DOI:10.19735/j.issn.1006-0863.2020.12.07

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*

王禄生　王　爽

[摘　要] 我国个人信息保护面临个人控制虚化、安全保障弱化、信息共享不足的实践困境。从国家治理体系与治理能力现代化的视角来看,上述困境源起于现有治理框架和治理工具无法有效调和信息主体、信息业者与政府等多元主体的利益冲突。区块链技术因其链式存储、加密算法、分布式架构、共识机制和智能合约的技术特征能够强化个人控制和信息安全,推动个人信息可信共享,为个人信息治理困境的破解提供全新可能。下一阶段需要在“共建共治共享”的理念指导下构建基于区块链的个人信息合作治理模式,以“自主身份认证”为突破口,打造多方参与的许可区块链平台,实现公共服务机构向“信任服务节点”转型。

[关键词] 区块链;个人信息保护;数字身份;合作治理;共建共治共享

[中图分类号] D035　[文献标识码] A　[文章编号] 1006-0863(2020)12-0056-06

2016年12月《“十三五”国家信息化规划》提出“要将区块链作为战略技术加以应用,以抢占新一代信息技术的主导权”后,区块链技术与大数据、人工智能技术一道,成为炙手可热的话题。2019年10月24日,习近平总书记在中央政治局第十八次集体学习时强调,要把区块链作为核心技术自主创新的重要突破口,明确主攻方向,加大投入力度,着力攻克一批关键核心技术,加快推动区块链技术和产业创新发展。这在强化各界对区块链技术的信心的同时也为该技术的发展指明了方向。目前,尽管区块链技术已经取得了一定的先期应用,但主要成果仍然局限在金融领域。实际上,区块链技术的特性与公民个人信息保护具有极强的契合性。然而,学界对区块链与个人信息保护的融合途径尚缺乏理论与技术紧密结合的细致观察。申言之,区块链技术特性如何破解个人信息保护的困境?如果要推动个人信息保护的区块链创新,突破点何在?国家在区块链去中心化的个人信息保护机制中应该扮演何种角色?本文正是对上述问题的一个初步探讨。

一、个人信息保护的实践困境及其成因分析

(一)个人信息保护的实践困境

我国有关个人信息保护的立法一直可以追溯到2000年全国人大常委会出台的《关于维护互联网安全的决定》。其后,个人信息保护日益受到重视并广泛进入不同层级立法。据统计,当前我国个人信息保护规范散落在接近100部法律、行政法规、部门规章、国家标准等规范性文件中。[1]尽管在一定程度上表现为碎片化、术语冲突等问题,但在立法理念上总体采纳以“个人控制论”为核心的人格权保护架构。所谓的“个人控制论”是指信息主体对其个人信息拥有支配和决定的权利。它既是信息主体拥有个人信息权利的标志和宣示,也是个人信息权的核心和其他权能的基础。[2]从世界范围来看,“个人控制论”是英美法系与大陆法系普遍遵循的基本原则。[3]

令人遗憾的却是,经过近二十年的法律适用,个人信息的实际保护水平与规范体系仍有较大差距。在新兴技术的冲击下,传统的个人信息保护架构日益陷入困境。申言之,其一,个人控制虚化。一方面,当前

* 基金项目:国家重点研发计划项目“面向诉讼全流程的一体化便民服务技术及装备研究”(编号:2018YFC0830200)

作者:王禄生,东南大学法学院研究员、东南大学人民法院司法大数据研究基地研究员;王爽,东南大学法学院博士研究生,南京 211189

个人信息生态系统角色更为多元，不再是以往信息主体与信息业者间的简单闭路循环，而是演变为信息主体、信息业者、信息中间商、信息后续利用者等多重主体参与，信息主体对信息的控制权被大大削弱。再加上知情同意机制面临冲击，信息主体的控制权更是被实质架空。另一方面，信息业者对个人信息处理机制的透明度不足。众所周知，个人信息收集与处理的透明度是实现个人控制的重要前提。大数据技术的开发应用使得个人信息极易在信息主体不知晓的情形下被挖掘。[4]其二，信息安全弱化。网络信息传播具有的即时流转与分散难控的特征导致个人信息面临侵害风险，个人信息潜在的价值诱惑以及大数据分析技术的广泛应用进一步加剧了此类风险。近年来，信息安全问题愈演愈烈，呈现出日益复杂的严重态势。其三，信息共享不足。大数据时代，个人信息的社会属性日益强调共享。当前，公民的个人信息由不同的第三方机构掌握，呈现出零散化与非标准化的特点。共识机制的缺乏使得各平台在加速集中数据的同时对外逐步走向自我封闭。个人信息在平台的垄断需求、安全风险、信任困境等多重影响下导致共享严重不足。

（二）个人信息保护实践困境的成因分析

在大数据时代，个人信息兼具人格尊严、商业价值与公共管理价值。因此，个人信息的保护涉及个人（信息主体）、企业（信息业者）和国家多方主体，也必然面临多元的利益冲突。[5]个人信息保护实践困境正是多元利益冲突难以调和所导致的治理困境。

众所周知，伴随着社会信息化的进程，出现了专门以信息的收集、处理、储存、利用和传输为主要业务的信息服务提供者。[6]信息业者的商业应用逻辑与信息主体的个人控制逻辑之间存在着显著张力。首先，商业应用逻辑要求灵活的目的明示与知情同意机制。大数据的价值挖掘往往是在数据样本之上的多次挖掘。在获取数据之初，数据挖掘主体无法完全预测到可能的挖掘目标，也就无法在收集个人信息的同时对个人信息的使用做完整列举。尽管我国法律规范允许个人信息收集者在重新获得用户授权之后调整数据的用途，但却可能面临时间、成本等多方的制约。因此，大数据的应用逻辑一定程度上倾向于概括性的使用授权和灵活的目标调整，这便与个人权利逻辑中知情同意等具体制度设计形成直接的冲突。[7]其次，商业应用逻辑催生中心化数据控制主体并导致安全风险。按照大数据的应用逻辑，信息业者以追求数据库的体量为首要任务，并在控制足够数量个人信息的基础之上通过相关性的挖掘实现大数据的价值。[8]由此，个人信息的收集极易产生中心化主体。世界范围内个人信息泄露事件大都与中心化个人信息控制主体的安全漏洞相关。最后，商业应用逻辑催生数据垄断并阻碍个人信息共享。尽管大数据强调数据的汇聚与联通，但不同中心化主体之间缺乏足够的共识机制，无法实现无障碍的安全共享，与个人信息天然具有的非独占性形成冲突。[9]

可见，信息主体的个人控制逻辑与信息业者的商业应用逻辑处于坐标轴的两端。个人信息保护规范的实施程度既取决于信息主体与信息业者力量对比，又取决于国家对于上述两者张力的调和。实践中，个人与商业主体之间的力量严重失衡，缺乏强有力的对抗手段。因此，国家的个人信息治理成效就将决定个人信息保护的走向。然而，国家的个人信息治理至少存在三大困境：其一，零和博弈。在现有制度框架和治理工具之下，强化信息业者对个人信息的运用势必要以削弱个人控制为代价，反之亦然。其二，角色冲突。在个人信息保护和利用中，政府积极加入其中，具有了利用者和管理者的双重身份角色。[10]作为个人信息最重要的利用者，国家/政府需要时刻回应自我监管有效性的质疑。其三，信息不对称。大数据时代，国家对于网络运营者的外部监管由于技术门槛的存在而导致严重的信息不对称，无法充分发挥作用。

综上所述，从深层成因来看，对个人信息保护困境的解决需要在国家治理体系与治理能力现代化的视角下，将其作为国家治理困境提出和观察。当前个人信息保护中存在的诸多问题源起于国家对个人信息的治理未能充分调和个人控制逻辑与商业应用逻辑冲突。只要治理框架和治理工具未实质更新，信息主体、信息业者与国家的互动关系没有发生根本性的改变，个人信息保护的困境就很可能无法从根本上得以改观。

二、区块链与个人信息保护理念的契合性证成

（一）以强化个人控制为基准的个人信息保护理念

前文已经提及，个人信息保护实践困境来源于国家治理过程中面临的零和博弈、身份冲突与信息不对称等诸多困境。因此，以利益平衡的方式推进个人信息保护与利用的协同发展逐步成为各界共识。随着研究的推进，强化信息应用的路径日益成为主流选项。有学者认为，以“知情同意”为核心的传统保护模式既无法为公民个人信息提供实质性保障，又在实践中成为数据价值开发的障碍。[11]有学者主张为了推进个人信息的有效运用，应当将个人信息视作公共物品而无需设置私权。[12]也有学者认为，考虑到个人信息的社会性与公共性，在个人信息保护相关制度构建中需要平衡个人利益与社会整体利益，建构由“个人控制”向“社会控制”的转变。[13]

上述观点包含共同的理念主线，即以不同程度牺牲或削弱信息主体的个人控制为代价来确保信息自由流通。[14]尽管它们在客观上有利于我国大数据产业的发展，但考虑到我国个人信息保护的现状，以限制/削弱个人控制为代价的个人信息自由流通不应成为新时期个人信息保护的基本理念。首先，我国信息主体与信息业者之间力量悬殊，对于弱势的一方在制度安排中予以倾斜性保护，方能纠正失衡状态。[15]其次，

个人作为目的性的存在，只有消除个人对“信息化形象”被他人操控的疑虑和恐慌，才能有自尊并受到他人尊重地生存与生活。个人信息对于信息主体的人格尊严和自由价值，应当是个人信息立法中首要考虑的因素。[16]因此，在新时期仍然需要坚持以强化个人控制为基准的个人信息保护理念。国家应该提供强大的制度工具来支撑对个人信息全生命周期的有效控制，实现全程可追溯的有序共享。

（二）区块链与新时期个人信息保护理念的契合性

以强化个人控制为基准的个人信息保护理念固然具有理论正当性，但却需要时刻面对可行性的诘问。前文已论及，借助我国现有的治理框架与治理工具，个人控制逻辑与商业应用逻辑之间的冲突难以调和。因此，在明确新时期个人信息保护的基本理念之后，还需要在保持理念系统性与完整性的同时，对不断涌现的技术进步和商业创新保持足够的敏感性。[17]实际上，国内外技术界已经展开了区块链技术应用于个人信息保护的研究，借助区块链技术，不仅能实现数据的可靠存储、同步和分享，还能够避免数据泄露和数据滥用的问题。[18]-[21]可见，区块链技术为强化个人控制基础之上的个人信息有序共享理念的实现提供了全新可能。

1. 强化信息主体的个人控制

我国个人信息保护的规范体系是依据个人控制理念构建。其中，与个人控制最为相关的制度设计便是知情同意。然而，由于个人控制逻辑、商业应用逻辑和公共管理逻辑之间的冲突，文本规范难以被有效执行。区块链技术为强化信息主体的个人控制提供了可能。

其一，区块链链式存储的技术特征所导致的可追溯特性为实现信息主体的个人控制提供了可能。传统架构中，用户控制难使得用户权利几近架空，欧美国家均未提出切实可行的操作机制，尤其未针对用户与第三方机构联系缺失的困境指明正确方向。[22]按照区块链特殊的数据结构，上链数据的区块头都标有时间，用于标记区块生成时间和区块连接顺序，这些数据和时间戳将被永久保存且不可篡改。当任意节点发现不合理问题，都可随时随地逐一查证，实现事件追踪的可追溯。[23]由此清晰界定个人信息的权属，并使得个人信息从收集、使用、流通到计算分析都留存于区块链上，个人信息流转全程可跟踪。其二，区块链加密算法的运用强化了信息主体的个人控制。从技术角度来看，区块链借助加密算法进行数据的传输和共享。个人掌握着配对的公钥和私钥，私钥加密后的上链个人信息只有在个人授权的情况下才能解密使用。个人若无授权，即使链上信息发生节点间的转移，但显示的只是无法破解的密文。

2. 实现个人信息的安全保护

个人信息的安全保障是网络运营者最为重要的义务之一。对此，现有个人信息保护的规范体系均要求网络运营者必须采用必要措施，加强对收集个人信息的安全保障。区块链的技术特征使其形成了一种防篡改、防伪造的数据结构，因此被视为可靠数据库。

首先，区块链的技术特征可以有效防止个人信息数据的泄露。传统大规模个人信息泄露主要两种情况：其一，黑客攻击；其二，持有者售卖。这都是中心化数据存储结构的弊端。区块链可以很好地回应上述弊端。一方面，区块链有完善的加密机制，因此，区块链之上的个人信息明文通常转换为哈希值上链，传输时通过秘钥进行二次甚至多次加密，因此可以在数据共享的基础之上有效保障隐私与安全。另一方面，区块链采用的分布式账本技术可以避免中心化机构被攻破所导致的批量泄露。尽管，分布式的节点实际上都有完整的区块链信息，但正如前文提及的，个人信息不以明文的形式存在，攻破一个节点无法获得所有节点的秘钥，因此也无法破解所有的区块链信息。其次，区块链的技术特征可以有效预防个人信息数据的篡改与伪造。在区块链系统中，由于相连区块间后序区块对前序区块存在验证关系，若要篡改某个区块的数据，就要改变该区块及其所有后序区块数据，并且还须在共识机制的特定时间内改完。因此，参与系统的节点越多，区块链的安全性就越有保证。[24]最后，区块链的技术特征可以有效预防个人信息数据的丢失。分布式存储使得每个节点都有完整的数据备份，因此即使一个节点被黑客攻破，其他节点仍然可以正常运转，数据增加、访问和获取不受影响。

3. 推动个人信息的可信共享

区块链的不可篡改性能有效改善数据篡改、数据造假现象，同时也有助于建立多方共识下的用户信任机制。具体而言，将个人信息上传至区块链中，每个节点都无法更改和删除，链上的任何流程都需经过全网参与主体通过共识机制进行认证，达成共识，如此便形成了一个全网监督互信、共同维护治理的系统。[25]更进一步，借助区块链中的智能合约技术还能预先设定合同条件，在触发时自动完成个人信息的流转。智能合约的嵌入以及代币机制的存在也使得财产权利益在个人信息领域延伸具备可能。

三、基于区块链的个人信息合作治理模式构建与路径展望

（一）基于区块链的个人信息合作治理模式构建

尽管区块链技术特征在整体层面与个人信息治理理念具有高度契合性。然而，宏观理念需要结合具体的机制与方案设计得以落地，尤其需要着力实现强化个人控制基础之上的多元主体利益均衡。此时，就必须借助合作治理的模式。合作治理是政府在行政治理与外部需求不匹配的背景下，引入社会性的治理资源，丰富公共事务中的交换方式，形成复合的治理结构和应对能力。[26]从形式上看，合作治理采取跨部门、跨组织合作的制度安排，其特征是公共机构、营利和非营利机构、社会公众等多元主体的共同努力、互惠互利和

自愿参与。[27]当然，合作治理的理念还要与新时期的国家治理创新结合起来，融入党的十九届四中全会《决定》强调的以科技支撑“共建共治共享”的社会治理创新理念，①形成基于区块链的个人信息合作治理模式。具体而言，就是结合我国个人信息治理的现状和区块链的技术特征，打造一种全新的以强化个人控制为基准的合作治理模式，由信息主体、信息业者、政府共同建设个人信息区块链平台，基于区块链平台展开个人信息收集、储存、传输和利用完整链条的共同治理，推动个人信息的有序共享，真正实现多方主体的利益均衡。

这种区块链支撑的个人信息合作治理模式可以从以下几个方面展开理解：第一，个人信息合作治理的实质是公共服务合作治理的有机组成部分。公共服务合作治理是推进我国国家治理体系与治理能力现代化的重要方面，更是提升公共服务供给质量的时代要求。[28]第二，合作治理模式是以强化个人控制为基准的个人信息保护理念的具体细化，其立足点是通过区块链技术实现信息主体对个人信息的实质控制，在此基础之上推动个人信息的有序共享。第三，合作治理模式吸纳了信息主体、信息业者和国家共同参与。个人信息合作治理模式是对一元主导的政府管理模式的打破，引导信息主体与信息业者共同参与，推动政府职能转变，激发信息业者活力，提升信息主体参与意识，形成多元参与良性互动的格局。合作治理中每一个利益相关者从他人那获得其所需并贡献其所有，以此来建立互惠互利的关系。[29]第四，区块链是个人信息合作治理的关键所在。区块链的技术特性为个人控制逻辑、商业应用逻辑与公共监管逻辑之间的正和博弈提供可能。

（二）基于区块链的个人信息合作治理路径展望

从我国当前个人信息治理的现状出发，结合世界范围内个人信息区块链应用的发展现状，基于区块链的个人信息合作治理模式的路径展开应该以“自主身份认证”为核心突破口，激励信息主体的权利自觉；打造多方参与的个人信息许可区块链应用体系，强化信息业者在许可区块链中的作用；改变国家单纯管理者的角色，推动公共服务机构以TSP信任节点的身份“合作治理”。由此多管齐下，实现个人信息治理机制的创新。

1. 围绕公民“自主身份认证”展开区块链应用创新

个人信息合作治理模式仍然以强化个人控制为基准。从域外经验来看，区块链与个人信息保护结合最为主要的场景便是围绕“数字身份”所推出的基于区块链的“自主身份认证”应用。下一步需要借助区块链技术打造公民“自主身份认证”（self-sovereign identity，简称SSI）的体系。所谓的“数字身份”（digital identity）并非单一的事物，而是公民在数字环境中个人信息的总和，它是一个不断增长和发展的信息集合。在数字身份世界中，附加到某人或某物的身份上的离散信息称为“身份属性”。这种属性实际上有无限可能，比如姓名、年龄、民族、外表、指纹、语音等。[30]“自主身份认证”则是一种去中心化的“数字身份”认证体系，它关注个人对身份的“数字主权”，强调将个人置于整个框架的核心位置，个人对“数字身份”具有绝对的控制权，负责身份数据的维护与上传，自我决定身份数据的使用与浏览权限。实际上，这与我国法律规定不谋而合。《网络安全法》第24条就规定，国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

在传统的架构中，公民的“数字身份”往往被第三方主体掌握。区块链为去中心化的“自主身份认证”提供了现成的基础架构，使得个人可以以去中心化且可信赖的方式自主管理身份数据。具体而言，每名用户可以获得区块链系统发布的私钥，这也是区块链的身份认证。然后，用户可以在私钥的支撑之下添加各种个人信息，通过关联公共机构的可验证凭证，可以创新特定凭证的的数字等效物。每条个人信息的增加都需要所有节点认可的数字签名和时间戳方能写入，确保每条个人信息的可追溯性。与过去相比，“自主身份认证”可以使信息主体选择在何种情况下共享何种个人信息，从而拥有比现在更好的控制权，甚至可以为新的业务模式打开大门，潜在地允许用户在他们希望的情况下通过其个人信息获利。[31]该应用可以作为数字时代的基础设施，产生大量的衍生应用，比如服务于个人征信、身份认证、学历认证、医疗信息共享等领域。

2. 打造多方参与的个人信息许可区块链体系

在明确了以“自主身份认证”作为个人信息区块链应用的核心领域之后，还必须构建区块链的平台体系。从合作治理的模式需求来看，自主身份认证的区块链需要由个人信息收集、存储、传输和利用各环节的多方主体（公共服务机构、社会组织、信息业者、个人）共同建设、共同治理，鼓励多方主体通过彼此协作形成利益共同体。

当前，区块链技术存在具体样态的差异，以“是否需要许可”为标准可分为“无许可区块链”和“许可区块链”。根据场景和设计体系为标准还可分为公共链、联盟链和私有链。[32]一般而言，私有链和联盟链是许可区块链，而公共链则是非许可区块链。不同区块链的区别体现在：其一，在信息开放性层面，公有链系“无许可区块链”，属完全分布式，各节点自由加入，数据呈完全公开状态。“许可区块链”上的数据可以是公开透明的，也可以选择仅内部流通。其二，在参与主体层面，由于公有链可自由进出，使得各节点缺乏清晰的成员边界。[33]“许可区块链”架构从根本上关闭了非授权节点接触数据的渠道，[34]其参与者有能力限制访问，从而使得参与主体相对可控，且可信赖程度较强。[35]

① 实际上，“共建共治共享”的理念在党的十九大就已明确提及，并细化为党委领导、政府负责、社会协同、公众参与、法治保障的二十字方针。十九届四中全会进一步扩展了“共建共治共享”的治理体系，将科技支撑纳入指导方针中。

其三，在责任承担层面。在公链中，所有完整节点都处理信息，难以识别对数据处理负有最终责任的个人或实体。[36]“许可区块链”中节点的加入均经授权，责任追溯较为容易。可见，“许可区块链”比“无许可区块链”能更好地应用于个人信息保护。[37]

更进一步，许可区块链的架构能够有效回应传统合作治理面临的困境，为各方主体解决个人信息共同事务而对各方治理性资源进行交换和共享的平台。其一，信任是合作治理不可或缺的要素。[38]在传统合作治理的模式中，各方主体面临互信构建困难的问题。联盟区块链的架构中，共识机制支撑互信的形成。其二，在信息管理学和组织行为学的视角中，信息共享需要采取有效的治理措施来确保共享者内部的组织有序。[39]与公有链相比，联盟链的参与主体经授权方能加入成为节点，并且在加入时通常达成特定的协议，因此有较为有序的内部组织分工。其三，合作治理还需要通过有效的激励手段来提高主体间的整合效率。对此，区块链架构中代币机制确立了明确而清晰的分配机制。按照分配机制，各方主体基于不同的贡献共享收益。其四，合作治理中多方主体在合作过程中容易出现权责边界不清的问题。[40]联盟链可以在许可主体加入时明确权责边界，降低争议的可能性。

因此，自主身份认证区块链平台应该采用许可区块链的架构。对于非敏感个人信息的保护与共享，可以奉行社会主导的理念，由信息业者牵头建设私有链或联盟链平台；对于特定敏感或重要个人信息的保护与共享，则可以采用政府主导的联盟链模式，由特定公共服务机构发起，明确设定准入的标准与程序，最大范围内吸收社会组织共同参与区块链共识的形成。

3. 推动公共服务机构向“信任服务节点”转型

在个人信息合作治理的架构中，政府仍然是极其重要的一元，一方面需要不断提高自身监管能力；另一方面，也应该以包容性面对区块链创新对传统个人信息监管格局的冲击。由此，在个人信息区块链中，代表政府的公共服务机构需要转变职能，以“信任服务节点”的身份加入到合作治理的框架中。

在当前的身份制度下，数字身份和“离线”身份之间通常存在较弱的联系。这使得创建虚假身份相对容易。[41]区块链应用通常采用平台化的运作，排除操作失误等原因，上链数据在上链前仍然面临真实性的难题。韩国推出的区块链应用 Metadium 虽然取得了不错的成效，但其需要依托官方机构完成个人信息的验证。加拿大的 SecureKey 的推行也得益于 80 种公共服务的加入和数据共享。因此，去中心化的“自主身份认证”区块链应用中，政府不能停留在监管职能的发挥，而是需要在区块链的逻辑中实现功能的转型，即从管理者转向“信任服务提供者”（Trust Service Provider，简称 TSP）。换言之，公共服务主体可以以“信任服务节点”的身份加入到“自主身份认证”的区块链应用建设中。由此，建立个人信息区块链应用的生态圈，打通区块链应用“最后一公里”，破解上链前数据的真实性难题。需要特别指出的是，联盟链的各个节点依据需要可以设置差异化的权限，这与公有链中绝对平等的节点形成区别。在个人信息治理的联盟链架构中，信任服务节点具有超过一般节点的验证权限，因此也构成个人信息区块链的核心。此种定位与合作治理由“政府主导”向“政府负责”转型的需求相一致。换言之，在个人信息合作治理的模式中，政府仍然是最为主要的行动者和协调者。

四、结语

毋庸置疑，区块链技术是个人信息合作治理模式得以顺利实施的关键所在，其发展为国家打破在个人信息治理中面临的零和博弈、角色冲突、信息不对称困境提供了有力支撑。更进一步，基于区块链的个人信息合作治理模式与十九届四中全会以来强调的科技支撑共建共治共享社会治理的路径具有内在逻辑的高度一致性，客观上将为我国国家治理体系和治理能力现代化的理论与实践发展提供有效助益。当然，任何技术都是双刃剑。在肯定区块链应用于个人信息保护前景的同时，我们也不能忽视特定的区块链技术路径可能与个人信息保护规范存在不完全一致性。因此我们在建构基于区块链的合作治理模式时不应该把区块链技术视作一种静态、固化的技术，而是应该根据个人信息法律规范的相关规定，灵活地调整技术实现路径。当然，本文只是对区块链技术在个人信息保护应用场景中的合作治理创新作出初步探讨，在这个领域的推进过程中，仍有诸多理论问题和技术细节值得深入研究，这些都应成为未来研究的努力方向。

[参考文献]

[1]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[J]．重庆大学学报(社会科学版)，2018（12）．

[2][14]王成．个人信息民法保护的模式选择[J]．中国社会科学，2019（6）．

[3]张新宝．“普遍免费+个别付费”：个人信息保护的一个新思维[J]．比较法研究，2018（5）．

[4][11][22]范为．大数据时代个人信息保护的路径重构[J]．环球法律评论，2016（5）．

[5][6][10][16]张新宝．从隐私到个人信息：利益再衡量的理论与制度安排[J]．中国法学，2015(3)．

[7][13]高富平．个人信息保护：从个人控制到社会控制[J]．法学研究，2018（3）．

[8]王秀哲．大数据时代个人信息法律保护制度之重构[J]．法学论坛，2018（6）．

[9]程啸．论大数据时代的个人数据权利[J]．中国社会科学，2018（3）．

[12]丁晓东.个人信息私法保护的困境与出路[J].法学研究,2018(6).
[15]吕炳斌.个人信息权作为民事权利之证成:以知识产权为参照[J].中国法学,2019(4).
[17]郭春镇,马磊.大数据时代个人信息问题的回应型治理[J].法制与社会发展,2020(2).
[18]刘明达等.区块链在数据安全领域的研究进展[J].计算机学报,2020(1).
[19]黄小菊等.基于区块链技术的个人信息管理[J].软件工程,2018(10).
[20]郑露露等.基于区块链技术的个人信息管理系统[J].物联网技术,2018(9).
[21]刘帝,吴鹏.一种基于区块链的个人数据保护模型[J].信息与电脑,2018(21).
[23]中国信息通信研究院.区块链赋能新型智慧城市白皮书(2019年)[EB/OL].http://www.caict.ac.cn/kxyj/qwfb/bps/201911/t20191108_269147.htm.
[24]刘敖迪等.区块链技术及其在信息安全领域的研究进展[J].软件学报,2018(7).
[25]Michèle Finck. *Blockchain and the General Data Protection Regulation*, *European Parliament* (*July 2019*). https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.
[26][40]敬乂嘉.从购买服务到合作治理——政社合作的形态与发展[J].中国行政管理,2014(7).
[27][29]蔡岚.合作治理:现状和前景[J].武汉大学学报(哲学社会科学版),2013(3).
[28][38]王家合,赵喆,柯新利.公共服务合作治理的主要模式与优化对策[J].中国行政管理,2018(11).
[30][31][37][41]Tom Lyons, Ludovic Courcelas and Ken Timsit. *Blockchain and Digital Identity*, *The European Union Blockchain Observatory & Forum* (*2 May 2019*). https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf.
[32]谢辉,王健.区块链技术及其应用研究[J].信息网络安全,2016(9).
[33]丁宇翔.协力保护个人信息安全[N].人民日报,2019-10-15.
[34]祝烈煌等.区块链隐私保护研究综述[J].计算机研究与发展,2017(10).
[35]Anisha Mirchandani, The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR. *Media & Entertainment Law Journal*, 2019(29):1201-1241.
[36]Cristian-Silviu Busoi, Energy Ana Gomes. *On Blockchain:A Forward-looking Trade Policy*, *European Parliament* (*27 November 2018*). https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EN.html.
[39]李仪.大数据下个人信息共享的风险及其知识治理对策[J].管理现代化,2019(6).

(责任编辑 葛 东)

Dilemma Traceability and Model Innovation: Research on Personal Information Cooperative Governance Based on the Blockchain

Wang Lusheng Wang Shuang

[**Abstract**] China's protection of personal information is faced with the dilemma of the loss of personal control, the weakening of security guarantee and the insufficiency of information sharing. From the perspective of modernization of national governance system and governance capacity, the above dilemma originates from the fact that the current governance framework and governance tools cannot effectively resolve the interest conflicts of diversified players such as information subjects, information industry practitioners and the government. The blockchain technology, characterized by the chain storage, encrypted algorithm, distributed architecture, consensus mechanism and smart contract, can strengthen personal control and information security, and promote reliability and sharing of personal information, thereby providing brand-new possibilities for the breaking of personal information governance dilemma.For the next stage, we need to build blockchain-based personal information cooperative governance model under the philosophy of "co-construction, co-governance, and co-sharing", taking the "self-sovereign identity" as the breakthrough, creating permitted blockchain platforms with the participation of multiple players, to realize the transformation from public service institutions to "trust service nodes".

[**Keywords**] blockchain, personal information protection, digital identity, cooperative governance, co-construction, co-governance and co-sharing

[**Authors**] Wang Lusheng is Research Professor at Law School and Research Center for Judicial Big Data, Southeast University; Wang Shuang is Ph.D Candidate at Law School, Southeast University. Nanjing 211189