简单理解为“义务主体应当销毁数据”的法定义务。事实上，该义务可拆解为两个部分：第一个部分是义务主体在满足何种条件时应当销毁数据以及在何种条件时可以选择销毁数据作为数据安全保障的备选方案，即“因法定事由而必须销毁的数据”和“因安全事由而可以销毁的数据”。该部分的义务功能在于明确数据销毁行为本身不是强制性义务，而是可以选择的安全技术方案。如果过度强调数据销毁义务的制度功能在于明确义务主体销毁数据的法定情形，则与“删除权”的基本内容并无本质差异，无法凸显在数据全生命周期中“销毁”和“删除”两类数据处理行为的功能差异。第二个部分则是数据销毁行为的法定要求，即数据销毁的基本流程、销毁技术、销毁范围、销毁记录应当满足法律要求和技术标准，保障数据销毁活动的最终结果能够达到不可复原的状态，且其他法律主体无法在数据销毁之后非法采取其他技术手段重新获得数据。数据销毁义务的立法目的不是为了限制义务主体获取、存储、使用数据的能力，而是为了确保义务主体在数据全生命周期的各个阶段都能

〔20〕 参见齐爱民、张哲：《识别与再识别：个人信息的概念界定与立法选择》，载《重庆大学学报（社会科学版）》2018年第2期，第119—131页。

〔21〕 参见苏宇、高文英：《个人信息的身份识别标准：源流、实践与反思》，载《交大法学》2019年第4期，第64—66页。

〔22〕 参见张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，载《中国法学》2015年第3期，第52页。

〔23〕 强制履行数据销毁义务有可能给企业施加不合理的影响，影响企业的正当权益。参见丁晓东：《个人信息权利的反思与重塑——论个人信息保护的适用前提与法益基础》，载《中外法学》2020年第2期，第350页。

保障数据安全以及风险可控。在业务实践中，由于数据销毁流程的不规范、存储介质未彻底消磁、数据覆写不完全等原因，销毁环节所存在的数据安全风险并不低于数据收集、存储、加工、传输等环节的安全风险水平。

第三，数据销毁义务与去标识化义务。在个人信息处理场景下，信息处理者通常有义务采用技术措施去除个人信息中的可识别要素，中断这些信息直接识别或间接识别特定自然人的可能性，这与数据销毁义务所欲达成的技术效果具有相似性，即均是以个人信息可识别功能的丧失作为“清除个人信息”的结果形式之一。两者之间的体系逻辑表现为两个层面：第一，在义务主体安全技术能力能够保障数据安全风险处于可接受范围内时，义务主体可以“二者选其一”，因为数据处理实践活动的复杂性决定了以“一刀切”的方式明确限定数据销毁范围不具有可操作性，个人信息的存在形态并非是以每行记录代表特定自然人个人信息的表格记录方式，而是以零散拆分的数据要素分布式存储在数据库中，数据销毁范围显然不可能销毁“一切与自然人相关的信息”，其销毁结果只要达成“个人信息”的实质消除即可，即自身无法复原业已销毁的数据和其他人也无法通过销毁之后剩余的其他数据再次识别特定自然人。这种销毁效果与去标识化的技术效果均满足“无法识别特定自然人”的要求，义务主体“二者选其一”的法律效果并无本质差异。第二，数据销毁与数据去标识化在技术逻辑层面终究属于两种完全不同的安全技术方案，数据销毁的直接结果是部分数据的彻底消除，而去标识化的技术逻辑则是“去除个人信息中能够标识或关联至特定自然人的要素”，〔24〕识别要素被“隐藏”而未彻底销毁，所以前者的数据安全保障效果明显优于后者，一旦数据安全风险评估结果认定义务主体无法控制数据安全水平，则义务主体只能选择数据销毁这一方式来控制数据生命周期最后阶段的安全性，因为现有信息技术不可能保证绝对的数据安全，保障个人信息安全最有效的方式是直接切断所有可能获取个人信息的渠道，以去标识化方式继续持有个人信息只会加剧个人信息泄露的实际风险。

总结而言，数据销毁义务的直接功能在于避免个人数据、业务数据、重要数据等在数据销毁之后复原并造成大规模数据泄露事件。同时，需要注意的是，数据销毁义务在整个数据安全立法体系中属于《数据安全法》“数据安全保障制度”的阶段性义务，即数据生命周期最后环节的“安全保障义务”，数据销毁义务与个人信息删除权之间在技术效果层面确实容易混淆，但前者的适用范围和正当性是以社会公共利益和国家安全层面的数据安全为基础，而后者则是个人信息权益的自然延伸，亦是处理个人信息的合法事由和必要性丧失时的必然结果。在《重庆市公共数据分类分级指南（试行）》中，更是将“数据销毁”与“数据处理”“数据开放”“数据共享”等概念并列，数据销毁的技术功能明显有别于其他数据处理流程，且按照该标准的四级管控要求，“删除”仅是“销毁”的一个步骤，数据删除之后，还需要确保采用其他逻辑销毁方法，保障所有其他副本均被安全地删除。

（二）数据销毁义务的履行标准

数据销毁义务的制度功能是以嵌入数据安全风险评估机制的方式实现，通过评估流程和评估结果确定特定场景中义务主体和销毁数据的具体范围。在义务主体层面，数据销毁义务制度建构最主要的问题在于存在业务关联的第三方是否同样应当履行数据销毁义务，或者说信息处理者与业务关联第三方之间如何协商履行数据销毁义务。数据销毁义务的理论基础是信息保密方式的异化，业务关联第三方是否有义务销毁相关数据的认定关键仍然需要回归至数据安全

〔24〕《个人信息安全规范》3.15和《个人信息去标识化指南》3.3均将“去标识化”界定为“通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体的过程”。

风险评估机制，如果评估结果认定第三方所留存的数据将导致主要的或相当程度的安全风险，则第三方理应销毁数据确保重要数据始终维系在有限范围内予以处理或个人信息无法被外部环境获取，而义务主体则应当对第三方的数据销毁行为承担连带责任。在销毁范围层面，数据销毁义务面临着与删除权同样的问题：销毁的数据范围是包括所有相关数据，还是仅以“涉及国家安全和社会公共利益”的数据要素为限。根据前文所讨论的数据销毁义务理论基础和功能定位来看，数据销毁义务的适用场景主要集中于“数据确已达到销毁环节”和“数据需要销毁来保障安全”两种情形，前者主要指向商用价值丧失或合法处理基础丧失的重要数据、个人信息，后者主要指向处于安全异常状态的重要数据和个人信息，且信息处理者继续存储这些数据无法保障安全，此时则需要采用数据销毁方式彻底消除数据。数据销毁义务的销毁范围实际上与销毁效果密切相关，义务主体所选择的销毁范围能满足数据销毁义务的法定要求和安全技术标准，即便没有销毁重要数据和个人信息的全部内容或者没有采用存储介质直接销毁的方法，也可视为义务主体已经履行数据销毁义务。以用户注销账户为例，用户可以要求信息处理者履行删除其个人信息的法定义务，此时的“删除”的数据范围存在三种认定方式：一种方式是直接在信息处理者的数据库中删除用户账号及该账号使用期间所形成的所有使用数据，另一种方式是直接在用户端界面删除账户相关的所有信息，其他用户无法获得该用户之前的信息服务使用记录，还有一种方式则是信息处理者仅删除用户姓名、账号昵称、账号唯一识别码、IP 地址、电话号码等关键信息要素，对用户在使用账号期间所形成的使用数据予以保留。仔细分析这三种销毁方式，实质上代表了三种不同的个人信息保护立场，第一种方式是以自然人在网络空间的“数字身份”作为实际的销毁对象，确保自然人有能力选择“重新塑造”自己在网络空间的社会形象；〔25〕第二种则是将个人信息与个人隐私置于相同的保护方式之下，以一般理性人能否识别特定自然人身份作为直接的判断依据，确保个人信息的私密属性；〔26〕第三种则是立足“个人信息”概念所要求的可识别标准，数据销毁的真正对象不是数据本身，而是个人数据的可识别性和可关联性，只要销毁后的数据不再具有识别能力，则已经满足数据销毁义务的法定要求。〔27〕从我国《个人信息保护法》第 1 条所规定的“规范个人信息处理活动”和“促进个人信息合理利用”两项立法目的来看，第三种数据销毁方式更符合我国个人信息保护的实践需求，一方面“销毁”了信息处理者以及第三方识别个人信息的可能性，另一方面也为信息处理者扩大数据商业价值预留了一定空间，例如在部分用户画像应用场合，即便结构化数据中销毁了自然人的姓名、年龄、电话、IP 地址等关键信息要素，但信息处理者仍然可以将剩余不具备识别特定自然人功能的数据用于用户群体的行为偏好分析。〔28〕审视现有的立法制度和商业实践，数据销毁义务的履行方式和销毁范围需要考量“中断识别”和“损害预防”两个因素。在中断识别层面，数据销毁义务的履行方式包括全部数据销毁和部分数据销毁。前者主要出现在信息处理者不再运营其产品或服务之场景，中断识别的判断标准是用户相关的所有数据均已彻底销毁。后者则主要出现在信息处理者需要留存部分数据作为用户群体画像分析等业务活动中，中断识别的判断标准可延伸至三个层面。一是与其他用户采用同一体系的唯一识别信息要素均已删除，即销毁范围既包

〔25〕 参见王琰、赵婕：《大数据时代被遗忘权的现实逻辑与本土建构》，载《南昌大学学报（人文社会科学版）》2020 年第 6 期，第 104 页。

〔26〕 参见房绍坤、曹相见：《论个人信息人格利益的隐私本质》，载《法制与社会发展》2019 年第 4 期，第 109 页。

〔27〕 参见程德理、赵丽丽：《个人信息保护中的“识别”要素研究》，载《河北法学》2020 年第 9 期，第 48 页。

〔28〕 参见丁晓东：《用户画像、个性化推荐与个人信息保护》，载《环球法律评论》2019 年第 5 期，第 92 页。

括敏感个人信息，也包括唯一设备编号，但是如果信息处理者采用其他编号方式为销毁对象的其他非个人数据进行唯一编号，同样满足不具有识别特定自然人的法定要求。二是数据销毁的范围既包括信息处理者本身，还包括与信息处理者存在业务链关系的其他关联主体，确保个人数据在这些整体性提供信息服务的信息处理者之间均已彻底销毁。三是如果采取软销毁方式，数据销毁的效果应当满足现有信息技术不足以或需要以极其不合理的代价重新恢复原始数据或再次识别特定自然人，如果销毁的数据范围涉及敏感个人信息时，数据销毁的效果应当仅以数据不可复原或回档作为唯一判断标准。〔29〕除此之外，数据销毁义务的现实依据还在于避免信息处理者因为不合规或不恰当的数据销毁流程而导致数据意外泄露，〔30〕故而该义务履行还应当包括销毁后的数据能够有效避免数据泄露、数据非法访问等安全风险。〔31〕

四、数据销毁义务的制度建构的几个特殊问题

（一）信息处理者有义务销毁死者个人数据吗？

《个人信息保护法》第49条规定了自然人近亲属可以基于“自身的合法、正当利益”主张对死者的相关个人信息行使删除权，相较于《个人信息保护法草案（二次审议稿）》〔32〕的表述而言，该条规定在承认死者近亲属可以针对死者个人信息行使相关权利的基础上，还设置了行使权利的“合法性”限制条件。这种立法表述变化的原因在于死者个人信息保护的基本立场明显不同于自然人在世时的个人信息保护逻辑。自然人死亡之后既不会因为个人信息的不当处理而感受到精神痛苦，也无法根据自己的意愿继续决定个人信息处理的具体方式，即信息自决权益的实现基础早已丧失，在立法层面继续承认死者享有与其他自然人同样内容的个人信息权益有悖立法宗旨。类比传统人格权保护学说，〔33〕死者不再享有个人信息权益不等于死者的个人信息不被保护，只不过是死者个人信息所承载的法益内容从自然人信息自决权益转变为死者近亲属的合法权益。信息处理者滥用死者个人信息有可能侵害死者近亲属的人格尊严以及其他人格权益，故而立法者允许死者近亲属以自身合法正当利益受到侵害为由，主张信息处理者履行死者个人信息删除义务。然而，需要注意的是，此时的“删除权”与自然人本身行使的“删除权”存在内容差异：死者近亲属行使“删除权”的目的是维护自身而非死者的人格权益，其主张删除死者个人信息的场景多为信息处理者擅自公开死者个人信息、不当处理死者个人信息、贬低死者社会形象而造成近亲属精神痛苦等情形，删除死者个人信息的方式与删除死者个人隐私的方式

〔29〕 参见田野、张晨辉：《论敏感个人信息的法律保护》，载《河南社会科学》2019年第7期，第48页。

〔30〕 See Solon Barocas & Helen Nissenbaum, *Big Data's End Run around Anonymity and Consent*, in Julia Lane et al., eds., Privacy, Big Data, and the Public Good: Frameworks for Engagement, Cambridge University Press, 2014, p.44－75.

〔31〕 参见吕炳斌：《论网络用户对“数据”的权利——兼论网络法中的产业政策和利益衡量》，载《法律科学（西北政法大学学报）》2018年第6期，第64页。

〔32〕 二审稿第49条规定：“自然人死亡的，个人在个人信息处理活动中的权利，由其近亲属行使。”

〔33〕 学界通说认为，自然人已经死亡的，不再享有姓名权、肖像权、隐私权等人格权，但死者的姓名、肖像、名誉权、隐私等人格利益仍然受到法律保护，其理论学说包括死者权利保护说、死者法益保护说、近亲属权利说、人格利益继承说、延伸保护说等学说。参见程啸：《论死者个人信息的保护》，载《法学评论》2021年第5期，第13—23页。

较为相似，均是通过删除等操作方式将信息内容从公开状态重新转变为私密状态。而一般意义上的“删除权”则是要求信息处理者在不具备合法处理个人信息的情形下不再持有自然人的个人信息，删除方式多为数据库后台的个人信息识别要素的剔除或者个人信息相关记录的全部删除。简言之，死者近亲属的“删除权”是以信息处理者不当处理死者个人信息或非法公开死者个人信息为前提，权利的本质是自身人格利益的保护，并未涉及信息处理者是否有义务销毁后台数据库所存储的死者个人数据。

既然自然人在死亡后不再享有个人信息权益，那么这是否意味着信息处理者只要满足个人信息处理方式，在不损害死者近亲属人格利益的情况下可以无期限地存储和处理死者个人信息？换言之，信息处理者是否有义务按照法律规定销毁个人数据？不妨预先假设：信息处理者有义务销毁死者的个人数据，其依据显然是为了保护死者的人格尊严和其他人格利益，但以二进制数值等形式存在的个人信息在不对外公开的情况下，不涉及对《民法典》第994条提及的“对死者姓名、肖像、名誉、荣誉、隐私、遗体等人格权益的侵害”以及《个人信息保护法》第49条提及的死者近亲属的“合法权益”，这种数据销毁义务的依据显然无法成立。此外，数据销毁义务的理论基础意在强调数据的安全状态以及恰当的数据保护方式，倘若以信息处理者继续存储死者个人数据而无法保障这些数据安全状态为由，要求信息处理者履行数据销毁义务，既缺乏直接的权利主体（死者），也缺乏足够的强制销毁事由，因为这种数据安全并不涉及国家安全、社会公共利益，是否予以销毁完全属于信息处理者经营自主权的决定范畴。即便死者个人数据存在数据泄露风险，也是由死者近亲属自行选择是否要求信息处理者删除死者个人信息，而非在立法层面强制要求信息处理者必须销毁个人数据，并且，强制性销毁义务模式本身也与《数据安全法》所追求的数据合法利用目标相悖。因此，在不侵害死者近亲属合法权益、不对外公开或传输死者个人数据的前提下，信息处理者并没有需要强制销毁死者的个人数据的义务。

（二）去中心化技术方案下数据销毁义务应当如何履行？

现阶段的区块链技术主要集中应用于金融交易、产权登记、司法公证等领域，尤其是依托该技术所建构的智能合约具有不可篡改性和自动执行等技术优势，能够有效满足金融、医疗、版权等行业的业务需求。区块链技术本身是一种去中心化的分布式记账系统，实质上是集体维护数据库的一个技术方案，〔34〕其底层的技术逻辑可以表述为所有参与节点共同维护交易活动以及数据库，在系统中将已经达成交易的区块连接成一条主链，所有节点基于密码学原理共同对区块记载的内容予以承认，不需要第三方的介入，而非传统的金融活动中通常需要依靠中立第三方以维护商事秩序。〔35〕恰恰是这种交易信息数据修改需要主链超过50%的节点共同认可的不可篡改优势，致使数据销毁义务的履行变得不再那么容易，在区块链上删除之前的数据远比在个人计算机上将文件拖入回收站要难得多。法律不可能强行要求信息处理者以高昂的销毁成本在区块中彻底销毁数据，而是需要重新审视数据销毁义务的适用场景和履行方式。〔36〕诚如前文所言，数据销毁义务的直接目的是彻底销毁个人数据，但这种销毁方式并不只限于一般意义上的物理销毁，还包括加密销毁、访问权限销毁等方式，只要其实际效果能够满足法定“删除个人数据”之要求，即便是在区块

〔34〕 参见石冠彬、陈全真：《论区块链存证电子数据的优势及司法审查路径》，载《西南民族大学学报（人文社会科学版）》2021年第1期，第69页。

〔35〕 参见唐林垚：《我国信息披露违规增持股份之惩戒抉择》，载《西南民族大学学报（人文社会科学版）》2020年第4期，第93页。

〔36〕 参见陈奇伟、聂琳峰：《技术＋法律：区块链时代个人信息权的法律保护》，载《江西社会科学》2020年第6期，第170页。

链上销毁数据也不一定限于在区块上删除数据这一种方式。区块链上存储信息的访问往往需要私钥和公钥的相互匹配，故而数据销毁的方式可以采取直接对需要销毁的数据进行加密，之后将访问这些数据所需的私钥直接销毁，导致任何人在此之后均无法访问这些区块上存储的个人数据。但问题在于，这种“加密销毁”方式与数据销毁方式最大的不同在于前者并没有对个人数据的可识别性和关联性进行直接处理，而是直接以封锁所有访问权限的方式切断立法者设想的识别主体接触这些个人数据的路径，这种实际不可能接触数据并识别特定自然人的技术效果与立法者所追求的数据销毁效果仍然存在效果鸿沟。一方面，“加密销毁”的实质是隐藏区块链上的个人信息，并不妨碍个人数据存在于特定区块这一事实的成立，即便一般人无法破解区块链上的私钥访问权限限制，但这并不等于个人数据不会被再度访问和识别，区块链技术本身并不能达到绝对安全的状态，在付出足够多的代价之后，第三方仍然有可能绕过私钥的技术限制获取隐藏的个人数据。因此，“加密销毁”方式在此层面并没有达到《个人信息保护法》的保护要求。另一方面，《个人信息保护法》第47条有关“删除”的表述实质上也是在确保信息处理者所存储的个人信息具有法律依据和现实依据，既没有超出收集阶段与用户约定的存储期限，也没有通过非法途径获取用户个人信息。〔37〕而在“加密销毁”方式中，个人数据的存在事实无法否认，即便访问权限受到限制，也并不排斥个人数据存储在信息处理者的区块链这一事实，信息处理者存储应当删除的个人数据本身即与立法本意相悖。这是否意味着区块链技术可以作为数据销毁义务的例外情形？如果对此予以肯定，则会错误引导信息处理者将个人数据全部上传至私有区块链，以此避免履行数据销毁义务。数据销毁义务的履行主体是信息控制者或信息处理者，这些义务主体的共同特点在于能够有效控制和处理个人数据，而作为参与者的各个节点虽然看似缺乏中心化管理机构的控制能力，但是这些节点在将个人数据上传至区块链之前存在明确的处理目的和处理方式，将其视为信息处理者是合乎逻辑的。并且，在私有区块链模式下，通常存在一个法人实体作为主要运营商，并根据其确定的治理规则对区块链实施一定范围内的控制。既然区块链上的数据删除难以实现，倒不如直接要求信息处理者在数据量较大且这些数据会定期更新的情形下直接在链下存储个人数据，进而将数据销毁义务转化为擦除数据库。

五、结语：数据销毁义务的制度建构

数据销毁义务应用的特殊场景远不止前文所述，在信息处理者进入破产清算阶段，业务数据和个人数据并非当然可以作为企业破产财产，现行立法并没有直接规定企业数据财产权，并且数据财产权的设置显然是以数据安全为前提，倘若根据数据安全风险评估结果，处于破产阶段的企业已经无法保障包含业务数据的安全，破产管理人应当以保障自然人个人信息权益和重要数据安全作为优先事项，按照行业主管部门的监管要求直接销毁数据。数据销毁义务的制度建构还需要厘清数据安全和数据利用之间的法益平衡关系，即便因业务数据毫无商业价值而选择数据销毁，由于硬件存储介质本身也具有一定的经济价值，此时的数据销毁义务履行方式显然也不能采用焚毁法、水泡法等硬销毁方式，但在采用软销毁方式时，考虑到破产管理人对于业务数据安全保护能力有限，具体的销毁技术方案应当满足更高标准的不可复原性，且数据删除的范围应当是以全部个人信息为主。因此，我国在建构全生命周期个人信息保护体系的过程中，不仅需要重视数据收集阶段的合目的性、必要性等具体规则的构建，同时也需要重视数据销毁阶段的标准设置与规则

〔37〕 参见唐林垚：《“脱离算法自动化决策”的虚幻承诺》，载《东方法学》2020年第6期，第25页。

建构。首先，数据销毁义务应当与个人信息删除义务在制度层面进行明确区分，数据销毁义务应当安置于《数据安全法》的数据安全保障制度框架内，个人信息的销毁仅是数据销毁义务履行的一小部分，更重要的是义务主体按照法定要求和技术标准销毁“重要数据”。其次，应当在立法层面细化数据销毁义务的履行标准，以“数据的彻底清除和不可复原”为基本原则，允许义务主体在技术能力和经济成本允许的范围内自行选择最为恰当的数据销毁方式，物理介质的彻底销毁并非履行义务的唯一标准。最后，数据销毁义务的适用范围需要考虑到死者个人数据销毁、去中心化技术方案下的数据销毁以及破产清算时数据销毁等特殊情形，细化数据销毁义务的例外情形和特别规则。

Abstract China's current legislation stipulates that a natural person has the right to request information processors to delete personal information, but this does not mean that the last link of the data life cycle is "deletion", because "the right to delete" is the inevitable result of "the loss of the legitimacy and necessity foundation of information processing", and "data destruction" is the end of the processing process of "data elimination". The theoretical basis of data destruction obligation lies in the expansion of information confidentiality, that is, from maintaining information confidentiality to maintaining the controllability of data security risk. In the process of data security risk assessment, if the obligatory subject cannot ensure that the important data and personal information not used temporarily are in a safe state, an appropriate data destruction paradigm should be adopted to reduce the security risk of data disclosure or illegal recovery. In future legislative activities, China should clarify the specific system contents such as the obligation subject, destruction mode and destruction scope, and complete the "final closed loop" of data security legislation.

Keywords Duty of Data Destruction, The Right to Delete, Confidentiality Methods, Data Security Risk Assessment, Risk Management

（责任编辑：曹博）