财经法学 No. 2，2022
pp. 54 - 68

数字防疫中个人信息治理的“链”“法”协同机制研究

胡元聪　龚家锋*

内容提要：在本次疫情防控中，人工智能、大数据等数字技术在降低疫情传播风险的同时使个人信息治理面临新的风险。联盟链近年来在诸多领域得到广泛应用，成为化解数字防疫中个人信息治理风险的可行工具。但在应用联盟链治理风险的同时，还需要对相应制度予以优化，从而在技术迭代与制度优化的作用下实现联盟链与法律的“携手共治”。对此，应当消除联盟链与法律之间的张力，进而构建以法律治理为主、以联盟链治理为辅的“链”“法”协同机制。具体而言，通过构建与法律相匹配的联盟链治理机制及与联盟链相适应的法律治理机制，融合区块链技术和法律各自的优势，以此来提升“链”“法”协同机制在数字防疫中个人信息治理方面的能力，从而提高国家治理现代化水平。

关键词：数字防疫　个人信息治理　风险治理　联盟链　“链”“法”协同

一、研究背景与问题的提出

新型冠状病毒肺炎疫情（以下简称“疫情”）自暴发以来，即在全球迅速蔓延。预计到世界范围内的新冠肺炎疫苗普遍接种前，我国仍将长期处于“外防输入，内防扩散”的常态化疫情防控中。与之前历次突发重大公共卫生事件相比，本次疫情防控的最大特点是“将云计算、大数据、人工智能等新兴技术应用于疫情监测分析、人员流动和社区管理等联防联控的各个方面”〔1〕进

* 胡元聪，西南政法大学经济法学院教授、西南政法大学中国市场经济法治研究中心主任；龚家锋，西南政法大学人工智能法律研究院助理研究员。

本文为国家社科基金重点项目“人工智能研发与应用风险治理的财税法协同机制研究”（21AFX021）、重庆市研究生科研创新项目“疫情防控中个人信息保护的区块链技术进路研究”（CYS20152）的阶段性成果。

〔1〕《工业和信息化部办公厅关于运用新一代信息技术支撑服务数字防疫和复工复产工作的通知》，载 http://www.gov.cn/zhengce/zhengceku/2020-02/19/content_5480843.htm，最后访问时间：2021年1月17日。

行数字防疫。〔2〕但数字技术的不确定性和规制数字技术制度的不确定性导致疫情防控“危”“机”并存：通过对公民个人信息〔3〕的治理〔4〕进行数字防疫，一方面有效地降低了疫情传播风险，另一方面却使公民个人信息面临治理风险。易言之，数字技术为降低疫情传播风险而应用，但数字技术的应用又使个人信息治理产生了新的风险。如何消除数字防疫和个人信息治理之间的冲突龃龉问题以化解个人信息治理之“危”进而利用数字进行防疫之“机”，是数字防疫亟须解决的问题。

具体来讲，随着数字技术的不断应用，越来越多的部门开始大规模搜集和使用个人信息进行分析，与此同时，一些“不当利用个人信息的侵权行为愈发普遍”〔5〕。部分防疫部门实行“地毯式”搜查却可能疏于管理，一些有关疫情的图片、视频和数据等充斥于社交平台，部分确诊或疑似患者的个人信息在网络上广泛流传。在各地推出健康码、行程卡等应用程序和基层登记办法后，大量个人信息既留存于网页、应用程序等数字代码中，也广泛暴露在商超、银行等公共场所入口的纸质登记簿上。这使得为数字防疫而搜集的个人信息产生了治理风险。不同于传统商业领域的个人信息侵害行为，数字防疫搜集的个人信息搜集面广、覆盖人群多。不当利用行为不仅“侵犯了公民的个人隐私权益，可能成为下游犯罪的预备条件”〔6〕，而且增添社会恐慌情绪，给数字防疫增加阻力，甚至“可能危害国家政治安全与社会安全”〔7〕。

区块链技术具有去中心化、可溯源的特点，经过数年的研发创新，已针对不同的应用领域衍化出公有链、联盟链等多种类型。其在业界担忧的去中心化、总量、算力、跨链方面不断改进，〔8〕可能在全球范围内引起新的技术和产业变革〔9〕。我国已逐渐成为区块链技术大国，区块链专利数量位居世界前列。联盟链成为我国区块链技术应用的趋势，其在金融、政府治理、产品溯源等方面多有实践。习近平总书记强调，要发挥区块链技术在促进信息共享、提升协同效率等方面的作用，推进区块链和经济社会融合发展。〔10〕我国《“十四五”规划和2035年远景目标纲要》也提出要以联盟链为重点发展区块链服务平台和应用方案。具体在数字防疫的个人信息治理方面，联盟链在疫情防控和个人信息治理中均已有相关应用：如济南的“区块链＋疫情防控”〔11〕系统、

〔2〕 本文所称“数字防疫”是云计算防疫、大数据防疫和人工智能防疫的总称。

〔3〕 本文所称“个人信息”是指《中华人民共和国民法典》第1034条规定的个人信息，即以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

〔4〕 依照《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）第4条的规定，个人信息的处理包括个人信息的收集、储存、使用、加工、传输、公开等活动。本文所称“个人信息治理”主要是指对个人信息处理行为进行规范的活动。

〔5〕 孙莹：《大规模侵害个人信息高额罚款研究》，载《中国法学》2020年第5期，第106页。

〔6〕 叶名怡：《个人信息的侵权法保护》，载《法学研究》2018年第4期，第88页。

〔7〕《总体国家安全观视角下个人信息保护机制研究》，载http://www.gjbmj.gov.cn/n1/2020/0509/c411145-31702913.html，最后访问时间：2021年1月19日。

〔8〕 参见《利用区块链促进税收管理现代化的研究》课题组、张国钧等：《基于区块链的“互联网＋税务”创新探索——以深圳市税务局的实践为例》，载《税务研究》2019年第1期。

〔9〕 参见中国区块链技术和产业发展论坛：《中国区块链技术和应用发展白皮书（2016）》。

〔10〕 参见《习近平主持中央政治局第十八次集体学习并讲话》，载http://www.gov.cn/xinwen/2019-10/25/content_5444957.htm，最后访问时间：2021年1月19日。

〔11〕《济南全国首发“区块链＋疫情防控”标准》，载http://www.jinan.gov.cn/art/2020/4/10/art_1861_4197790.html，最后访问时间：2021年1月19日。

广州南沙的“疫情防控协同系统”〔12〕等，积极利用联盟链防控疫情；再如中国人民银行主导的“征信链”，利用联盟链确保包括个人信息在内的信用信息安全并推动信息共享〔13〕。此外，联盟链的技术特征与《个人信息保护法》的“信息保护义务”以及数字防疫中政府部门居中管理调度的要求相契合。基于此，本文拟探讨以下四方面的问题：数字防疫对个人信息治理产生了哪些风险，联盟链能否成为化解这些风险的工具，如何处理联盟链和法律在数字防疫中个人信息治理的关系，怎样构建全方位的数字防疫中个人信息治理“链”“法”协同机制。

二、数字防疫中个人信息治理面临的风险

在本次疫情防控中，大数据、人工智能等数字技术筑起了一道道防疫“数字长城”。但受技术特性和应用实践的限制，数字技术给个人信息治理带来了技术风险和制度风险。具体表现在以下三个维度：

（一）个人信息数量激增，挑战防控信息真实性

在本次疫情防控中，政府利用电信企业的通信信息配合其他实名制信息建立了健康码、行程卡等防疫工具。这些工具可以动态跟踪人员流向，从而有效降低疫情传播风险。与此同时，需要处理的个人信息迎来“数据核爆”。以北京“健康宝”为例，其以个人信息和通信信息为基础，出入公共场所必须校验个人“健康宝”信息。这一特殊工具为有效防控疫情、排查人员流向发挥了巨大作用，同时在短时间内产生了海量信息。其自上线以来，使用人数和查询次数激增，后台所需存储的对应信息量持续增高。截至 2021 年 8 月 13 日，其累计查询、使用次数达 79 亿次。〔14〕信息的真实性是数字防疫中个人信息治理的前提。如果不能及时处理激增的个人信息，便会出现挑战防控信息真实性的风险，从而动摇防控信息的真实性基础。“个人信息是大数据和人工智能的原料。”〔15〕激增的海量个人信息具有多样性、价值性和快速性的特点，这就要求防疫部门具备高水平的信息治理能力，以保障数字防疫基础信息的真实性。这对于习惯传统治理模式的各级防疫部门而言可能是一个不小的挑战。部分防疫部门因为防控压力激增，忙于落实防控要求，可能来不及处理激增的海量涉疫信息，进而会影响到防控信息的真实性。同时，个别防疫部门出于政绩考虑或防控压力，主观上可能有漏报、瞒报行为，或者选择性收集对自己有利的信息，这也容易挑战防控信息真实性进而影响到数字防疫的准确性。

（二）个人信息安全危殆，影响防控信息公信力

个人信息安全受到威胁的主要原因在于第三方的处理：若信息只在两个主体间传输，二者对信息的加工、处理涉及的安全问题通常有相关的合意，此时一般不易出现安全风险。但如果不能

〔12〕《打通防疫“数据烟囱”，广州南沙防疫信息化系统上线》，载 http://zfsg.gd.gov.cn/xxfb/dsdt/content/post_2883625.html，最后访问时间：2021 年 1 月 19 日。

〔13〕参见《科技赋能金融，“链”上无限可能》，载 https://www.thepaper.cn/newsDetail_forward_14441734，最后访问时间：2021 年 10 月 10 日。

〔14〕参见《北京市新型冠状病毒肺炎疫情防控工作新闻发布会（第 240 场）》，载 http://www.beijing.gov.cn/shipin/Interviewlive/514.html，最后访问时间：2021 年 11 月 7 日。

〔15〕王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019 年第 6 期，第 125 页。

在涉及第三方处理时实现可溯源，信息就容易被进一步转手并泄露。如在数字防疫中，个人信息往往辗转于多个防控主体之手。频繁的转移为恶意攻击提供了难得的机会，〔16〕出现安全风险在所难免。同时，数字防疫搜集的海量个人信息储存在传统中心化服务器中，通过开放的互联网传输和整合。信息可能没有时间标识，复制成本低，存在较大的泄漏及篡改风险。而常规信息加密方法只能在一定程度上缓解安全风险，并不能彻底防范外部攻击，无法根本解决个人信息的安全问题。信息的安全性及公信力是数字防疫中个人信息治理的根基。如果不能保证数字防疫中个人信息安全，便会出现影响防控信息公信力的风险，进而可能影响到数字防疫的权威。涉疫个人信息一旦被泄漏或篡改，配合防疫的公民隐私便暴露在公众的视线下，将使公民承受巨大的心理和舆论压力。这将影响公民填报信息的积极性并降低其对防控的信任度，进而影响到防控的效率、精度以及防控信息的公信力。以北京“健康宝”为例，其由公权力机关负责运营并受到多重技术保护和严格监管，却也出现了个人信息泄露事件：不法分子在网络上低价售卖大量明星的“健康宝”照片、身份证号码、核酸检测结果等相关个人信息。〔17〕不同于涉疫信息表格、截图、流调报告等泄露事件，该事件源自公共防疫应用程序。即使事故由技术服务商的程序漏洞而非政府的原因引起，也可能使防控信息的公信力受损。

（三）个人信息孤岛阻隔，降低防控信息共享度

“信息孤岛”是指信息被不同的主体储存，因储存、传输标准不统一或缺乏交流渠道等原因成为相互独立的数据集，而无法分享、整合的情形。在数字防疫中，个人信息控制主体众多，仅笔者就接触到三类：其一是基于法律法规授权的主体，如政府、医院等；其二是基于日常业务而成为信息控制者的主体，如电信企业、航空公司等；其三是处于模糊地带的主体，如商场、银行等需要统计人员流向的公共场所。每个信息控制主体都有各自的信息管理系统，信息控制主体之间相互独立，无法共享各自控制的信息。虽然近年来各界对破解“信息孤岛”提出了诸多观点并付诸实践，但受硬件设备和沟通渠道的限制，数字防疫中的“信息孤岛”现象仍然存在。信息的共享度是数字防疫中个人信息治理效率的衡量标准之一。如果不能解决“信息孤岛”问题，便会出现降低防控信息共享度的风险，从而降低防疫协同效率。个人信息控制主体本应相互配合，实现多向信息共享，减少不必要的重复步骤以提升效率。但实践中部分防疫部门仍在一定程度上各自为政，一些信息可能没有及时共享。以 2021 年春节地方政府为落实“就地过年”而排查外地返乡人员为例，部分相同的个人信息因缺乏共享而被多次重复统计。〔18〕在冬季部分地区疫情发散的背景下，各地面临严峻的防控形势。多次重复统计个人信息符合防控形势需要。但相同的个人信息因缺乏共享而被不同的防疫部门多次重复统计，一定程度上提高了防控成本并降低了防控效率。如果防疫部门之间加强信息共享，减少不必要的重复步骤，起码不再要求已经排查过的人员重复填报其他部门已经登记过的信息，则可以在一定程度上加快排查速度，提高信息的利用

〔16〕 参见邢会强：《论数据可携权在我国的引入——以开放银行为视角》，载《政法论丛》2020 年第 2 期。

〔17〕 参见《多名艺人“健康宝照片”遭泄露》，载 https://mp.weixin.qq.com/s/D198CIQsh_R5jaNdFiXeJQ，最后访问时间：2021 年 1 月 19 日。

〔18〕 仅笔者春节返乡就接触到五次统计，其中部分统计内容相同：其一是公民主动上报及相互检举；其二是社区等基层人员逐户排查上报；其三是教育部门统计学生返乡信息；其四是公安部门利用交通实名信息统计；其五是电信、互联网公司等对其用户流向进行分析。

效率。

三、数字防疫中联盟链应用于个人信息治理的可能性

个人信息的处理是数字防疫的必然要求，但数字防疫又给个人信息治理带来了新的风险。联盟链可以为数字防疫中的个人信息治理提供新的思路。联盟链存在多个中心，由多主体共同运行，〔19〕强调效率与秩序的共存〔20〕。联盟链是在克服传统区块链弊端的基础上发展而成的新形态：其不需要引入算力竞争确定写入权，可以节省计算资源和耗能；其节点数量和区块信息存量较少，有效地提高了数据吞吐能力、系统运行速度，并相应扩展了储存空间；多中心化的特征使其更容易完成特定的任务和目标，有利于提升系统的可控性并实现规范、良性监管。联盟链融合了业务去中心化和管理中心化的双重特点，〔21〕既可以解决信息不对称和隐私保护问题，又便于政府实现特定政策目标。因此，联盟链更适合在由政府主导的场景中应用，是各国政府普遍接受的区块链模式。具体在数字防疫的个人信息治理中，联盟链能够缓解当前数字防疫给个人信息治理带来的风险，且符合我国区块链政策推广和疫情防控的要求。因此，可以利用联盟链缓解数字防疫与个人信息治理之间的冲突龃龉问题。

（一）联盟链可以确保信息真实，创建防控优良信息基础

一方面，联盟链可以激励相关主体提供真实信息。“区块链技术创设的激励机制类似于制度机制，是区块链技术的核心机制之一。”〔22〕联盟链属于“无币区块链”〔23〕，一般不涉及节点争夺记账权问题，但也可根据实际需要设置激励层用来部署激励机制〔24〕。对于个人信息的真实性问题，联盟链可以以积分的方式激励防疫主体上传真实信息并激励有权限的部门积极验证信息的真实性。积分可以用于享有获取信息时的优先权或读取其他地域、部门信息的权限等。链上信息的真实性受到上传和验证的双重激励保证，虚假信息在上传或验证的过程中会被淘汰而不会被记录在系统中，从而保障信息的真实性以创建防控优良信息基础。

另一方面，联盟链可以保证信息真实不被篡改。联盟链具有区块链技术的基本链式结构，能够让链上信息一经储存就无法篡改。〔25〕联盟链系统中的每个区块都包含相连区块的哈希值并相互对应，其中任何一个数值的改变都会导致该区块无法与相邻区块对应，进而不被系统承认。因主观原因上传的虚假信息将永久保存至系统中，无法通过先上传后篡改的方式瞒报、漏报。信息的上传和使用数据同样被记录至系统中。一旦发现不实信息，可以通过系统溯源定位责任主体和使用主体，以尽可能减少损失。对于误记、错记信息的更正和变动，如核酸检测结果变化等，可以通过

〔19〕 参见卜学民：《区块链下证券结算的变革、应用与法律回应》，载《财经法学》2019 年第 3 期。

〔20〕 参见高奇琦：《智能革命与国家治理现代化初探》，载《中国社会科学》2020 年第 7 期。

〔21〕 参见马理、朱硕：《区块链技术在支付结算领域的应用与风险》，载《金融评论》2018 年第 4 期。

〔22〕 胡元聪：《正外部性的经济法激励机制研究》，人民出版社 2021 年版，第 15 页。

〔23〕 邓建鹏：《区块链的规范监管：困境和出路》，载《财经法学》2019 年第 3 期，第 36 页。

〔24〕 参见张楠迪扬：《区块链政务服务：技术赋能与行政权力重构》，载《中国行政管理》2020 年第 1 期。

〔25〕 参见徐琳、袁光：《区块链：大数据时代破解政府治理数字难题之有效工具》，载《上海大学学报（社会科学版）》2020 年第 2 期。

覆盖原有信息以完成，但原有信息不能被删除。此外，“联盟链上的节点采用了实名制的方式”〔26〕，身份相对透明。如果某一节点尝试篡改链上信息，破坏诚信的成本高昂也会使其有所忌惮。

（二）联盟链能够保障信息安全，增强防控信息公信力

一方面，联盟链可以保障信息系统内部安全。优化加密技术是个人信息和隐私保护领域的常用方案。而联盟链的非对称加密技术可以保障联盟链系统内部的信息使用和传输安全。在非对称加密技术的支持下，联盟链上的节点在其权限范围内读写信息。虽然各节点均储存全量账本，但在被系统授权之前，并不意味着该节点自动具备阅读全部账本的权限。这刚好契合防疫部门拥有的信息处理权限差异，即不同节点拥有不同的读写权限。如图 1 所示，可以通过哈希算法将防疫主体 A 上传的个人信息去标识化处理后储存，并借助非对称加密技术对读写权限进行限制，即权限不同的防疫主体对去标识化信息复原程度不同。防疫主体 B 根据其权限对信息复原后使用。这种根据权限非对称加密的有限共享方式，可以有效防控个人信息被泄漏的风险。这就确保了个人信息不会从系统内部泄漏从而增强防控信息公信力。

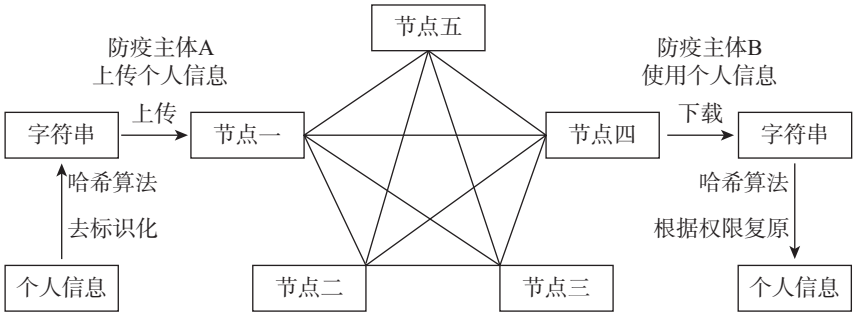

图 1　联盟链去标识化、复原个人信息示意图

另一方面，联盟链可以保证信息系统外部安全。哈希算法可以将储存的个人信息转化为无法破解的 256 位字符串。同时，系统仅保存由算法随机计算得来的字符串，系统外的其他主体无法获得系统内储存的字符串。而系统内的链上节点（即防疫主体）则可以通过匹配私钥和公钥的方式获取个人信息。即使系统因后门漏洞或外部攻击等原因泄露了字符串，也会因为私钥与公钥不匹配、没有签名等原因无法破解其代表的个人信息，不法分子也难以将有限的字符串用于其他用途。此外，联盟链的节点更容易达成新共识，便于进行系统的维护与升级，其算法、协议和加密技术都可以通过中心节点进行更新和审查，相较于其他区块链系统更利于抵抗黑客的外部攻击。〔27〕

（三）联盟链可以促进信息共享，提升防控合作协同效率

一方面，联盟链可以破解信息共享壁垒。联盟链的分布式记账本实质上是一种在节点之间共享、复制和同步的数据库，可以破解信息壁垒，〔28〕进而提高防控合作协同程度及信息治理效率。

〔26〕 翟晨曦、徐伟等：《区块链在我国证券市场的应用与监管研究》，载《金融监管研究》2018 年第 7 期，第 35 页。

〔27〕 参见王延川：《“除魅”区块链：去中心化、新中心化与再中心化》，载《西安交通大学学报（社会科学版）》2020 年第 3 期。

〔28〕 参见胡元聪、谢凤：《智慧司法下数据保护困境突破的区块链技术进路》，载《科技与法律（中英文）》2021 年第 6 期。

通过分布式记账本，防疫主体储存的信息、上传使用记录等储存在系统的每一个节点上。每个节点都是一个信息单元，系统储存的信息在每个单元上记录并共享。只要信息发生变动，就会自动同步记录至所有节点，其他节点则可以根据权限实时读取。同时联盟链只针对特定成员开放，成员需经准入才可参与。这就要求各节点统一信息的上传、储存和传输标准，否则便不能加入系统。这种准入机制一定程度上提高了系统交易性能，可以避免因成员的参差不齐而产生新问题，也在一定程度上缓解了信息不对称问题。〔29〕由此实现链上主体间的信息共享，有效打破“信息孤岛”以提升防控合作协同效率。

另一方面，联盟链可以提高信息共享程度。“代码即信任，是区块链技术的精髓。”〔30〕区块链技术通过算法加持信任以创造良性的去信任化环境，〔31〕利用计算机程序构建新型信任关系，实现点对点交流。联盟链中的节点均通过一定程序获得入链许可和准入，节点所代表的防疫主体资格有一定的保障。且上链信息已经过验证，原本并无合作关系、互不认识的防疫主体之间也无须担心信息的真实性与来源的可靠性，无须经过第三方认证或公证便可直接获取并使用。由此提升了防疫主体的信息共享程度进而提升防控合作效率。此外，可以通过智能合约技术确定信息共享程序，明确防疫主体获取信息的条件以及紧急情况下临时读取信息的处理规则，用代码的方式规范信息共享程序进而提高防控合作协同效率。

联盟链对于化解数字防疫给个人信息治理带来的风险具有天然的优势，在本次数字防疫中也已有相关实践。如广州市南沙区基于“南沙城市大脑”建立了“疫情防控协同系统”，将公安部门、卫生部门、工信部门加入联盟链中。通过联盟链汇总整合了涉疫人员相关个人信息、物资信息等防疫信息，在确保信息真实性、安全性的同时打通了各部门的“信息壁垒”。该系统利用联盟链的不可篡改特征实现企业登记备案的防疫信息不可篡改，保证了信息治理的真实性基础；利用非对称加密机制和哈希算法保障防控重点区域人员涉疫信息安全，提升了防控信息公信力；利用分布式记账本等实现区域内各部门的相关信息实时共享，提高了信息治理效率；利用智能合约技术为相关企业疫情防控承诺提高可信度。“南沙疫情防控协同系统”利用联盟链构建了传播过程不可逆、可有效溯源追踪且有约束力的信息治理系统，为数字防疫中个人信息的治理联盟链的应用提供了一定的经验。

四、数字防疫中“链”“法”协同机制的理论基础

联盟链因其特殊的技术架构对于化解数字防疫给个人信息治理带来的风险具有积极作用，但联盟链的技术特征与传统法律模式也存在天然的矛盾。联盟链虽然经过多中心化改造，对于政府实现特定政策目标和监管具有积极意义，但联盟链毕竟采用了区块链技术的基本架构，其应用将导致传统技术逻辑和业务逻辑发生较大变化，使传统法律法规的适用产生新问题。因此，应当妥善处理二者之间的关系。下面将对区块链技术与法律，即“链”“法”的关系模式进行分析，以

〔29〕 参见张礼卿、吴桐：《区块链在金融领域的应用：理论依据、现实困境与破解策略》，载《改革》2019 年第 12 期。
〔30〕 任仲平：《区块链领导干部读本》，人民日报出版社 2018 年版，第 10 页。
〔31〕 参见赵增奎：《以区块链技术推动互联网金融稳健发展研究》，载《经济纵横》2017 年第 11 期。

求得在数字防疫的个人信息治理中，联盟链与法律之间的最优“相处模式”，通过消除联盟链和法律之间的张力，使二者相互“磨合”，构建“链”“法”协同机制以提升其在数字防疫中个人信息治理方面的能力。

（一）“链”“法”的关系模式类型及评析

1.“链”“法”的关系模式类型

自科技革命以来，如何协调法律与新兴技术之间的关系成为人类社会发展面临的重要议题。新兴技术在基因改造、生物克隆、自动驾驶、信息交流等方面带来了空前的福利，也对现有法律产生了严峻的挑战。“技术一旦进入社会领域，必然会被社会制度、社会组织和社会群体的各种利益、诉求和价值判断所塑造和限制。”〔32〕目前，“链”“法”之间的关系主要有三种类型：管制模式、替代模式和互补模式。管制模式表现为国家通过法律对区块链技术进行严格管制，其坚持较为传统与保守的理念。如果区块链技术可以实现特定社会目标，就通过法律对区块链技术进行保护和激励；如果区块链技术不能实现目标，就要通过法律进行压制。〔33〕源于金融危机等历史原因，一些国家对虚拟货币和区块链技术采取非常谨慎的态度，因为担心技术创新和应用会对社会产生负面影响，所以对区块链技术进行严格管制。替代模式与管制模式截然相反，其是处理“链”“法”关系的前卫观点，认为区块链技术可以完全替代法律，即“政府可以利用区块链技术建立自己的规则系统，通过自动执行的代码系统以带来规则执行效果和效率的革命性提升”〔34〕。这种“代码即法律”的观点在国外已有诸多探讨。与前两种模式不同，互补模式介于管制模式和替代模式之间，其认为“链”“法”各有优势，应当发挥二者各自优势从而构建“链”“法”的共同应用模式。即应当在现有法律制度较为完备的情况下，应将区块链技术作为技术手段，补充现有法律以提高效率并降低交易成本。如“区块链＋发票”，通过应用区块链技术加强税收征管，促进了税收管理制度的完善。

2.“链”“法”的关系模式评析

管制模式和替代模式都是“链”“法”“分立”并相互“对抗”的结果。在管制模式中，法律占据了上风：面对区块链技术应用带来的挑战，法律拒绝做出大的调整，其强势要求区块链技术为符合社会利益而调整。这种模式可以最大程度上防范风险，对区块链技术应用暴露的安全性问题可以及时制止，但是其也会导致诸多负面影响：一方面简单将法律作为压制技术的工具，既否定了法律独特的治理价值，也破坏了法律实践的自主性及法律自身所具有的教义学结构；另一方面也否定了区块链技术的社会建构价值，最终破坏区块链技术的社会效用。在替代模式中，区块链技术获得了胜利：法律顺应区块链技术的价值进行自我调整和革新。但用区块链技术和代码完全替代法律未免过于极端。区块链技术是近年出现的新型信息技术，在智能合约、自动执行等方面迅猛发展。其作为一种去中心化的、安全的、难以破坏的数据簿，虽有自身的价值，但也有固

〔32〕 郑玉双：《破解技术中立难题——法律与科技之关系的法理学再思》，载《华东政法大学学报》2018 年第 1 期，第 87 页。

〔33〕 参见赵小勇：《法律与技术如何相处：区块链时代犯罪治理模式的双重重构》，载《探索与争鸣》2020 年第 9 期。

〔34〕〔法〕普里马韦拉·德·菲利皮、〔美〕亚伦·赖特：《监管区块链——代码之治》，卫东亮译，中信出版集团 2019 年版，第 211 页。

有的缺陷。用代码完全取代法律规则并不可行，也不合常理。法律作为带有国家意志的强制性社会规范，有其自身的优势并可持续修改完善，仍将长期作为规制社会信任的规则。在互补模式中，区块链技术与法律非但不会相互“对抗”，还可能“携手共进”，呈现相辅相成的关系。易言之，法律展现了对区块链技术的宽容，在现有法律框架内对区块链技术的应用进行回应。事实上，法律和区块链技术各有优势，区块链技术可以利用代码更好地实现事前预防和事中规范，法律凭借其强制力、规范性等可以实施有力的事后追责救济和监管。总之，区块链技术和法律各具优势，可以取长补短，通过区块链技术的应用补充和保障法律的实施。

（二）“链”“法”协同机制的选择原因及思路构想

1.“链”“法”协同机制的选择原因

联盟链对于化解数字防疫给个人信息治理带来的风险具有独特的优势，但是联盟链并不能完全替代法律，因为联盟链同样具有区块链技术自身的局限性。联盟链虽然经过多中心化改造，但同样具备分布式记账本的特征，其诞生之初就可能带有除实现特定目标之外的其他主观目的。〔35〕同时，“代码并不比制度更中立，其也受制于垄断和商业利益”〔36〕。此外，区块链技术虽然建立了特殊的信任系统，但信任系统并非完美无缺：其以现代密码技术为基础，仍存在被攻破的可能性；系统的安全和稳定还在不断地发展和变化之中，选择最优的运营模式还需一定时间；智能合约和其他软件代码一样也存在误差和安全漏洞，加之系统直接运作信息价值或财产权利，智能合约误差和漏洞的存在就显得极其危险；现有智能合约技术距离支撑法律的自动执行还有一定的差距。〔37〕因此，存在的悖论是：区块链技术为降低风险而应用，但区块链技术的应用带来了新的风险，其应用带来的外部性问题仍需要法律进行解决。

在数字防疫中，联盟链也无法全部取代法律在个人信息治理方面的作用。法律规范由人类语言构成，具有灵活性和模糊性，“具备通过不断的调试和进化来妥善处理新生事物的能力”〔38〕，可以适应立法者立法时不能预见到的各种偶然性。联盟链由代码语言构成，具有机械性和确定性，只能适用于可以客观验证并已经在底层代码中预先定义的规则。将人类语言构成的开放式法律转化为代码，容易产生歪曲法律含义的风险。这里存在的悖论是：虽然区块链技术是面向未来的技术，但其也无法适应编写时不可预见的未来。由于代码语言的确定性，用严格和正式语言编写的技术治理规则通常无法适用于处于法律灰色地带的意外案件，也很难提前充分考虑并在基础代码中写入即将出现的所有可能性。在出现更先进的“强人工智能系统”之前，代码对于数字防疫中个人信息治理方面可能出现的不可预见情况缺乏适应和解释能力。此外，法律可以通过强制力处罚公民财产、限制人身自由甚至剥夺公民生命，且有一定程度的纠错可能，而代码却无法承担如此重负：一旦代码误判、错判，当事人就会面临人身和财产被代码自动执行而受到严重侵害并无法纠错的巨大风险。因此，技术的迭代并不能完全代替制度的作用，联盟链也不能完全代替

〔35〕 参见赵蕾、曹建峰：《从“代码即法律”到“法律即代码”——以区块链作为一种互联网监管技术为切入点》，载《科技与法律》2018 年第 5 期。

〔36〕〔英〕罗伯特·赫里安：《批判区块链》，王延川、郭明龙译，上海人民出版社 2019 年版，第 32 页。

〔37〕 参见〔美〕凯文·沃巴赫：《链之以法——区块链值得信任吗?》，林少伟译，上海人民出版社 2019 年版，第 47 页。

〔38〕 殷秋实：《智能汽车的侵权法问题与应对》，载《法律科学（西北政法大学学报）》2018 年第 5 期，第 48 页。

法律。在应用联盟链治理风险的同时还需要对相应制度进行优化，从而在技术迭代与制度优化的作用下实现联盟链与法律的“携手共治”。基于此，我们认为，“技制共治”开辟了提升国家治理能力的新路径。

2.“链”“法”协同机制的思路构想

在数字防疫的个人信息治理中，可以采用互补模式，融合“链”“法”的优势构建协同治理机制。“如果现有法律信任结构仍可以普遍适用，按照现有的法律规则能够进行一定程度上的规制，那么区块链技术应该成为法律的补充和保障，其主要价值在于提升信息记录的效率和安全。”〔39〕管制模式和替代模式都有其不足，二者代表的区块链技术与法律分立的观点会带来各种弊端并增加区块链技术创新和传统法律之间的冲突龃龉问题。此外，联盟链和法律在数字防疫的个人信息治理中均有规范、保护个人信息的功能，只是实施方式和手段有所不同。联盟链通过技术手段，利用代码建立自动执行模式，规范个人信息的储存、利用程序，从技术角度实现对个人信息的技术治理。而法律通过制度手段，利用强制力规范各方权利、义务和责任，从制度角度实现对个人信息的法律治理。技术治理与法律治理尽管在治理逻辑上存在差异，但二者也存在巨大的互补性。正确处理技术治理与法律治理的关系，形成共治结构，是提升我国治理水平和能力的前提。〔40〕基于此，可以采用“链”“法”的互补模式。在数字防疫中，可以利用联盟链和法律各自的优势，采取联盟链和法律协同作用的个人信息综合治理模式，构建以法律为主体、以联盟链为辅助的“链”“法”协同治理机制。

具体而言，在“链”“法”协同治理机制中，联盟链和法律的分工有所不同。一方面，法律是数字防疫中个人信息治理的基础和前提。法律在此主要起到明确联盟链的法律地位和效力、实现追责救济、实现全程动态监管的作用。首先，法律可以明确联盟链在数字防疫中个人信息治理方面的法律地位和效力。法律具有普遍性的特征，可以根据数字技术的特征、个人信息的治理需求及疫情防控形势，明确联盟链的法律地位以及分布式记账本、智能合约等技术的法律效力，做到有法可依。其次，法律可以实现事后的追责与救济。法律具有国家强制力的特点，可以配合联盟链的溯源机制确定相关案件的事实问题，对相关案件起到定分止争的作用，对责任主体和损害主体进行强有力的追责和救济。最后，法律可以实现全程动态监管。法律具有规范性的特点，可以配合联盟链的多中心化特征进行实时监管，转变原有事前准入、事后监督的传统监管模式为实时发现风险、及时处理并加以预防的全程动态监管模式。

另一方面，联盟链是数字防疫中个人信息治理的保障和补充。联盟链在此主要起到降低个人信息治理风险、帮助法律进行追责和监管、一定程度上替代规则的作用。首先，联盟链可以降低数字技术对个人信息治理产生的风险。如前文所述，面对数字技术对个人信息治理可能产生的风险，联盟链可以提升个人信息治理的真实性以创建优良信息基础，能够保障个人信息的安全性以提升信息公信力，可以促进个人信息的共享程度以提升协同效率。其次，联盟链可以助力法律进行追责和监管。联盟链作为一种技术解决方案，有其自身的优势，从而帮助法律提升实施效果。

〔39〕〔美〕凯文·沃巴赫、林少伟：《信任，但需要验证：论区块链为何需要法律》，载《东方法学》2018年第4期，第107页。

〔40〕参见郑智航：《网络社会法律治理与技术治理的二元共治》，载《中国法学》2018年第2期。

如联盟链多中心化的特征可以帮助法律进行监管从而实现疫情的精准防控。再如数字时代个人信息保护的重点应当由传统的事前保护转移到事中、事后的保护，〔41〕而联盟链可以配合法律在数字防疫中规范个人信息的事前收集、事中处理的程序，以及在事后救济的取证方面提供助力。最后，联盟链可以实现一定程度上代替规则自动运行的作用。利用代码创设的自动化应用程序可以在一定程度上代替相关制度规则。如监管部门可以利用代码在监管节点创设自动执行的监管程序。当系统达到特定要求即可能产生风险时，自动发出警示以要求相关节点说明情况，甚至暂缓传输信息，以此代替原有规范性文件规定的相关程序性风险防范规则。

五、数字防疫中“链”“法”协同机制的构建思路

（一）构建与法律相匹配的联盟链治理机制

如前所述，联盟链是数字防疫中个人信息治理的保障和补充。在“链”“法”协同治理机制中，首先需要构建与法律相匹配的个人信息联盟链治理机制，即建立个人信息联盟链治理系统。这一过程既要动态认识联盟链的优势与法律的相对劣势，也要考虑我国数字防疫的现实，具体可以从以下三个方面展开：

1. 制定联盟链底层技术标准

联盟链作为新兴技术，其在数字防疫中的应用应当首先明确其使用的底层技术标准。建设数字防疫中个人信息治理的联盟链系统将是一个复杂的系统性工程，“链”与“非链”信息系统将长期共存。如果不能采用统一的信息格式和标准，则“容易引发系统错误、混乱等风险”〔42〕，也无法实现不同信息系统之间的信息互通。信息只能在联盟链系统内流通，使联盟链系统成为更大的“信息孤岛”，即“区块链孤岛”〔43〕，从而不能实现本质上的信息共享。制定统一的联盟链底层技术标准，可以彻底打破“信息孤岛”现象，使个人信息在“链”与“非链”中有序共享，从而提升信息治理效率；也可以为联盟链在其他领域的应用提供标准和参考，从而推动区块链产业协同发展。当前区块链产业仍处于发展初期，存在一定程度的行业乱象，各区块链服务商的技术水平和研发能力均有待加强。制定统一的联盟链底层技术标准，可以为区块链技术服务商提供标准指导，从而推进防疫主体控制的个人信息持续上链存储；也可以为数字防疫中的个人信息治理提供相关决策和监督尺度参考，从而提升监管能力和安全保障水平。本文建议：应当由防疫主管部门和工信部门负责，会同科研机构、专家学者立足现有联盟链成果，参考现有技术规范，制定数字防疫中个人信息治理联盟链系统底层技术标准，明确数据接口、共识机制、分布式记账、智能合约等代码标准和加密程度、算力空间、登录 IP 地址限制等运行规则；应当围绕数字防疫的紧迫性、个人信息的安全性需求和联盟链的优势提出此联盟链系统的底层技术要求，明确该系统的建设及运行标准；确保数字防疫中个人信息治理联盟链系统规范建立并良性运行，保证其和其他“链”与“非链”信息系统协同发展。

---

〔41〕 参见邢会强：《大数据时代个人金融信息的保护与利用》，载《东方法学》2021 年第 1 期。

〔42〕 杨东：《链金有法——区块链商业实践与法律指南》，北京航空航天大学出版社 2017 年版，第 309 页。

〔43〕 胡元聪：《区块链技术激励机制的制度价值考察》，载《现代法学》2021 年第 2 期，第 153 页。

2. 构建联盟链应用平台框架

联盟链对于化解数字防疫给个人信息治理带来的风险具有天然的优势，其多中心化的特征也有利于政府统一管理，从而实现精准防控。可以利用联盟链搭建数字防疫中个人信息治理的应用平台框架，建立包括监管部门、防疫主体（包括公权力防疫部门和社会防疫主体）在内的多中心联盟链系统。疫情防控需要社会各界共同参与，在国家的统一管理下实现联防联控。因此，新系统既要强化国家的中心管理作用，也要注重各行各业的参与。〔44〕在联盟链治理系统中，应当由各级政府和监管部门成为中心节点，强化国家的中心管理作用；并采用政府主导、法律政策推动的形式，将数字防疫中涉及的其他公权力防疫部门、相关社会防疫主体作为普通节点纳入系统中，使涉及疫情防控和个人信息治理的部门、企业一起联防联控，形成“共治”〔45〕机制。并根据数字防疫和个人信息治理的特点，在系统存储总量、响应速度等方面优化改进。对此，可以通过规范性文件明确各级政府和监管部门的中心节点资格，并明确其他公权力防疫部门、相关社会防疫主体的普通节点资格，并排除其他主体的节点资格。此外，可以在系统中设立没有写入权限的访问节点，供其他没有成为系统节点的主体获取信息。在数字防疫中，自然人作为信息的被处理者具有随机性，而个别社会防疫主体如社区、村委会等不容易满足加入联盟链的设备条件和制度要求，因而这些主体不被纳入联盟链系统中。但是，可以通过联盟链上没有写入权限的统一访问节点，使自然人访问其在系统中储存的本人和亲属的个人信息供其他防疫主体校验，从而使社区、村委会等个别没有成为节点的社会防疫主体也可以通过联盟链获取其权限范围内的相关防疫信息，由此在保障联盟链技术性能的前提下提升联盟链的覆盖范围，使更多主体分享技术迭代带来的“红利”。

3. 建立联盟链技术处理规则

具有规范、安全的技术处理规则是联盟链系统有序运行的前提。在联盟链系统的建设及运行过程中，应当依托现有地方联盟链防疫系统，建立信息上传、利用的技术处理规则，保证数字防疫中个人信息的安全利用。

首先，应当建立信息上传的技术处理规则，结合实践分批上传个人信息。数字防疫中涉及的个人信息数量众多，信息入链的先后顺序需要得到规范。因此，应当建立信息上传的技术处理规则，结合当前我国疫情防控实际和联盟链发展现实，根据地域分批建立联盟链系统，依据涉疫程度分批上传个人信息：其一是依托现有济南、广州等地的联盟链防疫系统优先上传济南、广州等联盟链防疫实践地区的疫苗接种者、确诊、疑似、无症状患者及密切接触者的个人信息；其二是上传当前及近期中、高风险地区的疫苗接种者、确诊、疑似、无症状患者及密切接触者的个人信息；其三是上传当前及近期中、高风险地区其他人员、境外入境人员、高危感染人员的个人信息；其四是进行疫苗接种者、曾经确诊、疑似及无症状感染者的个人信息上传；其五是进行全国范围内的普遍上传。

其次，应当建立信息利用的技术处理规则，按照分层分级储存、根据权限下载的原则利用个

〔44〕 参见黄茂汉：《基于区块链技术的疫情防控情报系统模型研究》，载《情报科学》2021 年第 8 期。

〔45〕 杨杨、杜剑等：《区块链技术对税收征纳双方的影响探析》，载《税务研究》2019 年第 2 期，第 116 页。

人信息。数字防疫中涉及的信息处理主体众多，个人信息的利用程序需要得到规范。因此，应当建立信息利用的技术处理规则，将节点搜集到的个人信息根据不同属性和来源利用非对称加密技术分级、分层储存，并依照防疫部门的权限确定其访问和使用的边界。个人信息在节点去标识化上链储存后，分为不同保密级别的信息。保密级别较低的信息主要包括去标识化的身份信息、活动轨迹等基础信息，对防疫主体的访问权限限制较低。保密级别较高的信息主要包括实名身份信息、接触史等个人涉疫信息，只允许具有较高权限的防疫主体访问。应当通过联盟链的共识机制和非对称加密机制设立差异化的信息访问权限，以此保证个人信息安全。

（二）构建与联盟链相适应的法律治理机制

法律是数字防疫中个人信息治理的前提和基础。在“链”“法”协同治理机制中，需要构建与联盟链相适应的数字防疫个人信息法律治理机制。法律应当改变传统的治理模式，适应联盟链环境并与之共同构建全方位的协同治理机制。具体可以从以下三个方面展开：

1. 明确联盟链的法律地位和效力

推动联盟链在数字防疫中个人信息治理方面的应用，应当考虑相关技术应用的法律基础，明确联盟链的法律地位和法律效力是“链”“法”协同作用的前提。首先，应当明确联盟链的法律地位。目前，我国个人信息治理的法律规则规定于由《民法典》和《个人信息保护法》组成的个人信息保护制度体系中，但其未对重大突发公共卫生事件背景下个人信息的治理和智能技术的应用给予明确规定，而仅为一些纲领性的总括，导致这一特殊背景下智能技术在个人信息应用方面的相关法律规范仍分散于诸多法律文本中。而联盟链对个人信息治理具有重大促进作用，将从技术手段破解原有信息治理难题。对此，应当肯定联盟链作为治理手段和治理工具的法律地位，并制定相关激励条款，肯定并鼓励联盟链在个人信息治理方面的应用，促进联盟链乃至智能技术在个人信息治理方面相关产业的发展。其次，应当明确联盟链的法律效力。目前，联盟链已经在司法层面初步得到肯定。最高人民法院在《关于互联网法院审理案件若干问题的规定》中对于利用哈希值校验、区块链技术搜集的证据予以认可，部分司法裁判中也已肯定利用区块链技术存证的法律效力。〔46〕但如果想让联盟链在数字防疫和个人信息治理中更好地发挥作用，需要给予更高层面的确认。联盟链可以成为法律的补充，和法律协同化解数字防疫给个人信息治理带来的风险。因此，应当出台相关法规或调整相应规范，对联盟链的分布式记账本的信息记录、智能合约等有效性进行确认，肯定联盟链在个人信息治理方面的法律效力。

2. 构建适合联盟链的节点责任制度

构建基于联盟链的节点责任制度是法律适应联盟链分布式分类账环境的重要转变。联盟链的分布式记账使得系统内并不存在传统平台上的唯一中心化管理主体，原中心化职能被分散给相关多个中心节点。故在“链”“法”协同机制中，为适应联盟链这一特征，可以立足于系统节点，建立适应联盟链的节点责任制度。

首先，应当通过法律明确节点为责任主体。节点对于分布式记账本具有重要意义，是整个联盟链系统的参与主体，系统通过节点之间的相互验证、记录得以运转。联盟链的节点身份固定且

〔46〕 参见吴京辉、胡兰：《区块链技术助推中小企业票据融资的法律完善》，载《江西社会科学》2019 年第 12 期。

透明，由防疫部门、监管部门组成，可以准确定位节点对应的防控主体，并不存在其他区块链系统因节点匿名而无法追责的问题。根据本次防控实践，个人信息可能部分泄漏于防疫机关。因此，应当明确联盟链系统节点的责任主体资格，即节点应当作为承担责任的主体。其次，应当明确系统节点的责任内容。我国对区块链系统节点的义务与责任已有初步规定。国家网信办《区块链信息服务管理规定》规定了提供区块链信息服务的主体或节点的管理、配合监管等义务及相关的责任，但该文本中的规定较为粗糙，更多的是一些纲领性的宣誓条款，其中一些概念的具体含义并不明确。〔47〕因此，应当对该部门规章进行修改，或就该文本展开进一步的解释与探讨。在数字防疫中，应当明确防疫主体在原信息处理相关义务外，作为联盟链系统节点而具有的权利、义务和责任，并明确其责任形式及追责程序。通过追责弥补联盟链“技治”无法涵盖的部分漏洞和不足，如联盟链可以通过激励机制保证链上信息的真实性，但对于上传前信息的真实性无法保证，对此可以发挥法律的约束功能，明确上传虚假信息的责任和相关过错或知情方的责任以弥补联盟链的不足，实现联盟链的技术激励与法律的制度约束的协同。同时，对于节点责任的形式应当注重民事、刑事和行政责任的并用，在对违反义务的行为加大行政处罚力度的同时辅以民事赔偿责任。此外，还要明确节点代表主体责任人的责任并落实到人，对于达到刑事责任标准的行为加以刑法的规制以发挥刑法的震慑作用。

3. 建立适应联盟链的动态监管制度

建立基于联盟链系统的动态监管制度可以助推法律由事前准入、事后监督的传统监管模式转向全程动态监管模式以适应联盟链系统。联盟链的加密机制、链式结构等将联盟链系统分隔为链上链下两个世界，链上的空间运行状态公开透明，每个节点都在参与系统的运行，而基于联盟链的多中心化特征也适合嵌入若干监管节点。故在“链”“法”协同机制中，可以构建基于联盟链系统的全程动态监管模式，将部分中心节点设为监管节点并使监管部门加入其中。如此不仅能够借助联盟链实现实时监管，还可以监测并预防联盟链应用可能带来的未知风险。首先，应当成立超级监管节点。在系统中将部分中心节点改造为监管节点，监听链上广播、储存信息，更新全网总账，掌握系统动态。一方面，监管部门通过监管节点实时获取系统内的共享信息，掌握链上活动，可以及时发现违法违规现象，提高监管效率。另一方面，监管部门通过监管节点实现一定程度上的自动执行和实时决策，可以及时根据系统运行情况变动系统规则进而有效预防可能发生的风险。其次，应当成立公权力监管部门，并通过法规或部门规章赋予其超级监管节点资格。即明确将数字防疫中个人信息治理监管权交由国家统一调度，由国务院主导，工信部会同网信办负责，协调多方职能部门，设立中央和地方层面的数字防疫中个人信息治理联盟链系统监督管理委员会。该委员会统筹领导联盟链系统的推进及监管工作，并作为超级节点被加入系统中，对系统进行实时监测。〔48〕同时明确该监管部门在事前审查、事中管理以及事后追责等阶段使用的程序和对应职责。还要赋予该监管部门独立的执法权和管理权，避免部门之间互相推诿等情况，促进数字防疫中个人信息治理联盟链系统监管规范化。最后，应当设立社会层面的行业协会。有必要

〔47〕 参见贾翱：《区块链信息服务监管对象研究——以〈区块链信息服务管理规定〉第二条为中心》，载《大连理工大学学报（社会科学版）》2020 年第 2 期。

〔48〕 参见时明生：《区块链技术在征信业的应用探析》，载《征信》2018 年第 1 期。

在监管部门之外设立独立的行业协会，并给予其一定自主权限。该协会可以针对联盟链系统发展的形势制定行业自律标准和实施细则，对系统进行定期风险评估与调查监测，同时促进信息持续上链和系统平稳运营以减轻公权力机关负担。

六、结　语

联盟链对于化解数字防疫的个人信息治理风险具有天然优势，可望缓解数字防疫与个人信息传统法律治理之间的冲突龃龉问题，进而破解个人信息治理之“危”，利用数字进行防疫之“机”。但基于联盟链的“技治”并不能完全取代基于法律的“制治”，以代码替代法律的设想也不可行。应当发挥联盟链的长处，结合法律治理的优势来构建数字防疫中个人信息“链”“法”协同治理机制。在大数据、人工智能等技术基础上继续应用联盟链是一项系统工程，应当在不断实践的基础上充分把握联盟链、法律各自的优势，以及数字防疫和个人信息治理的发展趋势，缓解联盟链与法律、数字防疫与个人信息治理之间的双重张力。同时需要指出：以联盟链为代表的区块链技术毕竟属于新兴技术，在应用方面仍处于探索阶段。联盟链应用可能带来的风险和挑战还需要进一步的探讨。

Abstract：In this epidemic prevention and control，digital technologies such as artificial intelligence and big data not only reduce the risk of epidemic spread，but also make personal information management face new risks. Alliance chain has been widely used in many fields in recent years，and has become a feasible tool to resolve the risk of personal information governance in digital epidemic prevention. However，while applying alliance chain governance risk，it is also necessary to optimize the corresponding system，so as to realize the “joint governance” of alliance chain and law under the action of technical iteration and system optimization. Therefore，we should eliminate the tension between alliance chain and law，and then build a “chain” and “law” coordination mechanism based on legal governance and supplemented by alliance chain governance. Specifically，by building an alliance chain governance mechanism matching the law and a legal governance mechanism matching the alliance chain，and integrating the respective advantages of blockchain technology and law，the “chain” and “law” coordination mechanism can improve its ability in personal information governance in digital epidemic prevention，thus improve the level of modernization of national governance.

Key Words：digital epidemic prevention，personal information governance，risk government，alliance blockchain，synergy between “blockchain” and “law”

（责任编辑：殷秋实　赵建蕊）