网络首发时间：2023-04-07 13:24:48
网络首发地址：https://kns.cnki.net/kcms/detail/61.1167.G3.20230407.1034.004.html

区块链技术应用下个人信息删除权适用挑战与应对*

赵丽莉[1]　陈家辉[2]

（1. 山东科技大学 数字法治研究院　青岛　266590；
2. 山东科技大学 知识产权学院　青岛　266590）

摘　要：[**研究目的**]为协调区块链的技术特征与个人信息删除权行使可能产生的矛盾，探求区块链技术、应用实践、法律主体与删除权的融合治理之路，提出区块链场景下保障个人信息删除权行使的具体举措。[**研究方法**]综合运用比较研究，考量区块链技术理念层面、实践层面、法律主体层面与删除权行使如何协同，从而实现区块链技术与删除权的共生共长。[**研究结论**]法律解释层面：合理法律解释推动区块链技术应用与删除权相适应；技术层面：寻求删除权“可替代”方案和链上链外双重保障机制；主体层面：区分区块链的用途和类型来确定区块链上个人信息控制者。

关键词：个人信息；个人信息删除权；信息保护；区块链；去中心化；相对删除
中图分类号：D912.29　　**文献标识码**：A

Challenges and Responses to the Application of the Right to Delete Personal Information under the Application of Blockchain Technology

Zhao Lili[1]　Chen Jiahui[2]

(1 Institute of Digital Rule of Law, Shandong University of Science and Technology, Qingdao　266590;
2. Institute of Intellectual Property, Shandong University of Science and Technology, Qingdao　266590)

Abstract: [**Research purpose**] To reconcile the possible contradictions between the technical features of blockchain and the exercise of the right to erasure of personal information, explore the path of integration of blockchain technology, application practice, legal subjects and the right to erasure for governance, and propose specific measures to guarantee the exercise of the right to erasure of personal information under the blockchain scenario. [**Research method**] The comparative study is applied to consider how the concept, practice and legal subject of blockchain technology and the exercise of the right to erasure can work together to achieve the symbiosis and co-growth of them. [**Research conclusion**] Legal interpretation level: reasonable legal interpretation promotes the application of blockchain technology and the right to delete; Technical level: seek “alternative” solutions for deletion rights and off-chain dual guarantee mechanisms; Subject level: distinguish the purpose and type of blockchain to determine the personal information controller on the blockchain.

Key words: personal information; right to erasure of personal information; information protection; blockchain; decentralization; relative deletion

0　引　言

区块链是一种分布账本式的互联网数据库，通过加密算法将得到验证的数据按上链时间顺序相连，并通过共识机制保障链上数据不可篡改性[1]。作为新一代数据管理和存储技术，不可篡改性、去中心化、透明

基金项目：2022 年度司法部法治建设与法学理论研究部级科研项目重点项目：“外商投资投资数据安全审查制度研究（编号：22SFB2004）”阶段性成果。
作者简介：**赵丽莉**，女，1978 年生，博士，教授，研究员，硕士生导师，研究方向：网络法学；**陈家辉**，男，1999 年生，硕士研究生，青创团队研究助理，研究方向：网络法学。

化、可溯源性等区块链的底层技术特征顺应了数据开放和信息保护的双重需求[2],并在物联网、数字资产交易、数字金融、供应链管理、智能制造等不同领域落地,服务个人信息处理和保护实践。与此同时,大型数据服务中心的一系列数据泄露事件使得其安全性受到质疑,个人信息删除的诉求被提出。个人信息删除权确认了特殊情况下信息主体请求信息处理者删除信息的权利,然而,当个人信息链上存储和流转时,区块链技术应用与链上个人信息无法有效删除的冲突产生。

已有研究实践显示:研究已经关注到区块链应用于个人信息保护的价值,诸如王禄生、王爽指出应对当前个人信息安全保护弱化、个人控制权虚化、数据共享不足实践困境,提出个人信息与区块链合作治理之路[3];还有学者论述了区块链技术下的个人信息界定问题[4],区块链上个人数据权属[5]等基础性问题。与此同时,区块链技术与个人信息保护兼容性问题也被提出,王从光从法理角度检视区块链与个人信息保护的张力[6];陈爱飞基于解释论立场,多维度解释链上删除含义,寻求当前法律框架下删除问题[7]。齐爱民从区块链技术特殊性出发,分析区块链技术带来的个人信息保护法律障碍[8]。Clare Sullivan 和 Eric Burger 从技术角度提出通过设计出只有用户自己才能访问私钥和公钥的区块链,实现用户自我控制[9]。前述学者虽然从不同角度指出区块链与个人信息保护的合作治理和冲突规范,但并未延申及区块链各种技术特性给删除权行使所带来的具体挑战,在具体治理方面尚缺乏基于删除权,个人信息保护,区块链技术综合治理对策分析。基于此,本研究从区块链三大技术特性出发,探求区块链技术、应用实践、法律主体与删除权的融合治理之路。

1 区块链技术应用下的个人信息删除权解读

区块链凭借其去中心化信息处理模式保障了链上信息透明、完整、可靠,我国立法上也不断加强个人信息保护,并基于个人信息控制权理论逐步确立了个人信息删除权体系。原则上,删除权与区块链技术有着共同的数据治理目标,都在一定程度上适应了信息保护的复杂要求。

1.1 区块链技术精准契合个人信息保护现实痛点

众所周知,大数据技术发展的前提是不断收集和存储数据,中央数据库中都积累了大量的个人一般信息和敏感信息。从外部看,中心化的数据管理模式一旦遭遇黑客入侵,其仅依赖于中央数据库系统的安全保护更容易造成数据全部泄露。从内部看,金融、销售等严重依赖数据的行业的数据买卖已形成一条黑色产业链,每年泄露的数据总量高达数十亿条,交易金额超10亿元人民币[10]。数据服务中心长期面临外部和内部双重的信任危机。此外,中心化数据存储模式不仅异化信息泄露风险,通过对大数据的挖掘和分析亦可能造成大数据“杀熟”等信息滥用行为,以及信息不对称导致的机会主义频发问题。当今社会依赖法律制度可以解决许多问题,但是法律重在事后补偿,个人信息泄露造成影响又是不可逆转,人们转而更愿意相信技术带来的保护[6]。

以区块链为代表的去中心化技术模式,使得信息自我控制成为可能,有效化解隐私泄露、数据滥用等问题,为数据安全、共享提供全新路径。首先,区块链不依赖于中心化的数据服务中心,而是通过点对点式的底层网络技术进行管理,链上每个块的形成都需要各个节点的共识,并打上时间戳,而且通过区块链网络透明机制每个参与节点都有能力监控链上整个交易流,保障链上记载信息的连续真实性。其次,加密存储和分布式存储保障存储用户数据的隐私和安全性问题。数据加密上链后必须提供私钥才能访问数据地址。私钥采用非对称加密技术比一般密码的安全性高,解决了密钥传输中的隐私问题。传统集中式存储,一旦遭受黑客袭击,数据容易全部泄露。采用分布式存储后,一定程度上降低数据全部泄露的风险。再次,通过加密算法,对用户身份信息进行加密,实现身份信息和交易数据分离。以哈希化加密为例,区块链上产生的交易数据(交易地址、金额、交易时间等)都以公开透明形式存储在区块链上以供查询。但是,与交易无关的用户个人信息则以哈希值形式存储上链。这在一定程度为服务提供商或第三方利用用户数据提供便利,服务提供商或第三方如果想要使用加密存储的数据,则必须向用户获得授权后才能访问。这种“用户隐私得到保护,数据完全可以自己掌握并参与交易”的模式完全可以实现。

1.2 个人信息删除权的确立强化个人信息控制

当前,个人信息呈现出体量巨、范围广、跨时空流动性强的特点,为了避免个人信息被过度收集和永久存储,确保信息主体的信息控制权,个人信息删除权应运而生。个人信息删除权是指当法定的或者约定的事由出现时,信息主体可以主动请求信息处理者及时删除与本人相关个人信息的权利[11]。删除权本质上是一种基于个人信息自决权的准权利,旨在保护公民自由和尊严,是人格权请求权的具体体现。2016 年通过的《网络安全法》第 43 条首次从法律层面规定了个人对信息处理者的删除权,之后《电子商务法》第 24 条、《未成年人保护法》第 72 条第 2 款及《民法典》第 1037 条第 2 款共同确定我国个人信息保护的权利框架,也为个人信息删除权的行使提供法律指南。2021 年颁

布实施的《个人信息保护法》,基于个人的信息控制权,从删除权行使方式、适用情形、行使主体等方面进一步完善了个人信息删除权体系。

区块链的去中心化运作架构使得链上每个节点平等协作,共同为区块链运行提供数据处理基础,其本质是一种分权式治理路径。然而,现行法律规定删除权的行使需要一个统一集中部门解释并执行法律,本质是一种集权式他律手段治理模式。区块链技术的运用虽然能带来公平、透明、准确的个人数据,但是,由于其去中心化技术架构与法律固有中心化治理思路之间存在矛盾,区块链技术应用于删除权之时必定会面临各种挑战。

2 区块链技术应用对个人信息删除权行使的具体挑战

区块链去中心化技术架构在某种程度上与个人信息控制权理念完美契合,这是值得肯定的。但是,区块链技术想要继续发展也必须解决其与删除权无法有效适用的冲突,具体来说两者主要存在三个方面的紧张关系:不可篡改性与信息删除理念适恰不足;记录连续性导致删除实践受阻;去中心化致删除义务主体不明。

2.1 理念恰适不足:区块链的不可篡改性致链上个人信息的删除碰壁

区块链不可篡改性的技术特征与我国个人信息控制价值相违背。增强信息主体对个人信息的控制是我国个人信息规范的目的之一,由此诞生出删除权、修改权、可携带权等制度设计[12]。但是,区块链的不可篡改性使得个人信息处理者面临在进行链上信息删除和更正时无法适用的矛盾。首先,从区块链总体设计上看,不可篡改性是其技术信赖基础。区块链与传统互联网相比最大的优点在于其节点间的高度信任,节点间需要相互合作保障数据完整性,可靠性,不能随意篡改链上数据。基于此,区块链的各种技术设计思路也都是围绕建立防丢失、防篡改,可追溯的数据,但这种设计理念又反向造成链上信息删除冲突。其次,区块链不可篡改性与信息可删除存在固有冲突,相比于传统 CRUD 组件数据库(Create、Read、Update、Delete)的四项基本操作,使用 CRW(Create、Read、Write)的区块链数据库只有三项操作,缺少 Delete(删除)功能。由此,横梗在个人信息处理者和信息主体间的就是寻求如何合作删除问题。最后,从区块链底层技术角度看,区块链的不可篡改性设计切断了链上寻求删除的路径。区块链就是哈希化数据链接形成的链条,经过哈希化的区块数据基于其单向性和防碰撞性,一方面承担着防止数据篡改的功能,另一方面链接各个区块。这种套构式链条结构使得某一个节点想要篡改区块体数据时上下区块就会发生变化,进而形成连锁反应(图 1)。另外,通过工作量证明(PoW)、权益证明(PoS)等验证区块记录数据是否具有一致性,补充避免了单个节点篡改历史数据,确保数据的真实可靠。由于区块链的上述特点,数据上链后,可以发现只有“添加”和“检查”功能,没有“删除”和“更改”功能。因此,如果在隐私领域广泛引入区块链创新,信息删除和修改都将面临无法有效操作的难题。

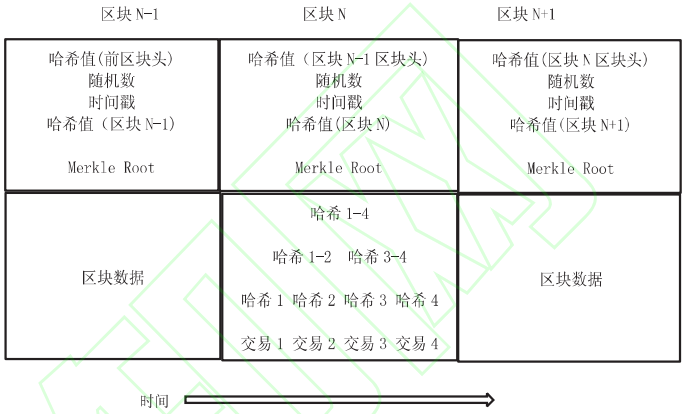

图 1 区块链链式结构图[13]

2.2 应用困境:区块链记录连续性致实践中个人信息删除权适用难度增加

区块链记录连续性是区块链核心技术特性之一,链上信息按照时间顺序打包不但可确保在数据流动过程中数据权属可追溯性,而且可以实现各节点信息全面、高效传递,缓解信息不对称。但另一方面,实践中随着区块高度堆叠和存储数据增加可能造成删除算力要求过高和数据最小化原则冲突的问题。

2.2.1 计算不足:区块链记录连续性致链上信息删除算力要求过高

区块链并非绝对不可篡改,理论上一旦 50% 以上的拥有控制权的节点达成共识,可以直接删除删除区块链内的数据[8]。算力要求过高是此种理论中存在的实践难题。因为区块链记录连续性,每次删除都需要计算整链数据,删除的难度增大,所需成本和算力也会成倍增加。如果个人数据被信息主体永久保留在区块链中,区块链本身的计算力要求将是制约删除的主要瓶颈。这是非常严重的缺点。除非,在少数私人区块链中,个人信息处理者可以通过协商、分叉修改或删除区块链中的数据。但是,我国目前对私人区块链限制比较严格,有关规定主要针对公共区块链和联盟链,而这两种类型区块链无法更改区块连续记录。并且,由于其记录连续性问题,一旦更改了一个区块中的数据,后续区块将无效,必须依据共识机制以使此链继续有效,以便根据更改前的数据状态重建区块链。这时,对计算力的要求会进一步提高,成本也会继续增加,现实中这就像“琥珀里的苍蝇”,随着验证节点增多,需要的算力越多,想从“琥珀”里取出“苍蝇”几乎成了不可

能。另外,强行删除还会面临删除失败的风险,例如,以太坊2016年遭遇黑客袭击造成以太坊分裂分叉,形成了两条链,即原链(以太坊经典,ETC)和新的分叉链(ETH)两条平行有效的链。(图2)这实际上将简单问题复杂化,不仅现实性和可行性下降,还给信息主体和个人信息处理平台带来了双重苦恼。

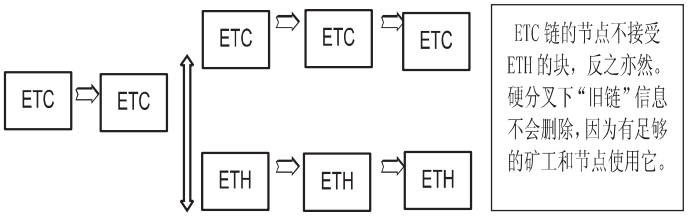

图2 原链ETC分裂平行副本ETH

2.2.2 原则冲突:区块链连续完整记录信息致删除权与数据最小化的内生冲突加剧

数据最小化原则要求网络服务提供商收集个人信息足够、相关,限于实现具体业务目的必需范围,且严格限定存储时间。我国《个人信息保护法》第六条规定网络运营者必须根据收集目的尽量减少没必要的个人信息收集和存储,确立了我国个人信息最小化原则。但是,由于区块链完整、开放、同步的体系结构,其能够持续、完整地扩展链中信息,导致了删除权与数据最小化的内生冲突加剧。删除权的行使与个人信息最小化原则息息相关,具体概括了以下两点。第一,关于个人信息的法律都规定收集、处理个人信息必须有具体、明确和合法的目的,不能以超出目的的或非法方式对个人信息进行收集、处理。但是,如果将个人信息添加到区块链中,则可以永久保留并持续扩展,随着数据块不断积累,保存的数据区块越多。更重要的是,区块链分布式账本的构造使得每个完整节点上都保存完整的数据副本,这进一步加剧了数据最小化的冲突。第二,《个人信息保护法》第四十七条规定个人有权主动请求删除的情况,那么存在网络运营商将最小化数据上链后,随着时间的推移,此种已过时的个人信息必须删除。此时,区块链上信息记录具有连续性,无法实现完全删除。最后,如果个人信息的上链处理程序本身不符合信息处理规范,大量不符合安全标准的信息被发送到链中,使得每个区块的生成都不符合数据最小化和有限存储原则,与删除权的冲突则会更加严重。区块链的信息记录连续性规则与数据最小化的目的不同,链上删除权的行使对数据最小化原则至关重要。

2.3 主体不明:区块链的去中心化架构致链上个人信息控制者不明

欧盟《通用数据保护条例》第四条规定个人信息控制者是指对个人信息的处理目的和方式起决定性作用的主体,这实际上是以集中数据管理模式为前提的。在数据集中处理过程中,监管机构也是通过辨别对处理目的和方式起决定性作用组织或个人来确定个人信息控制者。然而,区块链上数据存储是一种分布式体系,一般情况,各个节点对数据拥有平等的控制权,识别中心化的数据控制者必然会有困难。对于公链用户来说,其可以自主决定是否成为区块链控制者,并且享有完全自由加入或退出区块链网络的权力。因此,有一种观点认为,区块链的技术架构下的节点用户能够决定数据处理的目的和方法是信息保护的义务主体。对此观点提出两点反驳,第一,根据实质性判断标准,必须区分用户是处理自己的数据还是处理其他数据。节点用户对他人的个人信息不是当然的处理者,不能决定他人信息处理的目的和方式。第二,在用户将自己信息上链的情景下,个人节点可能拥有数据主体和数据控制者的双重身份[14]。例如,A接入区块链成为A节点后,通过区块链存储个人信息,同时A节点还必须保留整个区块链的全局账簿,在其他个人信息上链过程中积极参与其他节点的个人信息处理。因此,A是"个人信息主体"享受区块链服务,同时是"web服务提供者"导致责任主体和权利主体竞合。CNIL为此引入了一种联合控制者来确定链上信息控制者,即如果多个参与者希望使用区块链技术来实现共同目标,他们将通过创建法人或指定一名参与者来共同解决处理个人数据的原因和方法,这些共同参与者构成联合控制者[15]。这虽然提供一种解决思路,但使得区块链内共同控制者之间的义务分配以及共同控制者和数据主体之间的关系判断变得特别困难。

3 区块链技术应用下个人信息删除权行使的应对

区块链去中心化、不可篡改性、连续记录性是区块链的底层技术特征,是区块链运行的基础,技术信赖的基石。在此基础上,删除权的行使应首先确保区块链信息安全的技术信任,结合当前技术发展,寻求与个人信息删除权相统一之道。

3.1 合理法律解释推动区块链技术与删除权相适应

我国《个人信息保护法》第47条规定了行使删除的技术例外情况,但是区块链技术是否属于技术例外情形,进而完全排除删除权仍待商榷。相比来说,通过采取相对缓和的法律解释方法,力求实现一种区块链技术与删除权相兼容路径,更符合区块链技术健康发展的需要。

3.1.1 采取更严格告知、同意模式

当前,区块链技术和个人信息保护已经实现深度交互,但区块链技术不可篡改性仍是研究难题,传统告知同意模式已难以保持个人信息的保护与利用间的平衡[16]。因此,通过提前告知个人信息上链的好处和成

本,在信息主体同意撤销部分个人信息权益的情况下使用区块链进行信息的收集和存储也是更合适的解决方案。从上链成本来说,在告知个人信息上链需撤销其删除权、修改权、信息可携带权等个人信息权益,并取得信息主体同意的前提下,能够满足我国《民法典》第1036条和有关个人信息保护法的其他免责事由。这种方式一定程度上规避了法律与技术的冲突,实现了区块链技术应用下的个人信息保护和利用的平衡。

不可否认的是,当前"告知同意模式"也存在着异化的问题,主要包括:隐私条款冗长且繁琐、语言抽象不易理解或具高度模糊性、设置多种弹出窗口增加阅读负担等问题[17]。针对这些异化问题,建议网络平台提供商的隐私政策条款多采用简短白话文形式及多层次说明,充分保障用户知情权。"多层次说明"最早是2004年在《更加协调的信息规定意见书》被提到。该意见书认为如果单个告知信息组合在一起,以符合欧盟数据保护指令95规定的告知义务,则信息不必须出现在同一文档或同一网站上[18]。针对信息主体更倾向于跳跃阅读隐私保护条款,多层次说明的方式能够使用户在短时间内快速定位隐私条款,了解平台隐私保护政策。另外,学者们主张以一级菜单自动弹窗,强制阅读通知和体验式通知也能够提高信息主体对隐私政策的重视。总之,必须采取严格的告知同意模式,区块链平台尽到充分的引导,在充分保障知情权的基础上,信息主体撤销权益的同意才能有效。

3.1.2 确定链上"相对删除"的逻辑路径

我国《个人信息保护法》《网络安全法》《民法典》虽然都涉及"删除"文本,但没有规定"删除"的具体含义。理论上,学者将删除解释为绝对删除和相对删除。"绝对删除"即完全摧毁存储介质使系统数据达到完全不可用的程度,而"相对删除"则不使用物理手段,仅使数据不能被利用。我国《个人信息保护指南》5.1将"删除"定义为"使个人信息在信息系统中不再可用",这种"不再可用"未明说物理删除,为"相对删除"留下解释空间。从比较法的角度来看,强调数据保护的欧盟,也是采取的非绝对的软化删除。例如,欧盟委员会认为GDPR中的删除权不必要完全删除[19];英国信息委员会办公室采取更加灵活删除方式,使信息"无法使用"即达到删除目的[20]。在德国隐私删除权的保护框架中,采取和英国相同的做法,即可以使用替代解决方案,只限制数据处理。

解释路径的选择会影响区块链技术合法化方案,建议从相对删除的角度使用具体的解释路径。首先,相对删除是与绝对删除相比兼顾原则和灵活性的删除权限实施方法。绝对删除虽然有效保护个人信息的绝对控制权,但会对区块链应用产生毁灭性打击。而采用相对删除解释路径,不仅考虑到区块链不可篡改的技术特征,而且能够灵活实现个人信息保护目的。其次,我国《个人信息保护法》将保护和利用作为立法目的一同规定,体现立法者对个人信息的私人属性和社会属性并重的态度。大数据时代,数据大范围流动和利用是必然的,国家规制的原则应是防止滥用,而非严格保护。个人信息社会价值属性的显现与相对删除解释路径不谋而合。最后,现有技术下通过相对删除已经能够实现个人信息的有效保护。比如,通过访问与授权技术,当禁止其他用户访问链上数据时,在法律效果上就等同于"删除"。事实上,参照我国2017年版《个人信息保护法(草案)》30条第3款(3)项也采用了类似的相对删除战略,即当删除不能时,用"封锁"代替"删除",正式的《个人信息保护法》又将"封锁"替换成"停止除存储和采取必要的安全保护措施之外的处理"。这从一定程度说明立法者并不局限"封锁"这一种相对删除的策略,为多种"可替代"性删除策略留下解释空间。

就具体的删除途径而言,第一,立法机关、最高人民法院和有关的管理机关必须统一解释删除的内涵,引入相对删除解释路径,并说明在多大程度上可以承认为删除数据。例如,澄清个人行使更正或删除信息的具体情形是什么?对不准确或不完整的信息要删除到何种程度?简而言之,在区块链环境下,需要明确信息主体行使个人信息删除的标准。具体来说,可以将删除解释为无法访问链中的个人信息。从本质上看,无法从区块链自由存取资料就像删除一样。这类似于谷歌事件中从搜索引擎中除名或切断所有网络访问链接的方式。当前技术条件下,完全可以实现节点用户不可访问存储在本节点的数据副本。此解释路径意味着平台方有义务遵守信息主体在数据源位置的删除请求。第二,建议采用区块链技术的行为准则和认证机制。区块链世界有其区别于现实世界的行为准则和认证机制。例如,现实世界通过法律治理,而区块链中,通过节点共识构建起区块链世界的底层信任,节点共识就是区块链世界的法律、通过代码进行自动化决策、存储即所有等。法律融合区块链运行机制才能化解数据治理的现实冲突,对此应当承认节点共识的法律效果。另外关于区块链下代码的运作与法律的冲突问题,简单的数学逻辑代码太过绝对,不可能完全将复杂的现实社会囊括,但可以在简单的功能上提供互动的可能。最后,明确相对删除虽然避免了删除的绝对化,实现了个人数据的个人属性和社会属性的统一,但链中的个人信息可能通过特定的技术手段再次出现。为了防止这种情况发生,必须对信息处理者施加更严格的信息保护义务[7]。

3.2 探索删除权“可替代方案”,缓和实践算力困境

“删除”概念的多维解释路径为解决现有法律框架内的删除权与区块链上的删除困境的矛盾提供方法论。一般来说,不能直接从链中删除数据,但实际上可以通过“可替代”技术手段防止访问数据。从删除目的看,其所追求的的并非技术效果,而是信息自决和完整,而特定可替代技术方案可以在制度上实现删除效果,如对个人信息进行假名化处理、限制或屏蔽链中个人信息的访问路径或者删除公钥。这些方案已经考虑到技术限制和执行成本,是完全物理删除之外能够实现删除效果的替代方案。

3.2.1 利益平衡视角下,通过假名化实现相对删除效果

从现有技术路径看,严格的匿名化被证明是不太可能的。虽然 SHA-256 或 SHA-3 算法已经被法院和欧洲数据保护组织认定为匿名化成功的加密算法[21],但是,随着量子计算等技术的发展,理论上没有技术可以实现完全匿名化[8]。另外,匿名化也会导致用户的相对性,使其与个人人信息的控制权存在冲突。去标识化则按照我国《个保法》规定仅仅是不借助额外信息无法识别特定自然人,而且去标识化的删除路径可能也涉及链上删除,这就陷入难以删除链上信息的思维和实践的怪圈。相比来说,GDPR 规定的假名化不仅优化我国“去标识化”,增加了将额外信息妥善保存的要求,而且考虑到未来高度不确定的技术进步,能够更好地消解删除权和区块链技术架构的内生冲突。这就要求信息控制者从严格的程序路径实现假名化。第一,信息控制者切实履行合理注意义务,关注姓名、身份证号码、地址、性别等与数据主体的原始身份之间的可链接性要素。采取个人信息识别标准类型化思路,根据个人信息可链接性强弱将其分为直接识别性和间接识别性,间接识别性个人信息又可根据特定可识别阈值进行细分[22]。在此基础上根据识别能力和安全风险等级进行后续不同程度去标识义务设置,将信息上链风险保持在可控范围。第二,涉及个人信息必须加密才能上链,具体可以采用哈希函数、非对称加密、椭圆函数加密等方案,这与 CNIL 的建议也是不谋而合。最后,从技术角度提高加密技术的复杂程度,避免加密措施破解导致的侵害风险。通过各种加密技术实现完全假名化处理,那么信息主体请求删除假名化数据时,则可以拒绝删除。

3.2.2 限制或屏蔽链中个人信息的访问路径

承认禁止访问权限在功能上等同于“删除”,这将使区块链与我国保护个人信息的立法结构相一致。无论域外的谷歌被遗忘权案中信息无法被搜索引擎检索,还是我国 NFT 侵权第一案中将 NFT 在区块链上网络上断开并打入地址黑洞可认定停止侵权(杭州互联网法院(2022)浙 0192 民初 1008 号民事判决书),这些都是司法实践对目前缺乏法律规定下进行补救删除的有益尝试。他们本质上是建立一种黑名单系统,限制或屏蔽链中个人信息致使其无法流通和利用,而一旦信息无法被利用,也就失去其社会价值。当前来说,可以在区块链应用程序中嵌入访问与授权系统,开发者一般可以通过协议等永久访问个人信息,用户只有经过授权才可以通过专业工具区块链浏览器访问个人信息,从而实现用户的授权访问。当用户要求更正或删除信息时,仅需要区块链浏览器限制或屏蔽链中个人信息的访问路径即可实现用户不能继续检索。这时,“限制或禁止他人访问”在制度上实现了“删除”的法律效果。

3.3 构建链上和链外双重保障机制,缓解原则冲突

除了上面提到的个人信息假名化外,个人信息还可以直接存储在链下数据库中,只需通过哈希指针链(hash pointer),即应用在区块链技术中的一种数据结构,连接到区块链即可,哈希指针除了储存数据位置之外,还储存了这段数据的哈希值,能够反馈数据是什么以及是否被更改[23]。在这种情况下,实际上是设计两条区块链,一条是访问控制功能链,另一条具有链外存储功能,实现数据管理与数据存储相分离。链外信息由私人区块链控制,个人可以实现对数据的控制。链上信息共享,但只共享依据《个人信息保护法》下创设的匿名数据与哈希指针,不共享内容。实际上,这种链上链外结合的方式已经实现个人信息的删除,当保存目的不再有效或者信息主体行使删除权利时,个人可以删除存储在链外数据库的个人信息。此种方法最佳适用场景是在跨境数据司法管辖。这样可以保证即使在区块链技术下,个人信息保留在其收集的同一司法管辖区内,有效规避管辖权争议。然而,此方法一定程度上需要建立注重隐私的个人信息管理平台,这种引入第三方的行为,可能会损害区块链去中心化的底层技术信任架构。在此基础上,Eberhardt 和 Tai 开发了各种离链计算/链上验证解决方案,不需要引入可靠的第三方[24]。这包括请求/响应模板、链外签名模板和包含内容地址的存储模式。以区块链上内容寻址存储模型为例,将数据存储在可寻址的存储系统中,而不是区块链上,这允许将数据无信任地存储到链外存储系统,因为一旦数据更改,地址就会更改,链接将无效。这种方法不仅提供了更强大的隐私保护,而且大大减少了链中数据的存储和计算。另外,当前随着量子运算的发展,非对称算法已经能够被几秒破译,哈希算法也同样面临巨大威胁。对此一是扩大哈希化范围和强

化哈希手段,研究后量子密码算法(通过特定代数结构抵抗量子运算攻击);二是完善防火墙制度,自动拦截异常链接;三是增强对代码的审查,及时发现修复缺陷[25]。

3.4 运用区分原则,确定链上个人信息控制者

前文所述,我国《个人信息保护法》和《欧盟个人信息保护条例》都运用实质性判断标准来认定个人信息控制者,如果将此标准应用到区块链下可能产生责任泛化的极端结果,即区块链上所有节点控制者全部受到规制或全部不受规制[26]。一些学者认为:个人信息控制者,应是链上具有管理功能的节点[16]。这实际上与 CNIL 的观点相一致。但是,这些观点都有可能将个人作为个人信息控制者,即使由 CNIL 提出的共同参与者构成的联合控制者,本质上信息控制者仍是个人。现实情况是,个人不具备处理他人个人信息的意图和处理能力,将个人作为个人信息控制者会导致权利和义务缺位。另外,区块链去中心化程度不同,信息控制者判断方法也不同。建议采用区分原则,区分区块链类型以及用途确定个人信息实际控制者。首先判断的是区块链是否将用于业务、商业目的,因为只有用于商业目的的区块链才有规制的价值,而且具体的个人信息保护义务也根本不适用纯粹的私人用途的区块链;其次分析各类区块链下具有管理功能并控制数据的节点,因为个人信息控制者实质上就是控制数据的节点。对非公有链来说,节点控制者在技术和事实上控制链上数据,是《个人信息保护法》规定的信息处理者;而对公链来说,情况比较复杂。公链上节点控制者分散在世界各地,各个节点存在目的就是进行验证链上交易,并打包上链,并没有单独控制数据的主观目的和技术条件。因此,公链上的节点控制者并非《个人信息保护法》规定承担信息保护义务的信息控制者,其更类似于互联网下维护网络有效运行的基础设施。虽然,公链上节点控制者不承担信息控制者的义务,但是,基于公链开发出的应用(像 DAPP--去中心化应用)用户信息处理的个人和机构,应当承担个人信息保护义务,将成为个人信息法律上的信息处理者。

4 结 语

数据是数字经济发展的重要资源,加强对数据安全有序利用的保护不仅是我国新时代经济高质量发展的必然要求,也是各国应对大数据时代的共同选择。而区块链的分布式账本技术,是互联网下一种具有创新性的底层技术革命与经济现象。无可否认,由于区块链技术本身的一些技术特性,其与《个人信息保护法》所规定的个人信息权益之间有一些冲突,但是从原理上讲,立法数据保护目的与区块链的目的并没有冲突,冲突的产生源于它的运用。在此意义上,技术途径可以寻求合理设计实现链上删除;制度层面对相关法律法规进行规范的目的解释,明确新情况下“告知同意模式”“删除”等概念新内涵,以更好地实现技术创新与法律规制的良性发展。总之,针对区块链下个人信息的治理,必须以促进区块链技术与个人信息保护融合治理为前提,推动技术与法律的对话,走出技术“自嗨”和规范“封闭”困境。

参 考 文 献

[1] 张成岗. 区块链时代:技术发展、社会变革及风险挑战[J]. 人民论坛·学术前沿,2018(12):33-43.

[2] 李 轩. 区块链赋能政府数据开放的风险及其规制[J/OL]. 北京航空航天大学学报(社会科学版)[2023-02-28]. https://doi.org/10.13766/j.bhsk.1008-2204.2022.0703.

[3] 王禄生,王 爽. 困境溯源与模式创新:基于区块链的个人信息合作治理研究[J]. 中国行政管理,2020(12):56-61.

[4] 罗 勇. 特定识别与容易比照:区块链背景下的个人信息法律界定[J]. 学习探索,2020(3):59-65.

[5] 程 啸. 区块链技术视野下的数据权属问题[J]. 现代法学,2020,42(2):21-132.

[6] 王从光. 区块链技术应用于个人信息保护的法理解读与治理[J]. 西北民族大学学报(哲学社会科学版),2021(6):107-117.

[7] 陈爱飞. 解释论视域下的区块链个人信息删除权[J]. 南京社会科学,2022,(6):110-120.

[8] 齐爱民. 区块链环境中个人信息保护的法律障碍与应对[J]. 现代法学,2022,44(5):180-193.

[9] Sullivan C, Burger E W. E-residency and block-chain[J]. Computer Law&Security Review,2017,33(4):470-481.

[10] 张超文,李佳鹏,孙韶华,等. 数十亿条个人信息明码标价 “潜规则”盛行,售卖泛滥成灾[N]. 经济参考报,2021-04-19(A001).

[11] 王利明. 论个人信息删除权[J]. 东方法学,2022(1):38-52.

[12] 王禄生. 区块链与个人信息保护法律规范的内生冲突及其调和[J]. 法学论坛,2022,37(3):81-95.

[13] 王士博,王海霞. 区块链技术与个人数据保护规范的内源性冲突及调和路径——以欧盟 GDPR 为例[J]. 情报杂志,2023,42(2):142-150,165.

[14] 曾 炜. 欧盟《一般数据保护条例》下区块链的数据保护义务[J]. 科技与法律,2020(4):86-94.

[15] Commission Nationale Information & Libertes (CNIL). Blockchain and the GDPR:Solutions for a responsible use of the blockchain in the context of personal data[EB/OL]. [2023-02-10]. https://www.cnil.fr/ en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data.

[16] 江海洋. 论区块链与个人信息保护之冲突与兼容[J]. 行政法学研究,2021,(4):162-176.

[17] 万 方. 隐私政策中的告知同意原则及其异化[J]. 法律科学(西北政法大学学报),2019,37(2):61-68.

[18] Data Protection Working Party. Opinion 10/2004 on more harmonisd information provisions[EB/OL]. [2023-02-20]. ht-

tps://ec. europa. eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp100_en. pdf.

[19] STOA. Blockchain and the general data protection regulation: Can distributed ledgers be squared with European data protection law? [EB/OL]. [2022-12-01]. https://www. europarl. europa. eu/RegData/et - udes/STUD/2019/634445/EPRS _ STU(2019)634445_EN. pdf.

[20] Information Commissioner's Office of UK. Guide to the UK general data protection regulation[EB/OL]. [2022-11-23]. https://ico. org. uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

[21] Finck M. Blockchains and data protection in the European union [J]. EuropeanData Protection Law Review, 2018,4(1):17-35.

[22] 齐英程. 我国个人信息匿名化规则的检视与替代选择[J]. 环球法律评论,202 1,43(3):52-66.

[23] Mirchandani A. The GDPR-blockchain paradox: exempting permissioned blockchains from the GDPR[J]. The Fordham Intellectual Property, Media & Entertainment Law Journal, 2019, 29(4),1201-1242.

[24] Eberhardt J, Tai S. On or off the blockchain? Insights on off-chaining computation and data [C]//Service - Oriented and Cloud Computing. Springer, Cham, 2017:3-15.

[25] 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[J]. 江西社会科学,2020,40(6):166-175.

[26] Berberich M, Steiner M. Blockchain technology and the GDPR - how to reconcile privacy and distributed ledgers[J]. European Data Protection Law Review, 2016, 2(3):422-426.